Data collection on security flaws caused by design errors

Harald Terkelsen

Master's Thesis
Master of Science in Information Security
30 ECTS
Department of Computer Science and Media Technology
Gjøvik University College, 2006

Institutt for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Preface

After three years of studying in my spare time while working a full time day job, it has not always been easy to find the energy or the time to work on the thesis in the evening after a long day at work first. But the motivation of finishing what I started and getting the master's degree has kept me going. The time has unfortunately run out, and the thesis is not as complete as I hoped it should be at this time.

I would like to thank my employer, Oslo University College (Høgskolen i Oslo), for letting me have days off work to follow the lectures at Gjøvik two days a week, six weeks each semester to pursue the masters degree. I also thank my supervisor Hanno Langweg, who originally proposed the topic, for his feedback on the drafts he reviewed, and also for being patience with my slow progression being a part time student.

Contents

1 Introduction

Producing secure software is extremely hard to do right. The number of security flaws and vulnerabilities discovered in software each day is increasing at high speed. According to the National Vulnerability Database the number of vulnerabilities discovered in 2005 was 4859, more than twice the number of vulnerabilities discovered the year before. One way to classify vulnerabilities is to classify them after when in the development phase they are introduced, for example[28]:

- Design
- Implementation
- Configuration

Other phases like analysis (requirements), testing, or maintenance phase are also sometimes used [40, 34].

This thesis is a study of security related flaws with origin in the design phase. Such flaws are rooted in the design of the software, and exist even if the programmer implements the design perfectly making no mistakes in the programming. Security related design flaws are a lot about how security mechanisms like authentication, authorization and encryption are used and implemented, or how error handling is performed. Typical examples of design flaws include weak encryption, missing or insufficient access control.

What make design flaws different from other classes of flaws?

- They often cost more to fix.
- They are not easily detected by testing or static analysis tools as implementation flaws.
- Two different implementations of a flawed design will both be vulnerable

Implementation flaws can often easily be fixed with small changes to the code, adding an extra check or using a more secure API call. Design flaws, on the other hand, are rooted in the design. Fixing them means making changes to the design. If the design is already implemented, changes to the design often means recoding parts of the code, sometimes changing larger portions of the code. The later in the development phase a design flaw is found, the more it cost to fix it. It can be 6.5 times more expensive to fix a flaw during the implementation phase than during design. And if the flaw is not found before the maintenance phase, it can cost as much as 60-100 times more. [18]

Static analysis tools are programs built to detect flaws by automatically examine the source code of other programs. Design flaws are not as easily detected by static analysis methods as implementation flaws are. This means it is harder to create tools to automate the search for design flaws. Several studies conclude that design reviews are more efficient for detecting design flaws than testing[44].

Security functionality are often added to software applications at the end of the development process when the rest of the functionality is finished, with weak security solutions as a result. There have been launched several books, reports and projects lately to increase the awareness and the importance of including security considerations in software projects from the start and throughout the entire software development process. Most notably is the *Build security in*[1] project by the Strategic Initiatives Branch of the National Cyber Security Division (NCSD) of the Department of Homeland Security (DHS) in USA. The mission statement on the project's web page describe the goal as "seeks to reduce software vulnerabilities, minimize exploitation, and address ways to improve the routine development and deployment of trustworthy software products". The Internet Engineering Task Force (IETF) has also seen the need to focus more on security in their protocols. In RFC 3631 from 2003 they state that all protocols should provide appropriate security mechanisms, even if it is believed that the protocol's domain of application is limited.

Taxonomies and classification schemes are tools which can be used to classify and analyze the different vulnerabilities and flaws that can be found in computer software. Over the years many classification schemes for software vulnerabilities have been proposed. They take different approaches to classifying vulnerabilities, depending on the researchers goal. Many of them have a special focus on operating system flaws. From a designers view point, an operating system has a more standardized set of functionality needed to be implemented than a software application which can be one of a kind. But many of the classifications that consider application flaws, are based on the same categories as those designed for classifying operating system flaws. This leads us to believe they might not be optimal in classifying design flaws.

Collections of discovered vulnerabilities exist in different vulnerability databases. Several of these databases have a classification scheme they use to indicate the type of vulnerability when data on the vulnerabilities are presented. Categories for design flaws exist, but only the top-level class "design flaw". No sub-categories for different types of design flaws seems to be used. The classification of the vulnerabilities does not seems to be consistent over the different databases. A vulnerability classified as design flaw in one database can be classified as something else in another database. The lack of subcategories for design flaws and the inconsistent classification between databases makes it difficult to gather empirical information about design flaws by querying the databases directly.

The main goal of this thesis is to provide researchers, software architects, software designers, and software programmers with empirical knowledge of the different types of design flaws recorded in vulnerability databases and their distributions. To reach this goal, a classification scheme for design flaws needs to be created, and this classification must be applied to vulnerabilities in the databases identified as design flaws according to a definition of design flaws.

The following research questions was identified:

1. What properties do vulnerabilities caused by security related design flaws have?
2. What can a classification of security related design flaws look like?
3. What are the most typical design flaws?

[1] https://buildsecurityin.us-cert.gov/daisy/bsi/home.html

To answer these research questions, we will use a qualitative content analysis and quantitative observation study. In [31], Leedy and Ormrod describes terminology related to these methods are as follows:

Qualitative design: Typically used to answer questions about the complex nature of phenomena.

Quantitative design: Typically used to answer questions about relationships among measured variables with the purpose of explaining, predicting, and controlling phenomena.

Descriptive quantitative research: Involves either identifying the characteristics of an observed phenomenon or exploring possible correlations among two or more phenomena.

Content analysis: A type of qualitative analysis that is a detailed and systematic examination of the contents of a particular body of material for the purpose of identifying patterns, themes, or biases.

Observation study: A descriptive quantitative method where typically the focus is on a particular aspect of behavior. The behavior is quantified in some way.

Mixed-method design: Combine elements from quantitative and qualitative design

What properties do vulnerabilities caused by security related design flaws have?
Mixed method of literature review and qualitative content analysis.

The literature covering security design patterns seems to give us some answers to parts of this research question. Design patterns describe typical design problems and how to solve them. The collections of security design patterns are probably not complete, but they will give us ideas for what to look for in the content analysis.

For the qualitative content analysis part, we will examine real design error vulnerabilities from selected vulnerability databases. We will try to identify their properties suitable for use in a classification.

What can a classification of security related design flaws look like?
To answer this question we used a content analysis method. A body of vulnerability descriptions was examined, design flaws was located and examined in detail to find features usable to as uniquely as possible categorize design flaws.

According to [28] classifications can be developed either non-empirical (a priory) or empirical (a posteriori). By basing our scheme on data on real vulnerabilities, this classification scheme was built empirical.

What are the most typical design flaws?
This research question is answered using a quantitative observation study. The examined vulnerabilities will be classified according to our proposed classification. This dataset will then be analyzed statistically to try to identify vulnerabilities and properties that appear more frequently than other.

Validity of the developed classification
An experimental design was used to evaluate the validity of the developed classification. Vulnerabilities was classified according to the developed classification and a few other

classifications proposed in the literature, classifications used by vulnerability databases, and design principles. The results from using the different classifications was then measured against each other.

The answer to these research questions and the work done to answer them has provided:

- New empirical knowledge on the distribution of different design flaws
- An evaluation of some classification schemes and design principles
- An evaluation of the data in vulnerability databases

2 Previous and related work

2.1 Software design

2.1.1 Design principles

Design principles are guidelines for how to design secure systems. In their classic paper [45], Saltzer and Schroeder examines methods to protect information stored in computer systems. The paper presents a collection of design principles that applies especially to protection mechanisms. The design principles are:

Economy of mechanism - The design should be as simple and small as possible.

Fail-safe defaults - The default should be no access. Permission should be granted for access.

Complete mediation - Every access to every object must be checked for authority.

Open design - Object protection must not depend on the secrecy of the protection mechanism. The only item needed to be kept secret is the key or password.

Separation of privilege - A protection mechanism should not depend on one key or method alone. Two or more conditions should be met before access is granted.

Least privilege - To complete a job, no more privileges than absolute necessary should be needed. If you only need to read a file, you don't need write privileges.

Least common mechanism - Mechanisms should not be shared unnecessarily beetween users because it can provide a channel for information to travel.

Psychological acceptability - Human computer interfaces should be as easy to use as possible.

In addition to these eight principles, they also mention two other principles which do not apply well to computer systems, work factor and compromise recording.

Work factor - The cost of circumventing the protection mechanism versus an attacker's resources. For many computer protection mechanisms, it is not possible to calculate the work factor.

Compromise recording - Mechanisms that reliably record that a compromise has happend can in some situations be used instead of mechanisms that prevent the compromise from happening.

Ten security design principles are also presented by Viega and McGraw in [51]. Although some of these principles are different, others are the same or similar to those in [45] The principles are:

Secure the weakest link - A software security system is often only as secure as its weakest component, just like a chain is only as strong as its weakest link. A good risk analysis should identify the weakest links to address first.

Practice defense in depth - Several layers of defense is more secure. If one layer fails, then the next layer may prevent an attacker in getting more access.

Fail securely - If something goes wrong with a system, it's important that the system still is in a secure state.

Follow the principle of least privilege - Like *least privilege* from [45].

Compartmentalize - If a component of a system is compromised, the compromise should be local to that component, the security of the other components should not be affected.

Keep it simple - Like *economy of mechanism* from [45].

Promote privacy - Sensitive personal information must be handled with special care. Users must get to trust that their personal information is handled in a secure manner. This principle also applies to information given away about the type and version of your system.

Remember that hiding secrets is hard - Keeping secrets hidden in binary files secret is difficult to achieve. Given time and resources, an attacker will almost certainly be able to reverse engineer the binary file and extract algorithms, keys or other data. Also consider the insider threat.

Be reluctant to trust - Be skeptical to your peer. Servers shouldn't trust clients. Clients shouldn't trust servers blindly either. Social engineering is a problem because we trust people.

Use your community resources - Other people can find flaws you don't see yourself.

The book Secure Coding: Principles & Practices [16] presents an extensive list of 30 security architecture principles. We won't list them all here, but they are based on earlier work in [45, 42, 49] among others. They range from concrete principles like "fail safely" to more general high-level guidelines like "Start by asking questions" or "remember to ask, What did I forget?".

The NIST Technical report 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems [49], presents eight principles and fourteen practices. The principles are very abstract high-level principles based on OECD's Guidelines for the Security of Information Systems [38]. Some of the practices are more low-level like "Identification and Authentication" and "Logical access control". The principles in [38] have later been updated and published in OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security [39]

The principles and practices in [49, 38, 39] are not special for software design, but they are more general principles meant for building systems, policies, or controllers. This is why the principles are very high-level.

Many of the principles, even from the same collection, are not necessarily complementary. Some are overlapping and others are even in conflict with each other. Design

principles must therefore not be applied independently, but in the context of the whole system. A discussion of the conflicting characteristics of design principles is found in [37].

2.1.2 Security design patterns

Patterns are recurring solutions to common problems (in a given context and system of force). The concept of patterns was first used by Cristopher Alexander in buildings architecture. Parallels could be seen in software architecture, and the publication of *Design Patterns* in 1994 made the usage of patterns widespread in software design.

A security pattern is a design pattern in the context of information security. Schumacher defines security pattern as "A security pattern describes a particular recurring security problem that arises in specific contexts and presents a well-proved generic scheme for its solution" [48].

A pattern must include some mandatory elements. The "Mandatory Elements Present" pattern in [36] describes which elements a pattern should include. This patten can be considered a meta-pattern, a pattern describing what a pattern should include. According to [36], a pattern should at least include these descriptions:

- Name
- Context
- Problem
- Forces
- Solution

Security patterns does not only describe problems in computer programs, but can also describe security in whole systems or network design. Another class of security patterns identified in [27] is procedural patterns which describes patterns to improve the development process.

A collection of patterns for systems which "protect valuable resources against unauthorized use, disclosure, or modification"; and uninterrupted access is found in [6]. A often used example of a design error in vulnerability papers is weak encryption. Examples on patterns for encryption usage in software development can be found in [7, 32].

The website at http://www.securitypatterns.org/ has a list of work on security patterns. One of the more recent collection of security patterns is found in the book Security Patterns: Integrating Security and Systems Engineering [47].

2.2 Taxonomy and classification theory

In his Ph.D. thesis [28] Krsul discusses the differences of taxonomy and classification terms. He also show that many researchers confuse these terms by giving examples of proposed taxonomies and classifications and why they fail to be a taxonomy or classification as they claim to be.

Bishop does a detailed examination of this problem in [5] where he uses two vulnerabilities as examples to show how the taxonomies presented in [1, 4, 2] all fail the criteria of being a taxonomy by being able to classify the two chosen common vulnerabilities in multiple categories in each of the classifications. The reason being that the taxonomies fail to take into account the point of view of the flaw and the level of abstraction.

2.3 Software flaw taxonomies

Over the years, many different taxonomies and classification schemes for flaws and vulnerabilities in computer software have been proposed. Many of them have been developed to solve a specific research problem where the existing classifications have been found to be insufficient for the particular research problem the researcher wants study.

- Specialized security taxonomies
- General defect classifications

Software defect classifications have a broader scope than just classifying security problems with software. Typically they include all kinds of anomalies and defects found not only in the software itself, but also defects in other deliverables of the software development process like requirement documents and user documentation. This means they also include many attributes not needed in the more specialized security flaw taxonomies, for example which project activity was performed when the defect was found, or how to prevent the defect from happening again. Having a broader scope, they typically also tend to classify the defects at a higher abstraction level than security taxonomies do.

Security taxonomies are those specialized for classifying security problems in software. Such problems are often described as flaws, faults, vulnerabilities or attacks.

2.3.1 Security taxonomies

Some of the earlier works include the RISOS study published in 1976 [1] and the PA (Protection Analysis) study [4] published in 1978. Both of these studies came up with similar classes of flaws. Their focus was on flaws in operating systems.

The RISOS study [1] classified flaws into seven general classes:

1. Incomplete parameter validation
2. Inconsistent parameter validation
3. Implicit sharing of privilege/confidential data
4. Asynchronous validation/inadequate serialization
5. Inadequate identification/authentication/authorization
6. Violable prohibition/limit
7. Exploitable logic error

The *Incomplete parameter validation* category is for flaws where the parameters are not properly validated. Validation can be done for type, format, number, order, or values of parameters among others. *Inconsistent parameter validation* is a special case of *Incomplete parameter validation*, but it differs in that some parts of the system does the validation right, and one part does it incomplete. The paper uses an example where the creation of a file right accepts a space character in the permission name, while other functions for changing or deleting rights do not accept a space character in the permission name. *Implicit sharing of privilege/confidential data* is when privileged information is leaked to unprivileged users through other channels than the designated way to access the information. Such leaking can happen *explicit* in such a way that the information is directly

accessible or *implicit* where the data can be derived by comparing results of several operations on functions handling the data. *Asynchronous validation/inadequate serialization* are flaws that exist because it is possible to change an object in the timeframe from when its value is first checked to when it is used. This is also called a 'time-of-check to time-of-use flaw (TOCTOU). To the *inadequate identification/authentication/authorization* category belongs flaws that happens because a user or program is not identified sufficiently, or if a program or user try to access a resource and it is not sufficiently checked that the user or program have the needed privileges to access the resource. *Violable prohibition/limit* is used when the documentation specify a limit on some resource usage (table or buffer), but the operating system is not enforcing that limit. *Exploitable logic error* can for example be errors that happen because checks are done in the wrong order. The classification from the RISOS study has been built on by several other classifications published in recent years, like [30, 12, 29].

The protection Analysis study ended up with these ten classes:

1. Consistency of data over time
2. Validation of operands
3. Residuals
4. Naming
5. Domain
6. Serialization
7. Interrupted atomic operations
8. Exposed representations
9. Queue management dependencies
10. Critical operator selection errors

It was recognized that these ten classes could be categorized using only four classes: *Domain, Validation, Naming and Serialization* with the remaining classes falling into or being split into these four main categories.

Consistency of data over time means that the data should not change from when it is first checked to when it is used. *Serialization* means that the operating system should prevent concurrent use of some resources to prevent change. This is the same category as Asynchronous validation/inadequate serialization from the RISOS study. Also *Interrupted atomic operations* can be said to belong to this category. This class of flaws happen when an operation can be interrupted, leaving the operation in an insecure state. *Validation of operands* is the same as incomplete/inconsistent parameter validation from RISOS.

Residuals is "left over" information in re-allocated objects. *Exposed representations* means that it is possible to manipulate the internal structures of an object without using the designated API calls. *Domain* errors are when objects are associated with the wrong domain, or when there is not adequate checks when crossing a domain border. These three classes is the same as *Implicit sharing of privilege/confidential data* from RISOS. *Naming* errors are errors where it is difficult for the operating system to distinguish between two different objects. This class is equal to inadequate identification/authentication/authorization errors from RISOS. To the *Queue management depen-*

RISOS	PA
Incomplete parameter validation	Validation of operands
Inconsistent parameter validation	
Implicit sharing of privilege/confidential data	Residuals
	Exposed representations
	Domain
Asynchronous validation/inadequate serialization	Consistency of data over time
	Serialization
	Interrupted atomic operations
Inadequate identification/authentication/authorization	Naming
Violable prohibition/limit	Queue management dependencies
Exploitable logic error	Critical operator selection errors

Table 1: How the RISOS and PA categories maps to each other

Intentional	Malicious	Trojan Horse	Non-replicating
			Replicating (virus)
		Trapdoor	
		Logic/Time Bomb	
	Nonmalicious	Covert Channel	Storage
			Timing
		Other	
Inadvertent	Validation Error (Incomplete/Inconsistent)		
	Domain Error (Including Object Re-use, Residuals, and Exposed Representation Errors		
	Serialization/aliasing (Including TOCTTOU Errors)		
	Identification/Authentication Inadequate		
	Boundary Condition Violation (Including Resource Exhaustion and Violable Constraint Errors		
	Other Exploitable Logic Error		

Table 2: Landwehr et al's Genesis dimension

dencies category belong errors where the boundary of datastructures are not enforced properly. It is the same as Exposed representations from RISOS. Buffer overflow errors belongs to this class. *Critical operator selection errors* like *Exploitable logic error* from RISOS are a catch-all class to use when an error does not fit into one of the other classes.

Table 1 shows how the categories from the RISOS and the PA studies maps to each other.

Landwehr's taxonomy

Next to the RISOS and PA classifications, one of the classifications that has been most influential is the one presented by Carl Landwehr et al in 1994, *A Taxonomy of Computer Program Security Flaws*[29]. This taxonomy uses three dimensions: *Genesis* (how did the flaw enter the system), *Time* (when did the flaw enter the system) and *Location* (where in the system does the flaw manifest itself). The introduction of multiple dimensions allows researchers do describe flaws more accurately and it provides more statistical information than taxonomies using only one dimension. Its primary focus is on flaws in operating systems. No categorization of flaws in applications are done. He uses 50 actual flaws as examples on how to use use the taxonomy.

A hierarchical approach is used two classify the flaws. The genesis dimension has two

During Development	Requirement/Specification/Design
	Source Code
	Object Code
During Maintenance	
During Operation	

Table 3: Landwehr et al's Time of Introduction dimension

Software	Operating System	System Initialization
		Memory Management
		Process Management/Scheduling
		Device Management (Including I/O, networking)
		File Management
		Identification/Authentication
		Other/Unknown
	Support	Privileged Utilities
		Unprivileged Utilities
	Application	
Hardware		

Table 4: Landwehr et al's Location dimension

top level categories, *intentional* flaws and *inadvertent* flaws. Intentional flaws are features deliberately included in the program. Landwehr et al differentiate between *malicious* and *non-malicious* intentional flaws. Malicious flaws are logic/time bomb, trapdoor or a trojan horse, while non-malicious are *covert channels* or the catch-all *other* class. You have a covert channel when it is possible to transfer information with a mechanism not designed to be used to transfer that information.

Inadvertent flaws are introduced because of incomplete requirements, errors in the design or mistakes made by the programmer who implements the design. These categories are similar to those found in the RISOS and PA categories reviewed earlier in the chapter. Some of the classes are combined and use the most descriptive name from either the RISOS or the PA categorizes.

The time of introduction dimension is is easy to understand. A flaw can be introduced during development, maintenance or operation. During development a flaw can be introduced either at the requirement/design phase, in the source code during programming or when the source code is compiled into object code. While fixing a flaw during maintenance, it is easy to introduce new flaws either because of programming mistakes or because the design is not known well enough by the programmer assigned to the maintenance job. The paper uses viruses as example on flaws introduced during operations.

The *location* dimension describes where in the system a flaw is introduced or found. At the top level flaws can be found either in hardware or software. Only the software location are further classified into three sub-categories: *operating system*, *support* (privileged or unprivileged support tools) and *application*. No sub classification are done for flaws found in applications. This probably reflects the taxonomy's focus on operating systems, which the location can be specified more precisely by the following locations: System Initialization, Memory Management, Process Management/Scheduling, Device Manage-

ment (Including I/O, networking), File Management, Identification/Authentication, or Other/Unknown.

One problem with this taxonomy is that some of the classes are broad, like in RISOS and PA, and ambiguous. When describing validation flaws, failed or misplaced checks of file permissions on a file is used as an example. This is the same as ”permits a protected operation to be invoked without sufficiently checking the identity and authority of the invoking agent“ in the description of identification/authentication flaws. Even though it is acknowledged that such flaws could be classified as validation errors, it is not clear from the description to which category such flaws should be classified, neither from the name of the classes or the description. They would probably be classified best as identification/authentication flaws.

The division of the categories into subcategories does not seems to have any functional relevance, only logical, because the subcategories all have unique category names. If the same class existed both as an intentional and an inadvertent flaw, the division in subclasses would have a functional relevance.

Aslam's taxonomy

Aslam et. al. proposed a taxonomy [2] in 1996 focusing on security faults in the Unix operating system. Faults are classified as either coding faults or emergent faults. Coding faults are either synchronization errors or condition validation errors. Emergent faults are either configuration errors or environment errors. The reason the fault exist is not considered, which means that vulnerabilities caused by design errors can not be classified. Aslam provided a set of selection criteria to help classify faults in the right class. But as [5] shows, he failed to do so properly. Depending on the point of view, it is possible to classify a fault in different categories. A prototype vulnerability database using this taxonomy was also designed and built.

Lindqvist and Jonsson's classification

After trying to apply existing classifications on intrusion data, and finding them too superficial or not focusing on aspects they wanted to observe, a new classification was proposed in [33]. The focus of this classification is on external observations of attacks and breaches, that a system owner can make - from a system owner's view. Two dimensions are used: intrusion techniques and intrusion results.

Ivan Krsul's taxonomy

For his 1998 PhD thesis *Software vulnerability analysis*[28], Ivan Krsul examined flaws focusing on the ”assumptions that programmers make regarding the environment in which their application will execute”. He has a strong focus on taxonomic completeness. One of the results from his thesis is a list of taxonomic characters to be used as a foundation for classifications and taxonomies. Taxonomic characters make it possible to use a classification without using a decision tree. He divide such characters into two main groups:

- Environmental assumptions features
- Features on the nature of vulnerabilities

All environmental assumptions features are directly under the main category. But features on the nature of vulnerabilities are further divided into:

- Objects affected
- Effect on objects
- Method or mechanism used
- Input type

Another contribution from his PhD thesis is a classification of vulnerabilities. A hierarchical classification is proposed. It has four top level categories:

1. Design
2. Environmental assumptions
3. Coding faults
4. Configuration errors

Only the environmental assumptions are detailed. This category is subdivided into *environmental object, object attributes,* and *attribute constraints*.

The environmental objects defined are:

- Running program
- User input
- Environment variable
- Network stream
- Command line parameter
- System library
- File
- Directory
- Program string
- Network IP packet

If we look at the object *environmental variable*, its object attributes are *name* and *content*. The attribute constraints of the content attribute are: *length is at most x*, *length is at least x*, *matches regular expression* and *is free of shell metacharacters*.

Piessens' taxonomy

[40] is a taxonomy that treat design errors as a separate case. It focuses on causes of software vulnerabilities and uses a two-level hierarchy where the top level is the phase of the development cycle in which the vulnerability are introduced into the system. The phases are: analysis, *design*, implementation, deployment, and maintenance phase. It identifies five different kind of vulnerabilities in the design phase: *Crypto protocol design errors, relying in non-secure abstractions, security/convenience tradeoff, no logging,* and *design does not capture all risks*. This taxonomy can be used internally for a software

developer's own use, but it is not easy to use on public vulnerabilities because we seldom know the degree of risk analysis that has been done on software. The analysis phase is therefore of little value unless you know the whole development process behind the product.

Du and Mathur's classification

Du and Mathur wanted to test software with the goal of "detecting errors that might lead to security breaches" [12]. Their classification scheme focus on software faults in general, and is applicable for both operating system and application software. A vulnerability categorized using this scheme is a three-tuple consisting of a *cause, impact* and *fix* category. The cause is a modified version of [29]'s genesis category. It uses only the inadvertent class from genesis, but made some modifications to the definition of some of the categories to make it unambiguous. Validation flaws where changed to be of type input, origin or target. Flaws where the cause is failure to properly check the identity, ie authentication are placed in the validation class. The name of the second cause category, authentication error, is somewhat misleading as the description clearly states that it is meant for flaws not sufficiently checking the authority of the invoking agent. *Authorization error* would be a better descriptive name for this class. One class was also added to the cause category: *weak/incorrect design*.

The *impact* category consist of four possible actions the flaw can result in. The *fix* category consists of what can be done to correct the error. It is the same as described in [11] The fix attribute of the tuple seems to be of little value unless the source code containing the vulnerability is available.

Jiwnani and Zelkowitz' classification

With the goal of "devise a classification of vulnerabilities to abstract information about problems in software development, their location and their impact on the system to concentrate and increase testing effort in those areas", Jiwnani and Zelkowitz proposed a taxonomy for flaws found in operating systems[26]. It uses three dimensions: *Software development issues*, *Location of flaws in the system* and *Impact of flaws on the system*. The first two are simplified versions of the *genesis* and *location* dimension from [29] modified to only include the categories relating to flaws found in operating system. The simplification also includes getting rid of the tree structure, only using a flat dimension.

Langweg and Snekkenes' classification

A classification of attacks by malicious software [30] was proposed by Langweg and Snekkenes in 2004. It is a classification of attacks on software applications, not operating systems as many other classifications cover. This classification is based on modifications of earlier work. Attacks are classified by input (location), exploitable logic in processing (cause), and output of a program (impact). Location is different from [29], and is defined as the part of the application perimeter where an input can be introduced. Cause uses traditional categories and is the same as in [12]. Impact is also based on [12] but with subclasses borrowed from [33]. This classification is intended to be used in automatic searching for vulnerabilities with vulnerability scanners, and also to develop metrics to quantitatively evaluate application robustness.

Weber et al's taxonomy

Also using [29] as a starting point, this taxonomy described in [52] aims to help designers of code analysis tools. Certain classes of flaws not easily detectable with such tools, are therefore not included in this taxonomy. This includes many design error flaws. Only the *genesis* dimension from [29] is used, but it's modified to address the critics that has been held against it, and to include newer flaws which have been seen in recent years. Subcategories have been added to many of the categories from [29] to differentiate the flaws on a lower level of abstraction. This makes it clearer what kind of flaw it is. This taxonomy is not unambiguous, but the authors argue that if a flaw can be classified under several categories, it is a result of the characteristics of the flaw itself.

Interest in vulnerability classification seems to have risen again in 2005 with several new taxonomies published and projects started in 2005 and 2006 [52, 50, 9, 46, 41, 34]. Most of these new taxonomies are somewhat different from the earlier ones in their form. The new trend is to have a few top level categories (often 7 +/- 2) and many second level low abstraction subcategories, thus being much more precise than earlier classification schemes.

Tsipenyuk et al's taxonomy

The first of these new taxonomies we will describe is [50]. It was created with the intention of helping developers "understand common types of coding errors that lead to vulnerabilities". Each type of coding error is called a *phylum*. A collection of similar phyla is called a *kingdom*. There are seven plus one kingdoms. They are:

1. Input Validation and Representation
2. API Abuse
3. Security Features
4. Time and State
5. Errors
6. Code Quality
7. Encapsulation

- Environment

The taxonomy aims to be more practical than theoretical complete. But this trade off makes the taxonomy ambiguous. Several of the phyla in the *API abuse* kingdom seems to overlap with phyla in the *Input Validation and Representation* kingdom.

Common Weakness Enumeration

Another project trying to come up with a standard taxonomy the security community can agree on, is the Common Weakness Enumeration - CWE. The idea is that a common taxonomy can provide a measuring tool for comparing security software and serve as a common language for vulnerability identification. The approach they take is to merge most of the earlier work. This is still work in progress, and draft 2 is the latest published

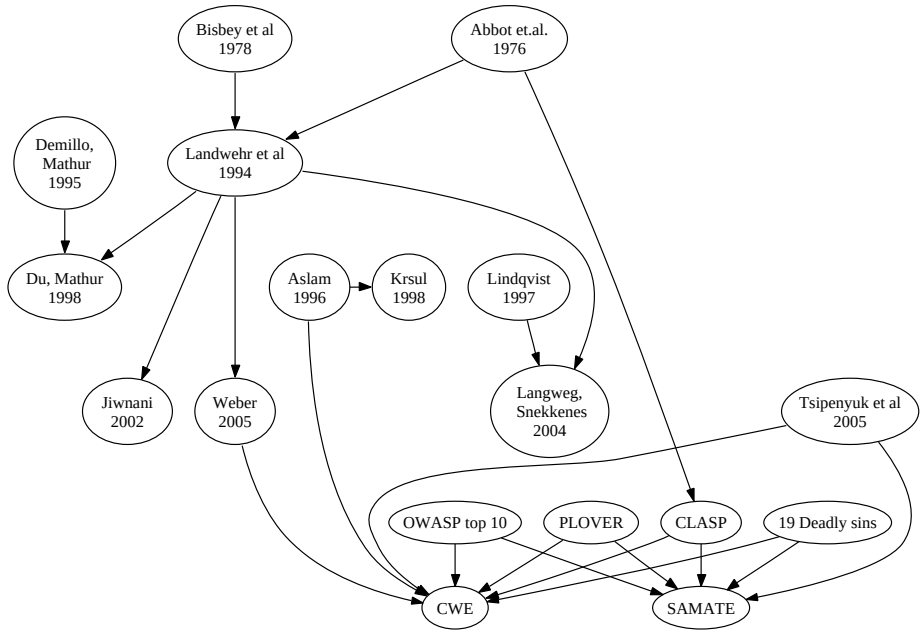

Figure 1: Overview of some of the existing taxonomies

on their web site as this is being written. CWE draft 2 uses three dimensions or top levels: Location, Motivation/Intent and Time of introduction. The majority of the classes being in the Location, Code, Source Code category.

Table 5 shows a list of the most important taxonomies described above. Figure 1 tries to give an overview of the relationship between the different taxonomies. It's not complete with regards to relationship, but tries to group those we can say are somehow similar.

Author	*Year*	*Name*
Abbot [1]	1976	Security analysis and enhancements of computer operating systems
Bisbey II [4]	1978	Protection analysis: Final report
Landwehr [29]	1994	A Taxonomy of computer program security flaws, with examples
Aslam [2]	1996	Use of a taxonomy of security faults
Lindqvist [33]	1997	How to systematically classify computer security intrusions
Du & Mathur [12]	1998	Categorization of software errors that led to security breaches
Krsul [28]	1998	Software vulnerability analysis
Piessens [40]	2002	A Taxonomy of software vulnerabilities in internet software
Jiwnani [26]	2002	Maintaining software with a security perspective
Langweg [30]	2004	A classification of malicious software attacks
Weber [52]	2005	A software flaw taxonomy: aiming tools at security
Tsipenyuk [50]	2005	Seven Pernicious Kingdoms: A taxonomy of software security errors

Table 5: List of vulnerability classifications

2.3.2 Defect classifications

One of the better known defect classifications is the *Orthogonal defect classification* developed by IBM and first described in [8] with the latest version found on the IBM website.[1]

[1] http://www.research.ibm.com/softeng/ODC/ODC.HTM

IEEE has developed “Standard Classification for Software Anomalies” [24]. This standard is intended to be tailored to each organization’s needs. The attributes marked as *Mandatory* must be included, but *Optional* attributes are just that, optional. The standard describes a process for the classification consisting of four steps:

1. Recognition
2. Investigation
3. Action
4. Disposition

Anomalies are recorded, classified and the impact are identified in each of the four steps.

An overview of how to create and use defect classifications can be found in [14]. It gives a list of attributes that can be classified, structures of classification schemes, and how to use classification schemes to analyze defect classification data.

2.4 The Common Vulnerabilities and Exposure list (CVE)

CVE can at first glance look like a vulnerability database, but it’s not. It really is a dictionary giving unique names to publicly known vulnerabilities and exposures. It’s a tool for vulnerability databases to identify their cataloged vulnerabilities and a tool which enable easy comparison off different security tools and services. The unique name given to each CVE entry is on the form CVE-yyyy-xxxx, where yyyy is the year and xxxx is a number given to the vulnerability or exposure. Each CVE entry contains the following:

- The CVE name
- Status (Entry or Candidate)
- A brief description
- References to more detailed descriptions

2.5 Common Criteria

The Common Criteria [10] is a standard for the evaluation of security functionality in information technology. It defines a set of common evaluation criteria for software to make it easy to evaluate the level of security provided by a product’s design and development process. It can also be used by designers to choose appropriate security measures to reach a certain level of security.

3 Software Design and Software Flaws

3.1 Software design

Depending on who you ask, you may get different answers to what software design is. This section will clarify the usage of the terms related to software design as used in this thesis.

According to IEEE Standard for Developing Software Life Cycle Processes [20] (p. 43), the following activities are to be performed during the design phase:

- Perform Architectural Design
- Design Data Base (If Applicable)
- Design Interfaces
- Perform Detailed Design

The IEEE Standard Glossary of Software Engineering Terminology (IEEE Std 610.121990) [22] gives definitions for several terms related to software design:

design: The process of defining the architecture, components, interfaces, and other characteristics of a system or component.

Architecture: The organizational structure of a system or component.

architectural design: The process of defining a collection of hardware and software components and their interfaces to establish the framework for the development of a computer system.

detailed design: The process of refining and expanding the preliminary design of a system or component to the extent that the design is sufficiently complete to be implemented.

interface: 1)A shared boundary across which information is passed. (2) A hardware or software component that connects two or more other components for the purpose of passing information from one to the other. (3) To connect two or more components for the purpose of passing information from one to the other. (4) To serve as a connecting or connected component as in (2).

Other sources seems to agree to the four activities to perform during design, but with slightly different wordings. For example [17] (p. 128) lists the following four phases in the design process:

- Data design: This phase produces the data structures.
- Architectural design: This phase produces the structural units (classes).
- Interface design: This phase specifies the interfaces between the units.

- Procedural design: This phase specifies the algorithms of each method.

And [2] cites [43] saying software design focuses on four attributes of the program: data structures, software architecture, procedural detail, and interface characterization.

The result of the design phase should be a design description, defined in [22] as:

Design description: A document that describes the design of a system or component. Typical contents include system or component architecture, control logic, data structures, input/output formats, interface descriptions, and algorithms.

Further details on what a software design description should describe can be found in IEEE standard 1016-1998, IEEE Recommended Practice for Software Design Descriptions [23]. A design entity is a functionaly distinct element or component of a design and can be a system, subsystem, data store, module, program, or process. A system should be divided into design entities which can be implemented with minimal effects on other entities. The description of a design entity should at least contain the following attributes, according to [23]:

Identification: The name of the entity.

Type: A description of the kind of entity.

Purpose: A description of why the entity exists. What requirements the entity is supposed to support.

Function: A statement of what the entity does. The transformation it does on input to produce output.

Subordinates: What other entities this entity is composed of. Gives a structural overview of the system decomposition.

Dependencies: The relationship this entity is having with other entities.

Interface: A description of how other entities interact with this entity.

Resources: A description of the elements used by the entity that are external to the design.

Processing: A description of the rules used by the entity to achieve its function. This is a description of the algorithms used by the design entity, and includes what to do in case of validation failures.

Data: A description of the data elements internal to the entity.

Table 6 lists more detailed information on what design attributes should describe. This table is derived from the detailed description of the attributes described in [23]. The lists of attribute values listed in the second column are not necessarily complete. Some of them are required, and some lists are incomplete lists of examples of what can be described.

Attribute	*Attribute values*
Identification	Unique name that identify the entity
Type	subprogram, module, procedure, process, data store.
Purpose	Rationale for the creation of the entity. Designate the specific functional and performance requirements for which this entity was created. Describe special requirements that must be met by the entity that are not included in the software requirements specification.
Function	State the transformation applied by the entity to inputs to produce the desired output. Data entity: State the type of information stored or transmitted by the entity.
Subordinates	Identify the *composed of* relationship of the entity
Dependencies	Data flow diagrams, transaction diagrams or other type of diagrams. Initiation, order of execution, data sharing, creation, duplicating, usage, storage, or destruction of entities.
Interface	Methods of interaction: mechanisms for invoking or interrupting the entity, for communicating through parameters, common data areas or messages, and for direct access to internal data. Rules governing those interactions: communications protocol, data format, acceptable values, and the meaning of each value. A description of the input ranges, the meaning of inputs and outputs, the type and format of each input or output, and output error codes. For information systems, it should include inputs, screen formats, and a complete description of the interactive language.
Resources	Physical devices (printers, disc-partitions, memory banks), Software services (math libraries, operating system services), Processing resources (CPU cycles, memory allocation, buffers).
Processing	Timing, sequencing of events or processes, prerequisites for process initiation, priority of events, processing level, actual process steps, path conditions, and loop back or loop termination criteria. Handling of contingencies: the action to be taken in the case of overflow conditions or in the case of a validation check failure.
Data	Method of representation, initial values, use, semantics, format, and acceptable values of internal data. Data specifications such as formats, number of elements, and initial values. The structures to be used for representing data such as file structures, arrays, stacks, queues, and memory partitions. The meaning and use of data elements: static versus dynamic, whether it is to be shared by transactions, used as a control parameter, or used as a value, loop iteration count, pointer, or link field. A description of data validation needed for the process.

Table 6: Attributes of design entities in a software design description as described in [23]

3.2 What is a design flaw?

Now when we have defined some basic terms about design, we can start clarifying what a design flaw is. Three definitions of design error/defect/vulnerability were found in the literature:

1. Design error: Failure to satisfy an understood requirement [15].
2. Design defect: A mistake made in the design of a software product.This includes defects found in functional descriptions, interfaces, control logic, data structures, error checking, and standards [13].
3. Design vulnerability as: a vulnerability inherent in the design or specification of hardware or software whereby even a perfect implementation will result in a vulnerability [19].

The definition of a design vulnerability in [19] tells most about the behavior of design flaws, while the definition of a design defect from [13] describes the properties that enables this behavior. A more supplementary definition can be created by combining elements from these two definitions:

Definition: 1 ***Design flaw****: An error in a software's design that exists independently of a concrete implementation. This behavior typically manifests itself in the algorithms, datastructures, or interfaces used*[1].

This is the definition used in this thesis.

Vulnerabilities caused by design flaws typically exist because of missing or weak design of a system's security functions, but they can also exist in parts of the program not directly related to security functionality. Examples of security functions are authentication, authorization, or cryptography usage.

While studying the literature for examples on design flaws, one can be lead to think that design flaws are of higher level of abstractions. Typical examples given on design flaws in the literature are:

- Missing or insufficient access control
- Missing or weak encryption
- Weak error handling
- Depending on untrusted components

But the content of design descriptions as presented in [23] shows that design can also be very low level. The data attribute for example states that initial values and acceptable values should be described in the design. The processing attribute states that such elements as loop termination criteria should be described.

3.3 Design versus Implementation

In a perfect world with a formal design process and access to the design documents, it would be very easy to decide if we are dealing with a design flaw or an implementation flaw. The roles of the designer and the programmer would be clearly separated, and the programmer is provided with a sufficient detailed design to implement. Flaws that

[1] Suggested by Hanno Langweg

are of lower level than provided in the design documents would be implementation flaws. But unfortunately the world is not perfect. Often no formal design process exist, or the design provided to the programmer is only a high level design or only consists of requirements. Provided with only a incomplete design document, the programmer is often finding himself doing the low level design of a program during implementation [35]. This blurs the borders of design and implementation since the detailed design would probably change with another implementation. The design a programmer does is also often not documented, making it even harder to know if it is an implementation error or design error.

If the design is sufficiently complete and we have access to the design document, it would be easy to decide if we are dealing with a design flaw or an implementation flaw. Without access to design documents, some assumptions must be made. One important assumption is that *the programmer is always following the design*. A design can say one thing, but the programmer can forget to implement a vital check, which would make it an implementation error. The design can be vague or insufficient, leading to two implementations where one is vulnerable and one is not. The next assumption is that *if the design is insufficient and the programmer must make assumptions about it, doing the low level design himself, we are talking about two designs*. Because of lack of access to design documents, the programmer is given the benefit of the doubt and the blame is placed on the designer when we examine the vulnerability databases.

If the programmer is doing both the detailed design and the implementation simultaneously, deciding if it is a design flaw or an implementation flaw can be hard.

But at what level is the design sufficient enough for implementation?

Some examples:

Sometimes a program can have access to data from several sources. For example a shopping cart application where the client returns to the server a list of items he wants to buy. This list also includes the items' prices. In a perfect program the server would calculate with its own stored prices. A flawed program makes the calculation with the prices it received from the client. The client did get them from the server in the first hand, didn't he? If the design says to calculate with the values it received from the client, then it's no doubt a design flaw. If the design just says calculate the sum of the ordered items, without going into more detail, then the design is probably not sufficient enough for implementation, meaning the programmer has to do parts of the detailed design. But common sense says that you should use the known secure prices read directly from your own database, and not the prices sent to you from the client. Since this is common sense and another programmer would probably do it right, does it make it an implementation error? A good design would only have the client send some sort of item number and probably not send the prices. So this is a problem with data flow, which should be a part of the design document [21]

3.4 Some common implementation flaws and why they are not design flaws

Buffer overflow and and similar flaws

This is probably the easiest class of flaws to ascertain not being a design flaw. They exist because the programmer don't make sure a buffer (array) is large enough to hold an input. It's a problem with low-level programming languages like C, C++ and Assem-

bly. Two different programmers can easily make one secure and one insecure program from the same design. Implementations in higher level programming languages like Java, Python, Perl or C# does not have this problem at all. These type of flaws are certainly at a much lower level than the what design should care about.

Input validation

Input validation flaws exist because of a failure to check the supplied input for legal characters and escaping illegal characters. The result being modification of SQL queries (SQL injection), execution of code (code injection), insertion of JavaScript in web pages (Cross site scripting - XSS) When it comes to SQL, some of the attacks can be easily stopped by using library calls that automatically does the needed escaping of the input characters, or by using prepared statements. Prepared statements separates the SQL query and the query parameters.

".." attacks

A special case of input validation is the ".." attack. An attacker can supply a file name of "./../../../../etc/passwd" to try to access files outside a given directory. This kind of flaw exist because the string containing the file name is not reduced to a canonical form before being used. The canonical form of a filename is the absolute filename. Most APIs have a function call to find the absolute filename.

(PHP) file include

This is mainly a problem with php applications, but other programming languages can also have this vulnerability. The problem is that an attacker is able to specify a local or remote file which is included in the code. One reason for this is if the PHP setting register_globals is set to on. Earlier versions of PHP had this set to on as default, later versions has turned this off, but still many administrators enable it. If set to on and variables used to contain the file name to include is not initialized, then it is in some situations possible for an attacker to specify this variable and the file to be included as an argument to the vulnerable PHP code.

Time of Check To Time of Use (TOCTOU)

Some TOCTOU errors certainly are design errors, but not all. One special type of TOCTOU error are those that make "symlink attacks" possible. These type of flaws exist because of failure to check that the file you are writing to in fact is the same you opened earlier in the program execution. This is mainly a problem with Unix like operating systems and their file systems that allow symbolic links. The Windows family of operating systems with FAT/FAT32/VFAT file system seems not to be affected by this type of flaw. It can be argued that with a better detailed design, these types of flaws can be avoided. But such detailed design also enters the programmer's domain.

Insecure temporary file creation is one kind of TOCTOU flaws. If programmers use old traditional ways to create temporary files, they may be vulnerable. But modern versions of programming languages usually provide more secure functions for the creation of temporary files. Although TOCTOU flaws exist because the program is not checking that a file already exist and because files are created with insecure ACLs, they can easily be prevented by using the secure variant of function calls. The opening of files is such a common low level task that it really should not be the programmer's responsibility to make sure it is handled securely.

3.5 Design versus configuration

One known design principle is fail-safe defaults[45]. This means that the system should have secure default values for its configuration. To follow this principle, programs should be designed to have a secure default configuration even if no options are configured in its configuration mechanism (file, registry). A configuration error would then be that the program is being deployed with configuration options enabled that make the program insecure.

But what if the program does not have fail-safe defaults built in, but still has safe configuration settings in the default configuration deployed? The program will still be in secure state, but can also be said to have a security related design flaw.

One class of flaws is when a system is having a known default password when it is installed. Such password are often not changed. It is the designer's responsibility to design the system to be secure by default. In this situation one can argue that the designer should make sure the program checks that the password is changed the first time it is run, thus making it a design flaw. But this type of flaws are more naturally considered to be a configuration flaw. The installation routine, not the application itself should force the user to set a password during installation.

Web applications are sometimes deployed without its own access control mechanisms. Since they are running on a web server, they can be protected by configuring the web server to do the access control. But the web server is not a part of the applications design. So even though it can be protected by changing the configuration, this is considered a design flaw in the web application running on the web server.

Programs having more rights than necessary

SUID and SGUID programs in Unix like operating systems allow a program to run with other privileges than the user running the program. Other operating systems also have similar mechanisms. This mechanism is often used if the program needs access to resources ordinary users usually don't have access to, like a special device. One problem with such programs is when it also access other restricted resources that the user running the program shall not have access to.

It is not always easy deciding from the descriptions if this kind of flaw is in the design, implementation or configuration. If it is no real reason for the program to run with other rights than the user running the program, then it is most reasonable to classify the flaw as a configuration flaw. If there is a reason for running with other rights than the user running the program, then a evaluation of whether it is a design or implementation flaw must be done. Examples of what we consider implementation flaws in SUID like programs are using the system() call instead of program code, relying on relational file paths. Trusting other components in such programs, is an example of a design flaw in SUID like programs.

4 Vulnerability databases

This chapter describes:

1. Vulnerability and advisory databases in general
2. Our criteria for selecting the ones to work with
3. How we extract data and eliminate duplicates.

4.1 Databases, Advisories and alerts

Vulnerability databases are collections of past vulnerabilities. Two types of vulnerability collections seems to exist: *general vulnerability databases* and *product specific databases*. The product specific vulnerability databases are collections of vulnerabilities a given security product are able to recognize or prevent. They are included with products like intrusion detection systems, firewalls, or vulnerability assessment tools. Normally they are not searchable, but some products include search options within the application itself or as a separate program or webpage.

The general vulnerability databases are stand-alone collections of vulnerabilities. These can also be found in different forms. *Advisories* and *alerts* are often smaller specialized collections. They can be collections of vulnerabilities specific for a particular program, which can be as small as less than 10 entries, or for a particular operating system distribution. Some collections include only vulnerabilities with a high risk or that have shown to or have the potential to be very widespread. One last type of database is the one we generally refer to when talking about vulnerability databases. They are larger collections of vulnerabilities for many programs and operating systems, often with some kind of classification. Many of them have more than 10,000 entries, and grow each day.

4.2 Evaluation and selection of databases

A few criteria was set to help decide which databases to use:

- CVE compatible
- Freely available
- Downloadable
- Language used must be English.

CVE compatibility is necessary to make sure a vulnerability is not classified multiple times if using multiple databases as sources, and to evaluate how a distinct vulnerability is classified in different databases. The database must be available free of charge. Some vulnerability databases are only available for a fee. The database must be downloadable in a format that can be worked with offline. By downloadable we mean that it must be available in some form of archive format (tar, zip etc.). Just being searchable on the web does not make it downloadable, even if a script could be made to search through

all possibilities of their numbering scheme. It would be possible, but would take too much time to create a parser for each web site and putting too much load on the web server. Many vulnerabilities are listed in several databases. Being able to work offline and integrate a public database with our own database can help save time by not having to manually examine vulnerabilities in one database that are already examined in another. Some of the vulnerability collections exist only in German, French, Spanish or other languages not easily understood by the author.

A short list of vulnerability databases can be found in [30]. CVE compatibility is a requirement, and an examination of the CVE web site revealed a more extensive list of organizations with CVE compatible products and services[1] On 2006-01-16 this list contained 144 organizations with CVE compatible services and products. Most of these organizations does not run a vulnerability database, but have products like vulnerability scanners. But a few more databases where located in addition to the databases already found in [30]. The freely available databases with English descriptions are listed in table 7. Content indicates the number of vulnerabilities registered in the database. These numbers are collected from January and February 2006, and they are increasing each day. National Vulnerability Database contains 19,566 CVE Vulnerabilities on 2006-09-25. Some of the databases do not provide a number on their web site, but it was possible to search the database for all entries and make an approximation based on the number of vulnerabilities returned on a web page and the number of links to web pages returned.

Name and URL	**Content**	**Downloadable**
Computer Associates Vulnerability Encyclopedia http://www3.ca.com/securityadvisor/vulninfo/browse.aspx	9979	No
Dragonsoft vulnerability database http://vdb.dragonsoft.com/	2242	No
ISS X-Force http://xforce.iss.net/xforce/search.php	21000	No
National Vulnerability Database http://nvd.nist.gov/	15494	Yes
Open source vulnerability database http://www.osvdb.org/	10767	Yes
Public Cooperative vulnerability database https://cirdb.cerias.purdue.edu/coopvdb/public/	10573	No
Secunia Advisories http://secunia.com/advisories/	11300	No
Security Focus http://www.securityfocus.com/vulnerabilities/	15570	No
Security Tracker http://www.securitytracker.com/	10000	No
US-CERT vulnerability notes database http://www.kb.cert.org/vuls/	1591	No

Table 7: Vulnerability databases

As we see from table 7, only two vulnerability databases conforming to the criteria are available for download, the National Vulnerability Database and the Open Source Vulnerability Database. It should be noted that although they both include CVE information for their vulnerabilities, neither of them have received their official certificate of CVE compatibility yet.

[1] http://www.cve.mitre.org/compatible/ (Visited 2006-01-16)

4.2.1 National Vulnerability Database

National Vulnerability Database (NVD) is closely related to CVE. Their FAQ states that NVD is CVE with extra analysis, a database and search engine. Updates to CVE will immediately appear in NVD. NVD integrates all publicly available U.S. Government vulnerability resources. In addition to CVE, this includes US-CERT alerts, US-CERT vulnerability notes, and OVAL queries. This makes it a very comprehensive database. US-CERT alerts are vulnerabilities with a certain severity threshold affecting a large number of installations. Severe vulnerabilities in less used applications are published in US-CERT vulnerability notes. Vulnerability notes often contain less information than alerts. OVAL is the Open Vulnerability and Assessment Language. It is a language used to describe and define tests in terms of component versions, configuration settings or other system characteristics to determine if a certain vulnerability is present in a system.

NVD is available for download in XML format. An example XML parser for NVD written in PHP is provided on the NVD web site.

Vulnerabilities can be classified using three dimensions:

Related Exploit Range: Remotely exploitable, Locally exploitable, Victim must access attacker's resource

Impact Type: Allows disruption of service, Allows unauthorized disclosure of information, Allows unauthorized modification, Provides unauthorized access (provides administrator access) or (provides user account access)

Vulnerability Type: input validation error (boundary condition error) or (buffer overflow), access validation error, exceptional condition error, environmental error, configuration error, race condition, design error, other error

Some simple statistics can be returned based on how NVD has classified the vulnerabilities. One can also search for vulnerabilities using most of the description fields available.

4.2.2 Open Source Vulnerability Database

Open Source Vulnerability Database (OSVDB) is a free, unbiased, and vendor neutral vulnerability database. It is run by volunteer security specialists. Vulnerabilities are entered into the database from different mailinglist. When first entered into the database, a vulnerability is not available to public. It must be reviewed and accepted by a moderator before being tagged as stable. Only stable entries are available on the web site or for download. OSVDB is available for download in XML format, but tools are provided to import the XML into a working MySQL and PostgreSQL database.

Vulnerabilities are classified using three dimensions:

Location: Console/Physical, Shell/Local, Network/Remote, Telephony, Unknown.

Attack type: Authentication Management, Cryptographic, Denial Of Service, Hijacking, Information Disclosure, Infrastructure, Input Manipulation, Misconfiguration, Race Condition, Other, Unknown.

Impact: Loss of confidentiality, Loss of integrity, Loss of availability.

10,767 entries was stable and available for the public. About the same amount is registered, but not reviewed yet. If a vulnerability is found in multiple applications, then it will have multiple entries in OSVDB. This can be a reason for the high number of vulnerabilities. Of the stable entries, only 5,303 entries do have a CVE entry.

4.3 Method for data collection

National Vulnerability Database was chosen as the first database to start with. The main reason for this is that it has the most complete CVE integration. All entries do have CVE numbers since NVD can be viewed as an vulnerability database implementation of CVE.

A copy of NVD was downloaded in February 2006. The format of the download was in XML as previously mentioned. A small Python program was written to parse the XML and extract the information needed, and insert it into a local database running MySQL. This copy of NVD includes 15,491 CVE entries. This is a huge number of vulnerabilities to examine, and the majority are probably not design flaws. To reduce the number of vulnerabilities needed to examine, some obvious candidates of vulnerabilities not being design flaws, could easily be excluded from our examination. The following keywords were used to locate and mark the vulnerabilities not interesting for this thesis:

- xss
- cross-site
- sql injection
- buffer overflow
- heap overflow
- format string
- sanit
- symlink
- input validat

Vulnerabilities with descriptions containing one of these keywords and also classified in NVD as a design flaw, were not marked. This marked 5,426 vulnerabilities, and leaves just more than 10,000 other possible candidates. More vulnerabilities could probably be excluded using more keywords, but inconsistent vulnerability descriptions in CVE would increase the risk of excluding some design flaws we are interested in. The chosen keywords have a low risk of being used in descriptions of design flaws. There still is a possibility that xss, cross-site, sanit[ize], or input validat[ion] are used to describe design flaws, but in most cases they are implementation issues.

CVE has a classification for vulnerabilities, and one of the categories is design. 3283 vulnerabilities are classified as design errors in NVD. Some random samples from this category showed that what is classified as a design flaw in NVD, is not always a design flaw according to the definition presented earlier. Some of them are clearly mis-classified, some are in the grey area between design and implementation, and some are classified as a design flaw and also in one or several other categories. This indicates that it is not

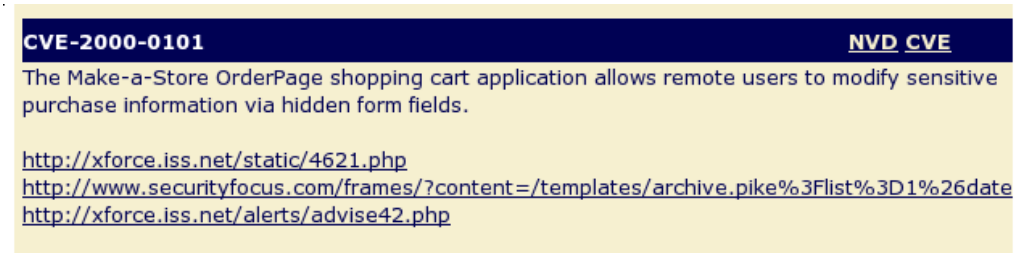

Figure 2: A vulnerability from the web page created to study the vulnerabilities

enough to just examine only the design class of vulnerabilities in the database, but design flaws can also be found in the other classes.

Another program was created to select vulnerabilities from the NVD database. Depending on the arguments given, this program would select a given number of vulnerabilities from a given category, and wrote two files. A plain text file and a web page. The text file contains two lines per vulnerability. Both lines starting with the CVE number. The first line contains in addition the letter *n* and a colon. This line is for writing notes about the vulnerability. The letter is changed to indicate what kind of vulnerability it is, and notes or comments on the vulnerability are written after the colon. The letters used are:

n: Not examined

d: Identifies a design flaw

m: Maybe a design flaw, but can be of another type too

o: Other type than design

u: Unknown. The descriptions does not contain enough information to decide what type of flaw it is

The second line contains the description of the flaw. An example line from a text file looks like this:

```
CVE-2000-0101 d: using client supplied data instead of server based data. Calculation
with untrusted data
CVE-2000-0101 Desc: The Make-a-Store OrderPage shopping cart application allows
remote users to modify sensitive purchase information via hidden form fields.
```

The web page also shows the CVE number and its text description. But it also contains clickable hypertext links to other references of the vulnerability. These references sometimes provides more information about the flaw, and they had to be consulted for most of the flaws. Links to the original NVD and CVE information page for the vulnerabilities are also available on this web page. See figure 2 for an example of how a vulnerability is presented on the web page. We borrowed the style sheet from the original NVD site to get the same look.

5 Developing a design flaw classification scheme

5.1 Design elements from existing classifications and related work

Many of the existing classifications and taxonomies are developed for a special purpose or to solve a specific research problem. How design flaws are handled in the different classifications can therefore vary depending of the intended usage of the classification. Some don't care about design flaws at all, some acknowledge design flaws, and some have classes that are design flaws but the classes are named according to the flaws nature. Table 8 lists the goals and motivation of some of the earlier mentioned classifications and taxonomies.

Author	*Year*	*Goal or Motivation*
Abbot [1]	1976	Provide an understanding of security problems in operating systems
Bisbey II [4]	1978	To get a better understanding of operating system vulnerabilities and identifying techniques for automatic identification of such vulnerabilities
Landwehr [29]	1994	A Taxonomy of computer program security flaws, with examples
Aslam [2]	1996	Security faults in the Unix operating system
Lindqvist [33]	1997	Intrusion techniques from the viewpoint of the system owner
Du & Mathur [12]	1998	Development of tools to detect security related software errors. Measuring effectiveness of methods for finding security related software errors
Krsul [28]	1998	Assumptions about the environment that do not hold under execution of the program.
Piessens [40]	2002	A structured taxonomy of the most frequently flaws. Usefull for learning material, checklist and avoiding common pitfalls software
Jiwnani [26]	2002	Better understanding of distribution of flaws to know where to consentrate testing efforts
Langweg [30]	2004	Flaws in application software. Help adapt testing strategies and development of robustness metrics
Weber [52]	2005	Help in the development of code analysis tools.
Tsipenyuk [50]	2005	Help developers and security practitioners to understand common errors. Can be used in a tool

Table 8: Motivation and goal of the classifications

Classes from the earlier classifications are often broad, with high abstraction level. They do not differentiate if the flaw is a design flaw or implementation flaw.

Landwehr et al [29] introduced dimensions. Their taxonomy uses three dimensions: genesis, time of introduction and location (See page 10). Time of introduction is used to classify a flaw according to when it was introduced into the system. Design flaws can be represented with the During development|Requirement/Specification/Design category of this dimension. The Genesis dimension is based on categories from [4] and [1]. Landwehr et al include examples on how they classified a number of vulnerabilities. In the examples flaws classified as During development|Requirement/Specification/Design in the time of introduction dimension are classified in all genesis categories except the in-

tentional|malicious category and the intentional|nonmalicious|covert channel category. One reason for this is that the categories are of a high level of abstraction, enabling both design errors and implementation errors to be classified in the same category.

Other classifications, like Du's [12] and Langweg's [30], do not have a dimension for when the vulnerability was introduced. Instead they use a dimension called *cause* with similar categories as those found in Landwehr et al's Genesis dimension and those found in [4, 1]. And to be able to classify design flaws, *Weak or incorrect design error* is added as a category to the *cause* dimension.

The newer and more detailed classifications

Some of the newer classifications proposed have classes with more detailed low level classes. In Seven Pernicious Kingdoms [50] the kingdom called *Security Features* seems to contain many classes of design flaws. They are:

- Insecure Randomness
- Least Privilege Violation
- Missing Access Control
- Password Management
- Password Management: Empty Password in Config File
- Password Management: Hard-Coded Password
- Password Management: Password in Config File
- Password Management: Weak Cryptography
- Privacy Violation

But also in the other kingdoms, mixed in between implementation flaws, one can find some phyla that can be attributed to insecure design. For example the *Time and State* kingdom contains the *Failure to Begin a New Session upon Authentication* phylum, and the *Encapsulation* kingdom contains the phyla *System Information Leak* and *Trust Boundary Violation*.

5.2 Design properties found in vulnerabilities from the databases

We started by using National Vulnerability Database (NVD). As mentioned in chapter 4.3, design flaws according to our definition of a design flaw are classified in different categories in NVD. To make sure we sample as many design flaws as possible, we wanted to take random samples from all categories. 100 samples from each category were randomly chosen. But a small bug in the program selecting the samples sometimes picked the same flaw more than one time, so the real number of individual flaws selected was a few less than hundred. Time permitted us to only examine flaws from 7 of the 9 categories. The two categories we did not get samples from are "race conditions" and "other". It is possible that not being able to include these two categories into our samples could influence the statistics to some degree. But after a quick look at the "race conditions" category, it looks like many of them are variants of symlink attacks, which we do not consider a design flaw. The "Other" category seems to include everything from input validation and cross site scripting problems to buffer overflows. So this probably does not influence the statistics on design flaws too much.

Many of the design flaws identified seems to be closely related to access control mechanisms. One such group of flaws is problems with how credentials are stored in the application. They can be stored in plaintext and easily obtainable by less privileged users of the application (CVE-) or they are embeded in the application and can not be changed by the user or operator (CVE-2004-1474). In other cases applications contained secret credentials (CVE-1999-0254). Once they are discovered they are not secret anymore.

One particular group of design flaws seen several time in the vulnerability database is applications which for some reason are designed to run with other privileges than the user running the application, often root privileges on Unix systems. Many of these flaws seem to not take into account the fact that they are running with other privileges. This means trouble if the program writes to a file the user can specify himself, and it does not check that the user does in fact have the privilege to write to that file (CVE-2000-0195).

The often quoted design flaw category "weak encryption" was not seen in many variations in the samples examined. Using electronic code book (ECB) mode and insecure use of the initialization vector (IV) in symmetric encryption was observed.

Design flaws not directly related to a security mechanism was also found in the examined samples. Examples include servers for handling electronic ordering of goods using prices sent by the client to calculate the total for the client to pay, clients sending a small amount of data to a server needing to do a lot of calculation or responding with large amount of network traffic, programs allowing a user or client to use all available resources, or programs leaking information by giving different answers to requests depending on the existens of a requested

Some of the more obscure design flaws observed include CVE-2000-0946 in which a program for locking the screen does not disable all the keys on the keyboard. Some custom keys can still be used to launch programs on the computer even if the screen is locked.

5.3 The proposed classification

5.3.1 Description

This classification consist of five top-level categories: Access control, Execution with other privileges, Encryption, Processing, and Miscellaneous.

Access control

The access control category is divided into two sub-categories: authentication and authorization.

Authentication

Authentication is about verifying the claimed identity of the communicating peer. Not only persons can be authenticated. Also programs, systems and even program components wanting to use your resources could, and should be authenticated. Flaws in the authentication class are weaknesses directly related to the authentication mechanism and the handling of authentication credentials.

- Missing: The program is not doing authentication although it really should do it.
- Insufficient state/algorithm: The program is doing authentication, but it is not doing it right. Some unwanted state in the authentication logic makes it possible to bypass

Access control	Authentication	Missing
		Insufficient
		Static credentials
		Plaintext credentials
		Weak obfuscation/encryption of credentials
		Backdoor
		Account lockout
	Authorization	Missing
		Insufficient
		Insecure permissions
		Hook to execute programs or code
		Action without user confirmation
Execution with other privileges	Missing access check	
	Insufficient access check	
	Trusting other component	
Encryption	Missing	
	Using ECB mode	
	Weak IV usage	
	No replay protection	
	Other weakness	
Processing	Validation	
	Incorrect execution order	
	Using untrusted data	
	Resource amplification	
	Unlimited resource usage	
	Insufficient cleanup	
	Information leak	
Miscellaneous		

Table 9: A classification of design flaws

the authentication. A typical example of this kind of flaw is web applications not checking if the client supplied user name is the one actually authenticated.

- Insufficient: The authentication credential is not secret, but is hardcoded into the application
- Static credentials
- Plaintext credentials: The authentication credential is not stored in a secure manner. It is available for every one to see, if they have access to the storage area. It is also possible to change it.
- Weak obfuscation/encryption of password: The designer have been aware of the risk of plain text storage of credentials, and he has attempted to make the password unreadable for users with access to the storage area. But if he does not use cryptographically secure methods to protect the password, it the provided method can often easily be broken and the original plain text password can easily be derived. Examples includes using BASE64, XOR, Caesar cipher.
- Backdoor: A backdoor is a designed secret way for service personell to access the application. It is often hardcoded. Thus it is similar to the static credentials category.

- Account lockout: This last authentication verification class is about problems with account lockout because of too many login failures. Some systems allow only one concurrent session and lockout time is not configurable (CVE-2001-0564), making it an easy target for denial of service attacks.

Authorization
Authorization problems are for flaws concerning what a user or program can do to or with resources.

- Missing: If no authorization check exist for the functionality, even though it should, then the flaw belongs in this category.
- Insufficient: Authorization checks exist, but the logic in them are flawed in such a way that it is possible to bypass or trick the check somehow. Authorization mechanisms not protecting all access paths or not protecting all data elements will be classified in this category. The same if the authorization functionality allows access to certain data elements, but it also allows access to data that should not be available through this functionality.
- Insecure permissions: New objects created are sometimes created with weak default access rights. The objects can be files, directories, registry entries and so on.
- Hook to execute programs or code: Some programs provide a way for the user to execute external programs.
- Action without user confirmation: Sometimes programs can be tricked into executing dangerous functions that can have fatal consequences. If the program does this without first warning the user, the flaw belongs to this class. This could be described as a reverse authorization since it is not the program that should control the access, but the user should authorize the action the program wants to take.

It is not always easy to decide if a flaw is a problem with authentication or authorization. They could be combined to one class called *access control*, but then we would loose some information about the flaw that are important when evaluating a design. Authentication and authorization are two distinct functions, and should therefore be two separate classes. Three combinations of authenticate and authorize are possible.

1. Some programs do not need to do authentication. They consider any user as authenticated, but limit, or should limit access to resources through white-lists or black-lists of resources the user can or can not access (no authentication - do authorization).
2. Other programs want to know who is doing what, but do not need to limit access to resources (do authentication - no authorization).
3. When a program supports multiple users, you want to know who the user are and limit access to resources depending on what the user are allowed to access (do authentication - do authorization).

Of course there is the fourth combination of no authentication - no authorization. But if there is no need for neither authentication nor authorization in a program, no flaw can

be classified as belonging to one of these two classes.

Execution with other privileges

When an application is running with higher or other privileges than the user running the application, the ordinary authentication mechanism is bypassed, or prevented from working. This is typical for Unix programs running with SUID root and accessing or executing other system resources without either first dropping the privileges or checking that the real user ID is allowed to access or execute the resource.

- Missing access check: The program does not have functionality to check the user's authority to do what he wants.
- Insufficient access check: There exist functionality to make sure the user is only doing what he is allowed to do, but this functionality is flawed.
- Trusting other component: The program is executing other components, and trust them to execute in a safe maner. But they include functionality that breaks this trust.

Encryption

- Missing: No encryption is done to protect data.
- Using ECB mode: ECB mode is used on a symmetric cipher. The effect is that if a block of plaintext appear in two different places in the message, these two blocks produce the same ciphertext.
- Weak IV usage: For best protection, the initialization vector should be kept secret. It should not be possible to guess which IV to use next.
- No replay protection: It is possible to capture communication and replay it to the peer to get access.
- Other weakness:

Processing

- Validation: This is a broad category. It includes flaws in which the program does not properly check the value of a variable and takes action based on that value. The problem can be because of values that are out of range, values that should not exist in the current program state, values that are inconsistent, etc.
- Incorrect execution order: The program is not executing code in the order it should do.
- Using untrusted data: Data a server gets from a client should not be trusted. Security functionality should not be done by the client. The server should not use data it gets from a client if that data is available to the server itself, even if the server sent the data to the client in the first place as part of the communication. The client can send back modified data. (For example CVE-2000-0101)
- Resource amplification: If the client can send only a few bytes and have the server respond with a large number of bytes or network traffic, or doing a lot of calculation, then we have what can be called resource amplification.

- Unlimited resource usage:
  Unlimited resource usage is when the program does not have any ways to limit the resources. It allows the user to grab them all, often resulting in denial of service for other users.
- Insufficient cleanup: This category is to be used if the program is not cleaning up properly by deleting all temporary resources used and leaving files or data available for others to see.
- Information leak: Sometimes programs gives attacker more information than they need. This can be given directly as a response to a query, or it can be indirectly by giving different responses depending on the existence of a queried object. A client connecting from the network should normally not be told the full path to the location of files if the server is unable to find them, or the name of internal databases.

Miscellaneous

The last category is the **miscellaneous** class. This is a category for flaws that clearly are design flaws, but they do not fit into the other classes. This can be because it is a flaw not discovered in our initial set of flaws from which the classification was derived, or the flaw was only seen once and seems so special that it does not justify its own category. It can be discussed if a miscellaneous category should be in a classification system. For design flaws we feel it is acceptable to have a category to catch vulnerabilities not fitting the other categories. There are many variants of design flaws, and you will find new ones not fitting any of the categories.

5.3.2 Selection criteria when using the classification

It turned out to be very hard to find unambiguous categories for design flaws. Without unambiguous categories, one has to rely on a classification decision tree to classify a flaw in the same category each time.

First of all one has to decide if the flaw is a design flaw or another type of flaw. We must ask ourself:

- Is this a flaw that exists in all implementations of the program's design? Will a implementation using another programming language also have the flaw? Will the flaw exist if another programmer makes an implementation based on the design?

While working with the flaw descriptions, it became apparent that four possible answers can come out of this question:

1. **Yes:** It is no doubt that this is a design flaw.
2. **Possibly:** It is possible that the flaw is introduced in the design, but it is also possible to be a mistake the programmer made.
3. **No:** It is not a design flaw
4. **Unknown:** The description does not contain enough information to decide what type of flaw it is

Figure 3 shows this question and the answers in a decision tree.

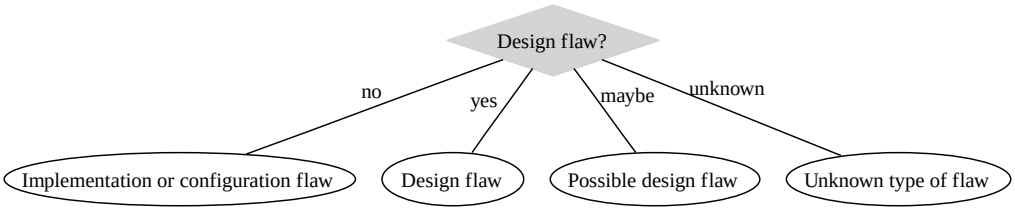

Figure 3: Decision tree to decide if the flaw is a design flaw

If the answer is “yes” or “possibly”, then we can proceed to find out what type of design flaw it is by using the classification decision tree in figure 4. If the answer is “no” or “unknown”, then the flaw is not of much interest for this study.

If the flaw is a design flaw or possibly is a design flaw, the next step is to find out what type of design flaw it is. This process can be in multiple steps if a category has several sub-categories. The decision tree to these questions can be seen in figure 4. The questions (Qx) are:

- Q1: Does the flaw exist because the program is running with other privileges than the user executing it?
- Q2: Is it a problem with the design of an authentication mechanism or authorization mechanism, with the exception of cryptographic mechanisms to protect the transfer of authentication credentials?
- Q2.1: Is it a weakness in the way an authentication credential is stored? Should the program authenticate users or differentiate between classes of users but does not try to authenticate or it is possible to bypass the authentication mechanism?
- Q3: Is it a problem with the design of a cryptographic mechanism used to protect user data while it is stored or transferred?
- Q4: Is it a problem with how data are processed?

If the answer to a question is yes, but we don’t find a properly category to classify the flaw, we go to the next category to see if it fits there. If neither of the existing categories fit, we end up in the Miscellaneous category. The only exception is from the first category, execution with other privileges, where we go directly to the miscellaneous category.

5.4 Other possible approaches

It turned out to be quite hard to find an way to make an unambiguous classification of design flaws. We did not succeed in this and had to settle for an approach that are practical, but sometimes it is possible for a flaw to be classified in two different categories.

The classification is partly inspired by and using elements from [25] and the Common Criteria [10].

A few alternative approaches where tried in the development of our taxonomy. One way to look at a taxonomy could be to use the elements of the design process as top level nodes in a hierarchical taxonomy. From the definitions of design terms, we identified

- Components

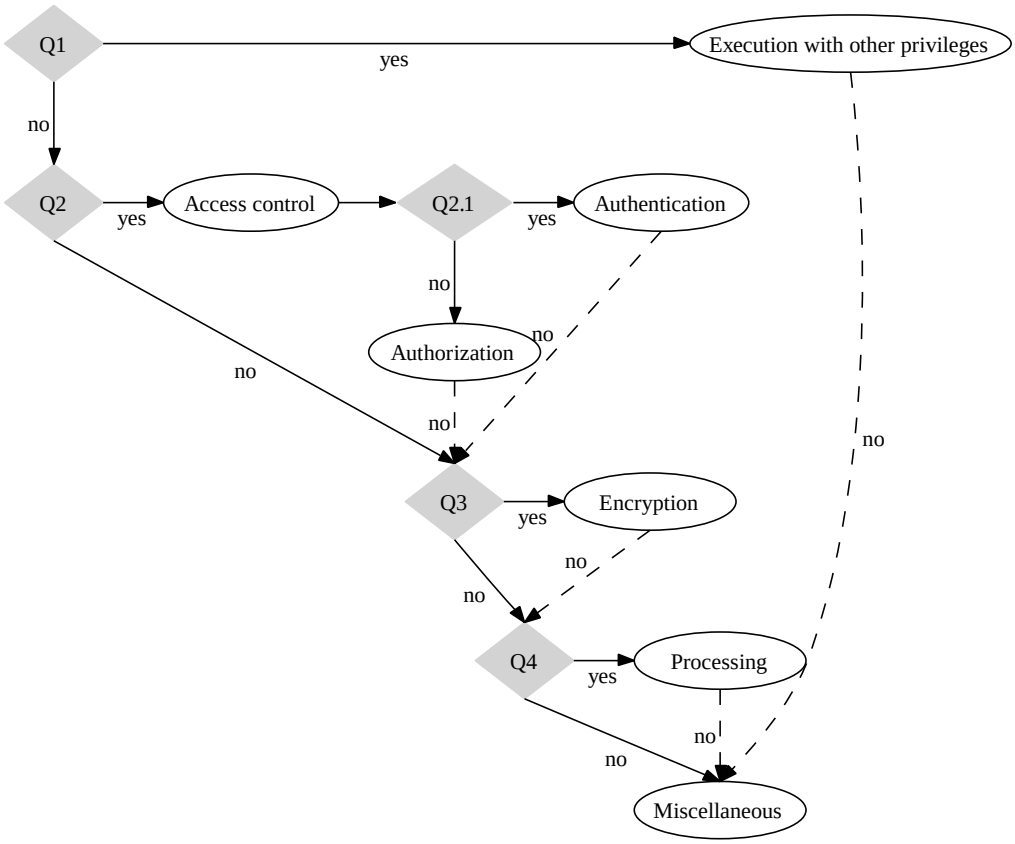

Figure 4: Decision tree to decide the type of design flaw

- Interfaces
- Algorithms
- Data structures

as possible top level candidates. Components can easily be excluded as a candidate, since all components also include interfaces, algorithms and data structures. The three remaining seems to depend on each other in order to produce an exploitable flaw. A simple interface or a simple data structure can in most cases not contain a security flaw by themself. More complex interfaces or complex datastructures includes themselves algorithms to function properly. It's the algorithm using the interface or data structure which mostly contains the vulnerability. A datastructure is also often passed through an interface to be processed by an algorithm. Although Basili and Perricone tried to classify errors (not security flaws) with a similar classification scheme [3], they also noted that it was not sure another classifier would use the same categories for the same flaws as they had used. But if we had more time, we would have revisited this approach and at least used more elements from the description of design documents found in [23]

Another approach is to use design principles [45, 51, 16] to build a taxonomy. The design principles are very broad and they overlap. One flaw very often violates several of these principles, failing to be unambiguous. They would therefore probably not make a very good taxonomy. But design principles can still be usable for data collection on flaws even if we look at a flaw as violations of several principles. One can for example look at the unique combinations of violated principles as one unique class.

6 Applying the classification

This chapter describes:

1. Results from using the developed classification by applying it to vulnerabilities
2. Actual statistics found by using the classifications to try to answer if there are any typical design error vulnerabilities

6.1 Data source and method

To test the classification and find the answer to our third research question, “what are the most typical design flaws?”, vulnerabilities from the National Vulnerability Database were used, just as for the other research questions. The intention was to:

1. Find a large enough number of vulnerabilities caused by design flaws
2. Examine this first set of vulnerabilities to discover their properties and develop a classification scheme.
3. Classify this first set of vulnerabilities using the developed classification and make the needed justifications, if any, to the classification scheme.
4. Find more vulnerabilities and classify them

Finding and examining the first set of vulnerabilities and the process of creating the classification scheme was a process that took much more time than anticipated. In the beginning of the process it was not easy to decide if it was a design problem or other type of problem, and a lot of time was used to study the references of each vulnerability. The process of creating the classification took a while because it was very difficult to find unambiguous categories. For each try, it did not take long time to discover a new vulnerability that could be classified into more than one category. A practical but not perfect classification was chosen when it was not more time to spend on creating the classification.

Spending too much time on examining vulnerabilities and creating the classification, it was not enough time to find even more vulnerabilities to have a larger number of design flaws to classify and to test the classification on a set of vulnerabilities not used to create the classification scheme. This means that there are some weaknesses in the method:

1. The number of vulnerabilities is not large enough
2. The sampling is probably not as random as it should be.
3. The classification is not tested sufficiently on diverse data
4. It is possible to classify some vulnerabilities in several categories, but the classification tree takes care of some of those ambiguities

But despite of this, some trends in the distribution of vulnerabilities across the categories are emerging, and some experience was gained by classifying the initial set of

vulnerabilities.

6.2 Experience gained from using the classification

Some of the vulnerabilities are quite hard to decide if they are design flaws or other types of flaws. For example programs executing with other rights than the person executing the program. Some of those programs need those rights to do what they are supposed to. If these programs don't take those special rights into consideration, it is a design flaw. But some programs don't need those rights at all, they are only distributed with them. These flaws are harder to classify. If a program is distributed to run as root on one Linux distribution, but is not distributed like this on any other distribution, Then it is probably more right to consider it a configuration flaw than a design flaw. But it is not easy to decide this without looking at how the program is distributed in other distributions or how it is distributed from the developer's. Some programs, like DOSemu, are designed to be run both as root or the user running the program depending on the functionality you want.

One type of access control problems not easy to classify, is web programs in which it is possible to bypass the authentication by directly accessing a sub-program. These applications typically have a front end program taking care of authentication and authorization. If the authenticated user is authorized to do what he tries to do, the front end program calls program B. The problem here is that it is possible to call program B directly with the necessary parameters without going through the access control mechanism in the front end program. It is obvious that the program does not check if the user is authorized to access its functionality, but it does neither check who the user is. Our classification separates problems with authentication and authorization. But such flaws are clearly a problem with both authentication and authorization, because it is possible to misuse the application without being authenticated or without being authorized. One way to look at this type of flaws is to consider the authorization mechanism. To authorize a user, it needs to know who the user is. The authorization mechanism should first check who the user is, and then decide what to do. If the user is not authorized, which he is not when he is not authenticated and unknown, access should be denied. The authorization mechanism is failing to do its job in this case. But it is also possible to look at this problem as a authentication problem. It is after all possible to use the program without authenticating, which should not be possible.

6.3 Results from applying the classification

134 design flaws were classified using the scheme presentend in this report. If we look at the top level categories only, one category stands out from the rest. Table 10 lists the categories aggregated at the top level category. Problems with the design of access control mechanisms seems to be responsible for more than half of the vulnerabilities caused by design flaws. General processing flaws not directly related to a security mechanism are responsible for one fourth of the problems. These two categories are responsible for 79 percent of the vulnerabilities examined. It is a little bit surprising that so few problems with encryption mechanisms was found. Weak encryption is very often used as an example of a typical design flaw in most of the literature talking about design flaws. There can be several possible reasons for this:

- More applications have some form of access control mechanisms than encryption mechanisms. This means that problems can be found more often in control mechanisms because of their numbers.
- If encryption is needed, standard libraries developed by cryptographers can be used. As mentioned earlier, security is often considered at the end of the development process. It can be more convenient to wrap communications in a SSL tunnel using stunnel or use OpenSSL to take care of the cryptographic need than to implement its own encryption tools. Sometimes this is the right approach anyway.
- Encryption protocols are maybe not attacked so often that flaws are found. Most times there are easier ways to attack an application than breaking encryption algorithm. As long as other, easier ways to attack applications exist, an attacker will probably concentrate his effort on what gives the best access with the least use of resources.

Category	Count	Percent
Access control	72	53.7
Processing	34	25.4
Execution with other rights	12	9.0
Encryption	10	7.5
Miscellaneous	6	4.5

Table 10: The aggregated number of vulnerabilities for the top level categories

Table 11 lists the number of vulnerabilities found in each individual category of the classification. We see that four categories stands out as more frequent errors than others when we look at the individual categories:

- Access control:Authentication:Insufficient
- Processing:Validation
- Access control:Authorization:Insufficient
- Access control:Authorization:Missing

These four categories amount for 46.2 percent of the vulnerabilities. Processing:Validation is the only category from Processing that stands out with significant more vulnerabilities than the other Processing categories. The other three categories are related to how authentication and authorization mechanisms are implemented.

Category	Count	Percent
Access control:Authentication:Insufficient	20	14.9
Processing:Validation	15	11.2
Access control:Authorization:Insufficient	14	10.4
Access control:Authorization:Missing	13	9.7
Access control:Authorization:Insecure permissions	7	5.2
Processing:Information leak	6	4.5
Miscellaneous	6	4.5
Execution with other privileges:Missing access check	6	4.5
Execution with other privileges:Trusting other component	5	3.7
Access control:Authorization:Action without user confirmation	5	3.7
Processing:Using untrusted data	4	3.0
Access control:Authentication:Static credentials	4	3.0
Processing:Insufficient cleanup	3	2.2
Processing:Incorrect execution order	3	2.2
Encryption:Other weakness	3	2.2
Encryption:Missing	3	2.2
Access control:Authentication:Plaintext credentials	3	2.2
Processing:Resource amplification	2	1.5
Encryption:No replay protection	2	1.5
Access control:Authorization:Hook to execute programs or code	2	1.5
Access control:Authentication:Backdoor	2	1.5
Access control:Authentication:Account lockout	2	1.5
Processing:Unlimited resource usage	1	0.7
Execution with other privileges:Insufficient access check	1	0.7
Encryption:Weak IV usage	1	0.7
Encryption:Using ECB mode	1	0.7

Table 11: The number of vulnerabilities found in each classification category

7 Discussions

- Hard to tell what kind of flaw we are dealing with
- Deciding if it is a design flaw is even harder
- Descriptions of unfamiliar technology
- Quality of data in the database
- Different classification for the same flaw in different databases

During this work, we discovered that classifying vulnerabilities is actually quite hard. Many research projects have done it in the past, and most of the conclusions are the same:

Several issues contribute to making this difficult:

- Some vulnerabilities can be a combination of several factors
- The technology is unfamiliar to the classifier
- The description of the flaw is insufficient
- The classification is not good enough

The vulnerabilities examined in this thesis are from a wide type of applications and operating systems. And one problem we noticed several times while examining the many vulnerabilities, is that not knowing the specific technology containing the flaw can sometimes make it hard to understand the vulnerability, and without understanding it, classifying the vulnerability in the right category is very hard, if not impossible. For example CVE-1999-1279: "*An interaction between the AS/400 shared folders feature and Microsoft SNA Server 3.0 and earlier allows users to view each other's folders when the users share the same Local APPC LU*". The author does not know anything about AS/400 and the belonging technology. The acronyms "APPC LU" was unknown, but "SNA" was heard of, but exactly what a SNA server does was unknown to the author. This vulnerability sounds like some kind of access control problem, but one can not be sure without a better understanding of what a "Local APPC LU" does and what the Microsoft SNA Server does.

Another example on unfamiliar technology is from the configuration of BEA Weblogic server. The flaw in question is CVE-2000-0684 in which it is possible to execute java code in arbitrary files. You need to understand the syntax of the configuration file to understand the vulnerability.

```
weblogic.httpd.register.*.jsp=weblogic.servlet.JSPServlet
```

The problem in this flaw is that a request for http://weblogic.site/*.jsp/path/to/temp.txt executes java code if embedded inside temp.txt, but it was only supposed to parse *.jsp files.

CVE-2005-0035 is an example of a flaw with insufficient description. The description is: “The Acrobat web control in Adobe Acrobat and Acrobat Reader 7.0 and earlier, when used with Internet Explorer, allows remote attackers to determine the existence of arbitrary files via the LoadFile ActiveX method”. We learn that it is a combination of Acrobat web control and Internet Explorer and the LoadFile function of ActiveX. But we do not get to learn exactly what goes wrong or why it goes wrong.

The CVE description for CVE-2000-0769 says: “O’Reilly WebSite Pro 2.3.7 installs the uploader.exe program with execute permissions for all users, which allows remote attackers to create and execute arbitrary files by directly calling uploader.exe.” From this description it can sound like a configuration error like it is classified in NVD or a design error where insecure permissions are used by default, or a program with a hook to execute code. But since this is a web application, uploader.exe is probably supposed to let users upload files. At least that is what it sounds like. There is no information on how uploader.exe is supposed to work or why it fails to work in a secure way. Looking at the other references for this vulnerability, X-Force ISS [1] says that uploader.exe allows users to upload files to the cgi-bin directory where they can be executed by the web server. Security Focus[2] says that cgi-bin directories are installed readable for any user and that uploader.exe allows a remote user to upload any file to the server. It is unclear what they mean by the server; the web server file tree?, anywhere else the user the web server is running as has write access to? anywhere on the file system? If it can write anywhere in the file system, does upload.exe run with higher privileges than necessary? Is upload.exe part of a system that is used to publish web pages on the server, so it is a necessary application to run? A post to the NT Bugtraq mailinglist reveals more information[3]. upload.exe is a demo application and it is not needed by the web server. The real problem with upload.exe is that it does not make any checks to make sure it only upload files to where it or the user is allowed to. It does not even seem to be configurable.

7.0.1 The need for more details in the vulnerability databases

The description of vulnerabilities used in CVE and the databases are often limited, and sometimes misleading. They therefore often does not reveal the real nature of the vulnerability. Vulnerability databases often have links to other databases, web sites, or postings on mailing lists providing more information on the vulnerabilities. But such external information can disappear without notice.

The corporate business are depending on software in toady’s world. If the software they depend on is flawed, businesses can lose money, and in worst case they can go bankrupt. Software is more and more important for the global economy. It is therefore important to have secure software. To build secure software, we must learn from other’s mistakes The best way to learn is to have detailed information on failures other people have made. Researchers and programmers would benefit from having more details available on the vulnerabilities in the databases. We therefore need more details on the vulnerabilities describing exactly what is wrong, the root cause of the vulnerability, and what was done to make the application secure again. Maybe software producers should be required to disclose the parts of the code enabling the flaw to be exploited?

[1] http://xforce.iss.net/xforce/xfdb/294
[2] http://www.securityfocus.com/bid/1611/discuss
[3] http://marc.theaimsgroup.com/?l=bugtraq&m=87602880019759&w=2

8 Conclusions and future work

This thesis has studied vulnerabilities caused by design flaws. We had three research questions we hoped to answers.

1. What properties do vulnerabilities caused by security related design flaws have? They are often described as flaws of higher abstraction level, but can also be more like low level programming errors. They exist independent of two different implementations, but it is not always possible to determine wether a flaw is an implementation flaw or a design flaw. They are often related to security functionality, but can also be found in general program logic.
2. What can a classification of security related design flaws look like? We have presented a classification developed based on the properties of design flaws found in the database. Creating a classification with unambiguous categories turned out to be very challenging, and we did not succeed with that. With the help of a classification tree, the classification can still be used to classify design flaws with properties from several categories.
3. What are the most typical design flaws? Using our classification on 134 design flaws, four types of flaws were registered more frequently than others: They are problems with insufficient authentication, insufficient authorization, missing authorization, and validation errors.

Future work

Since many vulnerabilities can have more than one characteristic and it can be difficult to classify such vulnerabilities into exact one category, it could be interesting to develop a classification consisting of many low level (possible taxonomic) characteristics, but let a flaw be able to belong to more than one of these characteristics. A category can then consist of more than one characteristic, and the number of categories would then be the number of possible combinations of these characteristics.

Bibliography

[1] R. Abbot, J. Chin, J. Donnelley, W. Konigsford, S Tokubo, and D. Webb. Security analysis and enhancements of computer operating systems. Technical Report NBSIR 76-1041, ICET, National Bureau of Standards, 1976.

[2] T. Aslam, I. Krsul, and E. H. Spafford. Use of a taxonomi of security faults. In *Proceedings of 19th National Information Systems Security Conference*, pages 551–560, 1996.

[3] Victor R. Basili and Barry T. Perricone. Software errors and complexity: an empirical investigation. *Communications of the ACM*, 27(1):42–52, 1984.

[4] R. BisbeyII and D. Hollingworth. Protection analysis: Final report. Technical Report ISI/SR-78-13, Information Sciences Institute, University of Southern California, 1978.

[5] M. Bishop and D. Bailey. A critical analysis of vulnerability taxonomies. *Technical Report CSE-96-11, Department of Computer Science, University of California at Davis*, 1996.

[6] B. Blakley, C. Heath, and members of The Open Group Security Forum. Security design patterns. Technical report, The Open Group, 2004.

[7] A. Braga, C. Rubira, and R. Dahab. Tropyc: A pattern language for cryptographic software. In *5th Pattern Languages of Programming (PLoP'98) Conference, 1998. Washington University Technical Report WUCS-98-25*, 1998.

[8] Ram Chillarege, Inderpal S. Bhandari, Jarir K. Chaar, Michael J. Halliday, Diane S. Moebus, Bonnie K. Ray, and Man-Yuen Wong. Orthogonal defect classification - a concept for in-process measurements. *IEEE Transactions on Software Engineering*, 18(11):943–956, 1992.

[9] The CLASP application security process. Secure Software Inc., 2005.

[10] Common criteria for information technology security evaluation, 2005. Version 2.3.

[11] R. DeMillo and A. Mathur. A grammar based fault classification scheme and its application to the classification of the errors of T E X. Technical Report SERC-TR-165-P, Software Engineering Research Center, Purdue University, W. Lafayette, IN 47907, USA, 1995.

[12] W. Du and A. P. Mathur. Categorization of software errors that led to security breaches. In *Proceedings of 21st National Information Systems Security Conference*, pages 392–407, 1998.

[13] W. A. Florac. Software quality measurement: A framework for counting problems and defects. Technical Report CMU/SEI-92-TR-22 ESC-TR-92-022, Carnegie Mellon University, Pittsburgh, Pennsylvania 15213, USA, 1992. The Quality Subgroup of the Software Metrics Definition Working Group and the Software Process Measurement Project Team.

[14] B. Freimut. Developing and using defect classification schemes. Technical Report 072.01/E, Fraunhofer IESE, 2001.

[15] John B. Goodenough and Susan L. Gerhart. Toward a theory of test data selection. In *Proceedings of the international conference on Reliable software*, pages 493–510, New York, NY, USA, 1975. ACM Press.

[16] M. G. Graff and K. r. van Wyk. *Secure Coding: Principles and Practices*. O'Reilly, 2003.

[17] D. Gustafson. *Software Engineering*. Schaums Outline. McGraw-Hill, 2002.

[18] K. S. Hoo, A. W. Sudbury, and A. R. Jaquith. Tangible roi through secure software engineering. *Secure Business Quarterly*, 2001.

[19] J. D. Howard and T. A. Longstaff. A common language for computer security incidents. Technical Report SAND98-8667, Sandia National Laboratories, 1998.

[20] IEEE-1074. IEEE standard for developing software life cycle processes, 1997.

[21] IEEE-12207-1-1997. IEEE/EIA software life cycle processes life cycle data, 1997.

[22] IEEE-610.12-1990. IEEE standard glossary of software engineering terminology, 1990.

[23] IEEE-1016-1998. IEEE recommended practice for software design descriptions, 1993.

[24] IEEE-1044-1993. IEEE standard classification for software anomalies, 1993.

[25] ITU/CCITT X.800. Security architecture for open systems interconnection for CCITT applications. International Telecommunication Union (ITU), The International Telegraph and Telephone Commitee (CCITT), 1991.

[26] K. Jiwnani and M. Zelkowitz. Maintaining software with a security perspektive. In *18th IEEE International Conference on Software Maintenance (ICSM'02)*, pages 194–203, 2002.

[27] D. M. Kienzle and M. C. Elder. Security patterns for web application development. Technical report, University of Virginia, 2002.

[28] I. W. Krsul. *Software Vulnerability Analysis*. PhD thesis, Purdue university, 1998.

[29] C. E. Landwehr, A. R. Bull, J. P. McDermott, and W. S. Choi. A taxonomy of computer program security flaws, with examples. *ACM Computing Surveys*, 26(3):211–254, 1994.

[30] H. Langweg and E. Snekkenes. A classification of malicious software attacks. In *Proceedings of 23rd IEEE International Performance, Computing, and Communications Conference*, pages 827–832, 2004.

[31] P. D. Leedy and J. E. Ormrond. *Practical research: planning and design*. Pearson Merril Prentice Hall, 2005.

[32] S. Lehtonen and J. Parssinen. A pattern language for cryptographic key management. Seventh European Conference on Pattern Languages of Programs (EuroPLoP 2002), 2002.

[33] U. Lindqvist and E. Jonsson. How to systematically classify computer security intrusions. In *Proceedings of 1997 IEEE Symposium on Security and Privacy*, pages 154–163, 1997.

[34] R. A. Martin, S. M. Christey, and J. Jarzombek. The case for common flaw enumeration. In *Proceedings of Workshop on Software Security Assurance Tools, Techniques, and Metrics*, number 500-265 in NIST Special Publication. National Institute of Standards & Technology, 2006.

[35] Steve McConnell. *Code complete: a practical handbook of software construction*. Microsoft Press, Redmond, WA, USA, 1993. Online Edition Books 24x7.

[36] G. Meszaros and J. Doble. A pattern language for pattern writing. http://hillside.net/patterns/writing/patterns.htm. (Visited July 2006).

[37] P. G. Neumann. Principled assuredly trustworthy composable architectures. Technical report, SRI International, 2004.

[38] *OECD Guidelines for the Security of Information Systems*. Organisation for Economic Co-operation and Development (OECD), 1996. ISBN: 9264145699.

[39] *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. Organisation for Economic Co-operation and Development (OECD), 2002. ISBN: 9264059172.

[40] F. Piessens. A taxonomy of causes of software vulnerabilities in internet software. In M. Vouk, editor, *Supplementary Proceedings of the 13th International Symposium on Software Reliability Engineering*, pages 47–52, 2002.

[41] PLOVER - the preliminary list of vulnerability examples for researchers. http://www.cve.mitre.org/docs/plover/plover.html. Work in progress. Last visited on 2006-06-18.

[42] R. S. Poore. Genereally accepted system security principles. Technical report, International Information Security Foundation, June 1999.

[43] R. Pressman. *Software Engineering: A Practitioner's Approach*. McGraw Hill, 3. edition, 1992.

[44] P. Runeson, C. Andersson, T. Thelin, A.Andrews, and T. Berling. What do we know about defect detection methods? *IEEE Software*, 23(3):82–90, 2006.

[45] J.H. Saltzer and M.D. Schroeder. The protection of information in computer systems. 63(9):1278–1308, 1975.

[46] SAMATE. A possible harmonizing software flaw taxonomy. http://samate.nist.gov/SSATTM_Content/ReadmeFiles/taxonomy.html. Work in progress. Last visited 2006-07-20.

[47] M. Schumacher. *Security Patterns - Integrating Security and Systems Engineering*. John Wiley and Sons Ltd, 2005.

[48] M. Schumacher and U. Roedig. Security engineering with patterns. In *8th Conference on Pattern Languages of Programs (PLoP 2001), Monticello, Illinois, USA, July 2001*, 2001.

[49] M. Swanson and B. Guttman. Generally accepted principles and practices for securing information technology systems. Technical Report 800-14, National Institute of Standards & Technology, September 1996.

[50] K. Tsipenyuk, B. Chess, and G. McGraw. Seven pernicious kingdoms: A taxonomy of software security errors. In *Samate Workshop on Software Security Assurance Tools, Techniques, and Metrics. November 7-8 2005, Long Beach, CA, USA*, pages 36–43, 2005.

[51] J. Viega and G. McGraw. *Building Secure Software: How to Avoid Security Problems the right Way*. Addison-Wesley, 2002.

[52] S. Weber, P. A. Karger, and A. Paradkar. A software flaw taxonomy: aiming tools at security. In *SESS '05: Proceedings of the 2005 workshop on Software engineering for secure systems–building trustworthy applications*, pages 1–7, New York, NY, USA, 2005. ACM Press.

A Vulnerability databases

Several properties of vulnerability databases where examined. They are described using the following fields in the tables in this chapter:

Name: The name of the vulnerability database.

URL: The Internet address where the vulnerability can be found

Content: The number of vulnerabilities in the database, its sources and other information on the content.

Classification: Whether the vulnerability database is using any kind of classification system and a description of the system that is used.

CVE: Whether the vulnerability database is using CVE.

Public: Whether the vulnerability is accessible to everybody free of charge.

Searchable: How it is possible to search the database.

Downloadable: Is it possible to download the database and install it on your own computer. If so, what format is it available in.

Active: Is it updated continuously with new vulnerabilities?

Other: Other interesting properties noticed about the database.

Name:	Computer Associates Vulnerability Encyclopedia
URL:	http://www3.ca.com/securityadvisor/vulninfo/browse.aspx
Content:	9979 vulnerabilities (2006-01-26)
Classification:	impact, root cause
CVE:	YES
Public:	YES
Searchable:	free text. Browsable by last 15 days or all (not sorted)
Downloadable:	NO
Active:	YES
Other:	Limited search and browsing.

Name:	Common Vulnerabilities and exposures
URL:	http://www.cve.mitre.org/
Content:	Total Unique Entries: 3052 (CVE Version Number: 20040901) Total Candidates: 12290 (2006-02-27) 76 sources, see http://www.cve.mitre.org/cve/refs/refkey.html for full list
Classification:	no
CVE:	YES, yes xml, cvs, text
Public:	YES
Searchable:	YES
Downloadable:	YES
Active:	YES
Other:	Aims to be a dictionary of vulnerabilities. Does not classify. The "Total Unique Entries" and "Total Candidates" don't add up to the number of entries in the downloaded file. "grep "Name: CVE" all-cves.txt | wc -l" gives 16088. 3052+12290=15342. The web page is probably not updated as often as the CVE-candidates file.

Name:	Dragonsoft vulnerability database
URL:	vdb.dragonsoft.com
Content:	2242 (2006-01-26)
Classification:	none
CVE:	YES
Public:	YES
Searchable:	free text, browsable by type of software.
Downloadable:	No
Active:	YES
Other:	

Name:	ISS X-Force
URL:	http://xforce.iss.net/xforce/search.php
Content:	More than 21000 (2006-01-26)
Classification:	Textual description, Consequences
CVE:	YES
Public:	YES
Searchable:	Free text
Downloadable:	NO
Active:	YES
Other:	Database not browsable. Advisories and alerts are.

Name:	National Vulnerability Database
URL:	http://nvd.nist.gov/
Content:	all publicly available U.S. Government vulnerability resources. 15494 CVE Vulnerabilities 50 US-CERT Alerts 1209 US-CERT Vuln Notes 1162 Oval Queries Last updated: 02/27/06
Classification:	Related Exploit Range: Remotely exploitable Locally exploitable Victim must access attacker's resource Impact Type: Allows disruption of service Allows unauthorized disclosure of information Allows unauthorized modification Provides unauthorized access (provides administrator access) (provides user account access) Vulnerability Type: input validation error (boundary condition error) (buffer overflow) access validation error exceptional condition error environmental error configuration error race condition design error other error
CVE:	YES
Public:	YES
Searchable:	Keyword, Vendor, product, version. Start date, End date, Vulnerability Severity, Related Exploit Range, Impact Type, Vulnerability Type. You can search for vulnerabilities that have: US-CERT Technical Alerts, US-CERT Vulnerability Notes, or OVAL Queries associated.
Downloadable:	YES, xml-format
Active:	YES
Other:	Provides some simple statistics on the vulnerabilities Extensive references to other sources of information for the vulnerabilities It is based on and synchronized with the CVE vulnerability naming standard. Searching for all vulnerabilities gives 15211 vulnerabilities from 1988 to 2006-02-27. This number doesn't match the number reported on the web page. It's smaller! 3274 vulnerabilities classified as design errors was returned. Windows WMF vulnerability (CVE-2005-4560) is classified as "Input validation error"

Name:	Open source vulnerability database
URL:	www.osvdb.org
Content:	10767 stable entries in the database. 2006-01-16 11059 new entries (not available for the public)
Classification:	Location: Console/Physical Shell/Local Network/Remote Telephony Unknown Attack type: Authentication Management Cryptographic Denial Of Service Hijacking Information Disclosure Infrastructure Input Manipulation Misconfiguration Race Condition Other Unknown Impact: Loss of confidentiality Loss of integrity Loss of availability
CVE:	Where applicable
Public:	YES
Searchable:	Vulnerability Title, Disclosure Date Range, Reference, Text, Vendor, Product, Version, and the classification categories from above
Downloadable:	YES, mysql, postgress
Active:	YES
Other:	Vulnerabilities can be classified with several classifications from each category. If a vulnerability is in severeal programs in an application, it is classified multiple times. From 1972-today. 5303 CVE entries from 1999-today

Name:	Public Cooperative vulnerability database
URL:	https://cirdb.cerias.purdue.edu/coopvdb/public/
Content:	Total number listed: 10573 from 2002 (searchable from 1995)
Classification:	Technical Risk, Threat, Nature
CVE:	YES
Public:	YES
Searchable:	Flexible search in all fields. Analysis, CERT, corevuln, CVE, description, detection, editor, envfeatures, fix, patches, policy, source, system source, submitter, title, workaround. Limit search by: Status, Total Votes, Date, Direct Impact, Operating System, Vendor, nature, Technique, Risk, Threat
Downloadable:	No
Active:	YES
Other:	public review, free account needed, must agree to classify vulnerabilities from time to time Became unavailable when i looked at it first time (unstable?) Uses CVE description as description

Name:	Secunia Advisories
URL:	http://secunia.com/advisories/
Content:	11300 (25 vulnerarbilities per page * 452 pages)
Classification:	Impact: Brute force Cross site scripting DoS Expousre of sensitive information Expousre of system information Hijacking Manipulation of data Privilege escalation Security bypass Spoofing System access Where: From local network From remote Local system
CVE:	YES (uncomplete?)
Public:	YES
Searchable:	Critical level, Impact, Where, Within: headline, software/OS, Body text, CVE; free text. Sort by: match , title, date
Downloadable:	NO
Active:	YES
Other:	Goes back to 2002-09-02. Free text search for "design error" returned 75 hits. Impact can have more than one value Browsable by vendor or product A search for CVE returned 514 entries. Secunia monitors vulnerabilities in more than 6500 products Vulnerabilities in multiple Linux distributions are registered multiple times + one time for the application

Name:	Security Focus
URL:	http://www.securityfocus.com/vulnerabilities
Content:	15570 (?) 30 vulnerabilities per page * 519 pages
Classification:	Yes, but the classes are not listed anywhere. Design error is one class.
CVE:	YES
Public:	YES
Searchable:	Must start with Vendor, product title then product version
Downloadable:	No
Active:	YES
Other:	vuldb@securityfocus.com Search for CVE on the website only returns 300 hits. CVE-2005-1606 (candidate) is f.e. not registered but is mapped from CVE to BID number at CVE http://cve.mitre.org/cve/refs/refmap/source-BID.html Free text search for design error returns 570 hits (includes hits from mailinglists and website. Some entries contains multiple vulnerabilities. Not all entries contains CVE number even when CVE references the BID-number. Not all entries are classified (BID-11047, CVE-2004-1461).

Name:	Security Tracker
URL:	http://www.securitytracker.com/
Content:	More than 10000
Classification:	Access control error Authentication error Boundary error Configuration error Exception handling error Input validation error Not specified Randomization error Resource error State error
CVE:	YES
Public:	YES
Searchable:	Free text. Browsable by advisory, category, cause, impact, reported by, target, the underlying OS, vendor and reverse chronological summary listing
Downloadable:	NO
Active:	YES
Other:	

Name:	US-CERT vulnerability notes database
URL:	http://www.kb.cert.org/vuls
Content:	Probably 1591 notes based on a value in the URL while browsing Goes from 2000-today
Classification:	description
CVE:	YES
Public:	YES
Searchable:	Text, browsable by name, vulnerability ID number, CVE name, date updated, date public, or metric
Downloadable:	NO
Active:	YES
Other:	Most of them included in NVD

B Design flaw vulnerabilities by category

Table 12: Vulnerabilities identified as design flaws

Category:	Access control:Authentication:Missing
Vulnerabilities:	

Category:	Access control:Authentication:Insufficient
Vulnerabilities:	CVE-2000-0696, CVE-2000-0946, CVE-2001-0034, CVE-2001-0250, CVE-2001-1094, CVE-2002-0301, CVE-2002-0396, CVE-2002-2083, CVE-2003-1095, CVE-2004-0593, CVE-2004-0607, CVE-2004-0671, CVE-2004-2144, CVE-2004-2393, CVE-2005-1817, CVE-2005-1905, CVE-2005-2424, CVE-2005-2515, CVE-2005-2798, CVE-2005-3034,

Category:	Access control:Authentication:Static credentials
Vulnerabilities:	CVE-2002-1558, CVE-2004-1474, CVE-2005-0349, CVE-2005-0496,

Category:	Access control:Authentication:Plaintext credentials
Vulnerabilities:	CVE-2002-2122, CVE-2005-2620, CVE-2005-4589,

Category:	Access control:Authentication:Weak obfuscation/encryption of credentials
Vulnerabilities:	

Category:	Access control:Authentication:Backdoor
Vulnerabilities:	CVE-1999-0254, CVE-2004-1884,

Category:	Access control:Authentication:Account lockout
Vulnerabilities:	CVE-2001-0564, CVE-2001-1406,

Category:	Access control:Authorization:Missing
Vulnerabilities:	CVE-1999-0173, CVE-1999-0177, CVE-1999-0191, CVE-1999-0360, CVE-1999-1267, CVE-2001-0352, CVE-2001-0846, CVE-2001-1275, CVE-2002-0027, CVE-2002-0409, CVE-2002-1288, CVE-2004-0135, CVE-2004-1038,

Category:	Access control:Authorization:Insufficient
Vulnerabilities:	CVE-1999-0682, CVE-1999-1485, CVE-2000-0684, CVE-2000-1145, CVE-2001-0482, CVE-2002-1534, CVE-2003-0501, CVE-2004-0162, CVE-2004-0727, CVE-2004-0835, CVE-2004-1157, CVE-2004-1635, CVE-2005-0316, CVE-2005-4697,

Table 12: Vulnerabilities identified as design flaws

Category:	Access control:Authorization:Insecure permissions
Vulnerabilities:	CVE-1999-0473, CVE-1999-1279, CVE-2000-0502, CVE-2001-1515, CVE-2002-0788, CVE-2004-0755, CVE-2005-3321,

Category:	Access control:Authorization:Hook to execute programs or code
Vulnerabilities:	CVE-2001-0722, CVE-2002-0622,

Category:	Access control:Authorization:Action without user confirmation
Vulnerabilities:	CVE-1999-0280, CVE-1999-1055, CVE-1999-1370, CVE-2000-0036, CVE-2002-0618,

Category:	Execution with other privileges:Missing access check
Vulnerabilities:	CVE-2000-0193, CVE-2000-0195, CVE-2000-0881, CVE-2001-0424, CVE-2003-1121, CVE-2004-1295,

Category:	Execution with other privileges:Insufficient access check
Vulnerabilities:	CVE-2002-0542,

Category:	Execution with other privileges:Trusting other component
Vulnerabilities:	CVE-1999-0412, CVE-2000-0703, CVE-2003-0703, CVE-2004-1313, CVE-2005-1371,

Category:	Encryption:Missing
Vulnerabilities:	CVE-2002-0848, CVE-2002-1623, CVE-2005-0744,

Category:	Encryption:Using ECB mode
Vulnerabilities:	CVE-2002-1697,

Category:	Encryption:Weak IV usage
Vulnerabilities:	CVE-2004-2135,

Category:	Encryption:No replay protection
Vulnerabilities:	CVE-1999-0391, CVE-2001-1475,

Category:	Encryption:Other weakness
Vulnerabilities:	CVE-2002-1653, CVE-2002-1872, CVE-2005-2915,

Category:	Processing:Validation
Vulnerabilities:	CVE-1999-0016, CVE-1999-0770, CVE-1999-0969, CVE-1999-1515, CVE-2000-0742, CVE-2000-1203, CVE-2001-0895, CVE-2002-2103, CVE-2004-0526, CVE-2004-1215, CVE-2004-1751, CVE-2005-0143, CVE-2005-0230, CVE-2005-2264, CVE-2006-0236,

Table 12: Vulnerabilities identified as design flaws

Category:	Processing:Incorrect execution order
Vulnerabilities:	CVE-1999-1432, CVE-2001-0393, CVE-2001-0427,

Category:	Processing:Using untrusted data
Vulnerabilities:	CVE-2000-0101, CVE-2001-0860, CVE-2002-0428, CVE-2002-1020,

Category:	Processing:Resource amplification
Vulnerabilities:	CVE-1999-1066, CVE-2004-0683,

Category:	Processing:Unlimited resource usage
Vulnerabilities:	CVE-1999-0250,

Category:	Processing:Insufficient cleanup
Vulnerabilities:	CVE-1999-0372, CVE-2004-0407, CVE-2005-2750,

Category:	Processing:Information leak
Vulnerabilities:	CVE-2001-0031, CVE-2001-1280, CVE-2002-0011, CVE-2002-0483, CVE-2005-0871, CVE-2005-0918,

Category:	Miscellaneous
Vulnerabilities:	CVE-2000-0329, CVE-2002-1637, CVE-2003-0677, CVE-2004-2527, CVE-2005-0591, CVE-2005-3344,

C Vulnerabilities identified as design flaws

Table 13: Vulnerabilities identified as design flaws

CVE name	Data
CVE-1999-0016	Land IP denial of service
	Comment: not checking validity of source address
	Classification: Processing:Validation
CVE-1999-0173	FormMail CGI program can be used by web servers other than the host server that the program resides on.
	Comment: no authentication/authorization for usage
	Classification: Access control:Authorization:Missing
CVE-1999-0177	The uploader program in the WebSite web server allows a remote attacker to execute arbitrary programs.
	Comment: no authorization, upload to wherever you want.
	Classification: Access control:Authorization:Missing
CVE-1999-0191	IIS newdsn.exe CGI script allows remote users to overwrite files.
	Comment: no restriction on file creation location and name
	Classification: Access control:Authorization:Missing
CVE-1999-0250	Denial of service in Qmail through long SMTP commands.
	Comment: no limit on number of recipients in a message.
	Classification: Processing:Unlimited resource usage
CVE-1999-0254	A hidden SNMP community string in HP OpenView allows remote attackers to modify MIB tables and obtain sensitive information.
	Comment: static access code, secret code. (NT-version not vulnerable)
	Classification: Access control:Authentication:Backdoor
CVE-1999-0280	Remote command execution in Microsoft Internet Explorer using .lnk and .url files.
	Comment: local execution of program remote link points to instead of displaying file in browser. 1) User clicks on link to .url or .lnk. 2) ie downloads this file. 3) ie executes the file locally without warning the user.
	Classification: Access control:Authorization:Action without user confirmation
CVE-1999-0360	MS Site Server 2.0 with IIS 4 can allow users to upload content, including ASP, to the target web site, thus allowing them to execute commands remotely.
	Comment: no restriction on file creation. Not checking if webroot/users exist.
	Classification: Access control:Authorization:Missing
CVE-1999-0372	The installer for BackOffice Server includes account names and passwords in a setup file (reboot.ini) which is not deleted.
	Comment: storing credentials in temporary files without cleaning up.
	Classification: Processing:Insufficient cleanup
CVE-1999-0391	The cryptographic challenge of SMB authentication in Windows 95 and Windows 98 can be reused, allowing an attacker to replay the response and impersonate a user.
	Comment: weak encryption in authentication, replay possible
	Classification: Encryption:No replay protection
CVE-1999-0412	In IIS and other web servers, an attacker can attack commands as SYSTEM if the server is running as SYSTEM and loading an ISAPI extension.

Table 13: Vulnerabilities identified as design flaws

CVE name	Data
	Comment: nvd calls it buffer overflow, bid race condition. untrusted code allowed to change privileges. access controll problem. When registering a DLL, GetExtensionVersion() in the DLL is called with SYSTEM privileges
	Classification: Execution with other privileges:Trusting other component
CVE-1999-0473	The rsync command before rsync 2.3.1 may inadvertently change the permissions of the client's working directory to the permissions of the directory being transferred.
	Comment: permissions changed
	Classification: Access control:Authorization:Insecure permissions
CVE-1999-0682	Microsoft Exchange 5.5 allows a remote attacker to relay email (i.e. spam) using encapsulated SMTP addresses, even if the anti-relaying features are enabled.
	Comment: missing access check. not checking all access paths.
	Classification: Access control:Authorization:Insufficient
CVE-1999-0770	Firewall-1 sets a long timeout for connections that begin with ACK or other packets except SYN, allowing an attacker to conduct a denial of service via a large number of connection attempts to unresponsive systems.
	Comment: not checking state properly. use long timeout for ack even when no syn is received first
	Classification: Processing:Validation
CVE-1999-0969	The Windows NT RPC service allows remote attackers to conduct a denial of service using spoofed malformed RPC packets which generate an error message that is sent to the spoofed host, potentially setting up a loop, aka Snork.
	Comment: looping. no authentication of ip address, answering responses to packets not sent
	Classification: Processing:Validation
CVE-1999-1055	Microsoft Excel 97 does not warn the user before executing worksheet functions, which could allow attackers to execute arbitrary commands by using the CALL function to execute a malicious DLL, aka the Excel "CALL Vulnerability."
	Comment: not asking user for permission before unsafe call
	Classification: Access control:Authorization:Action without user confirmation
CVE-1999-1066	Quake 1 server responds to an initial UDP game connection request with a large amount of traffic, which allows remote attackers to use the server as an amplifier in a "Smurf" style attack on another host, by spoofing the connection request.
	Comment: asymtric send-receive data size. no ip authentication.
	Classification: Processing:Resource amplification
CVE-1999-1267	KDE file manager (kfm) uses a TCP server for certain file operations, which allows remote attackers to modify arbitrary files by sending a copy command to the server.
	Comment: insecure use of TCP-sockets, no authentication/authorization?
	Classification: Access control:Authorization:Missing
CVE-1999-1279	An interaction between the AS/400 shared folders feature and Microsoft SNA Server 3.0 and earlier allows users to view each other's folders when the users share the same Local APPC LU.
	Comment: shared folders intended to be accessed directly and not over parallel sessions from a single LU-LU pair. rights are inherited from first user.
	Classification: Access control:Authorization:Insecure permissions

Table 13: Vulnerabilities identified as design flaws

CVE name	Data
CVE-1999-1370	The setup wizard (ie5setup.exe) for Internet Explorer 5.0 disables (1) the screen saver, which could leave the system open to users with physical access if a failure occurs during an unattended installation, and (2) the Task Scheduler Service, which might prevent the scheduled execution of security-critical programs.
	Comment: functionality disabled without notifying user.
	Classification: Access control:Authorization:Action without user confirmation
CVE-1999-1432	Power management (Powermanagement) on Solaris 2.4 through 2.6 does not start the xlock process until after the sys-suspend has completed, which allows an attacker with physical access to input characters to the last active application from the keyboard for a short period after the system is restoring, which could lead to increased privileges.
	Comment: xlock should be started before suspend. incorrect activation position
	Classification: Processing:Incorrect execution order
CVE-1999-1485	nsd in IRIX 6.5 through 6.5.2 exports a virtual filesystem on a UDP port, which allows remote attackers to view files and cause a possible denial of service by mounting the nsd virtual file system.
	Comment: no access control (authentication), binds to random port, mount file handle 32 zeroes
	Classification: Access control:Authorization:Insufficient
CVE-1999-1515	A non-default configuration in TenFour TFS Gateway 4.0 allows an attacker to cause a denial of service via messages with incorrect sender and recipient addresses, which causes the gateway to continuously try to return the message every 10 seconds.
	Comment:
	Classification: Processing:Validation
CVE-2000-0036	Outlook Express 5 for Macintosh downloads attachments to HTML mail without prompting the user, aka the "HTML Mail Attachment" vulnerability.
	Comment: no user confirmation before insecure action. validation
	Classification: Access control:Authorization:Action without user confirmation
CVE-2000-0101	The Make-a-Store OrderPage shopping cart application allows remote users to modify sensitive purchase information via hidden form fields.
	Comment: using client supplied data instead of server based data. Calculation with untrusted data
	Classification: Processing:Using untrusted data
CVE-2000-0193	The default configuration of Dosemu in Corel Linux 1.0 allows local users to execute the system.com program and gain privileges.
	Comment: suid, no authorization, not dropping privileges.
	Classification: Execution with other privileges:Missing access check
CVE-2000-0195	setxconf in Corel Linux allows local users to gain root access via the -T parameter, which executes the user's .xserverrc file.
	Comment: failure to drop privileges
	Classification: Execution with other privileges:Missing access check
CVE-2000-0329	A Microsoft ActiveX control allows a remote attacker to execute a malicious cabinet file via an attachment and an embedded script in an HTML mail, aka the "Active Setup Control" vulnerability.
	Comment: temporary files are stored in known places. A webpage/html-email could contain a malicous file and code to run the file from the temporary place
	Classification: Miscellaneous

Table 13: Vulnerabilities identified as design flaws

CVE name	Data
CVE-2000-0502	Mcafee VirusScan 4.03 does not properly restrict access to the alert text file before it is sent to the Central Alert Server, which allows local users to modify alerts in an arbitrary fashion.
	Comment: no authentication, origin
	Classification: Access control:Authorization:Insecure permissions
CVE-2000-0684	BEA WebLogic 5.1.x does not properly restrict access to the JSPServlet, which could allow remote attackers to compile and execute Java JSP code by directly invoking the servlet on any source file.
	Comment: executing untrusted code, executing code in .txt files
	Classification: Access control:Authorization:Insufficient
CVE-2000-0696	The administration interface for the dwhttpd web server in Solaris AnswerBook2 does not properly authenticate requests to its supporting CGI scripts, which allows remote attackers to add user accounts to the interface by directly calling the admin CGI script.
	Comment: Program A does authentication and calls another program B. Program B does not does not check if you are a authorized user. authorization problem. authentication bypass by other execution path?
	Classification: Access control:Authentication:Insufficient
CVE-2000-0703	suidperl (aka sperl) does not properly cleanse the escape sequence " !" before calling /bin/mail to send an error report, which allows local users to gain privileges by setting the "interactive" environmental variable and calling suidperl with a filename that contains the escape sequence.
	Comment: not dropping privileges, trusting other component.
	Classification: Execution with other privileges:Trusting other component
CVE-2000-0742	The IPX protocol implementation in Microsoft Windows 95 and 98 allows remote attackers to cause a denial of service by sending a ping packet with a source IP address that is a broadcast address, aka the "Malformed IPX Ping Packet" vulnerability.
	Comment: resource amplification
	Classification: Processing:Validation
CVE-2000-0881	The dccscan setuid program in LPPlus does not properly check if the user has the permissions to print the file that is specified to dccscan, which allows local users to print arbitrary files.
	Comment: not dropping priviliges, not checking acl
	Classification: Execution with other privileges:Missing access check
CVE-2000-0946	Compaq Easy Access Keyboard software 1.3 does not properly disable access to custom buttons when the screen is locked, which could allow an attacker to gain privileges or execute programs without authorization.
	Comment: locked keyboard doesn't lock all keys
	Classification: Access control:Authentication:Insufficient
CVE-2000-1145	Recourse ManTrap 1.6 allows attackers who have gained root access to use utilities such as crash or fsdb to read /dev/mem and raw disk devices to identify ManTrap processes or modify arbitrary data files.
	Comment: insufficient compartementalize, no access control
	Classification: Access control:Authorization:Insufficient
CVE-2000-1203	Lotus Domino SMTP server 4.63 through 5.08 allows remote attackers to cause a denial of service (CPU consumption) by forging an email message with the sender as bounce@[127.0.0.1] (localhost), which causes Domino to enter a mail loop.
	Comment: not blocking when destination is the same as source and it's its own address
	Classification: Processing:Validation
CVE-2001-0031	BroadVision One-To-One Enterprise allows remote attackers to determine the physical path of server files by requesting a .JSP file name that does not exist.

Table 13: Vulnerabilities identified as design flaws

CVE name	Data
	Comment:
	Classification: Processing:Information leak
CVE-2001-0034	KTH Kerberos IV allows local users to specify an alternate proxy using the krb4_proxy variable, which allows the user to generate false proxy responses and possibly gain privileges.
	Comment: configuration data read from changeable environment variables
	Classification: Access control:Authentication:Insufficient
CVE-2001-0250	The Web Publishing feature in Netscape Enterprise Server 4.x and earlier allows remote attackers to list arbitrary directories under the web server root via the INDEX command.
	Comment: unauthenticated users able to get directory listings.
	Classification: Access control:Authentication:Insufficient
CVE-2001-0352	SNMP agents in 3Com AirConnect AP-4111 and Symbol 41X1 Access Point allow remote attackers to obtain the WEP encryption key by reading it from a MIB when the value should be write-only, via (1) dot11WEPDefaultKeyValue in the dot11WEPDefaultKeysTable of the IEEE 802.11b MIB, or (2) ap128bWepKeyValue in the ap128bWEPKeyTable in the Symbol MIB.
	Comment: no access control, data should not be available
	Classification: Access control:Authorization:Missing
CVE-2001-0393	Navision Financials Server 2.0 allows remote attackers to cause a denial of service via a series of connections to the server without providing a username/password combination, which consumes the license limits.
	Comment: using licenses before user is authenticated
	Classification: Processing:Incorrect execution order
CVE-2001-0424	BubbleMon 1.31 does not properly drop group privileges before executing programs, which allows local users to execute arbitrary commands with the kmem group id.
	Comment: executing with too much privileges
	Classification: Execution with other privileges:Missing access check
CVE-2001-0427	Cisco VPN 3000 series concentrators before 2.5.2(F) allow remote attackers to cause a denial of service via a flood of invalid login requests to (1) the SSL service, or (2) the telnet service, which do not properly disconnect the user after several failed login attempts.
	Comment:
	Classification: Processing:Incorrect execution order
CVE-2001-0482	Configuration error in Argus PitBull LX allows root users to bypass specified access control restrictions and cause a denial of service or execute arbitrary commands by modifying kernel variables such as MaxFiles, MaxInodes, and ModProbePath in /proc/sys via calls to sysctl.
	Comment: insecure defaults, authorization not applied to all directories.
	Classification: Access control:Authorization:Insufficient
CVE-2001-0564	APC Web/SNMP Management Card prior to Firmware 310 only supports one telnet connection, which allows a remote attacker to create a denial of service via repeated failed logon attempts which temporarily locks the card.
	Comment: 3 failed login attempts locks out all users
	Classification: Access control:Authentication:Account lockout
CVE-2001-0722	Internet Explorer 5.5 and 6.0 allows remote attackers to read and modify user cookies via Javascript in an about: URL, aka the "First Cookie Handling Vulnerability."
	Comment: html/javascript/code execution by a usersupplied URL.
	Classification: Access control:Authorization:Hook to execute programs or code

Table 13: Vulnerabilities identified as design flaws

CVE name	Data
CVE-2001-0846	Lotus Domino 5.x allows remote attackers to read files or execute arbitrary code by requesting the ReplicaID of the Web Administrator template file (webadmin.ntf).
	Comment: no authentication, insufficient authorization check
	Classification: Access control:Authorization:Missing
CVE-2001-0860	Terminal Services Manager MMC in Windows 2000 and XP trusts the Client Address (IP address) that is provided by the client instead of obtaining it from the packet headers, which allows clients to spoof their public IP address, e.g. through a Network Address Translation (NAT).
	Comment: trust of client supplied data, IP address. Validation on user supplied data when real data is available.
	Classification: Processing:Using untrusted data
CVE-2001-0895	Multiple Cisco networking products allow remote attackers to cause a denial of service on the local network via a series of ARP packets sent to the router's interface that contains a different MAC address for the router, which eventually causes the router to overwrite the MAC address in its ARP table.
	Comment: trust in user supplied data? Data/configuration should not be allowed to change
	Classification: Processing:Validation
CVE-2001-1094	NetOp School 1.5 allows local users to bypass access restrictions on the administration version by logging into the student version, closing the student version, then starting the administration version.
	Comment: authentication bypass by killing less privileged process
	Classification: Access control:Authentication:Insufficient
CVE-2001-1275	MySQL before 3.23.31 allows users with a MySQL account to use the SHOW GRANTS command to obtain the encrypted administrator password from the mysql.user table and possibly gain privileges via password cracking.
	Comment: insufficient/missing authorization.
	Classification: Access control:Authorization:Missing
CVE-2001-1280	POP3 Server for Ipswitch IMail 7.04 and earlier generates different responses to valid and invalid user names, which allows remote attackers to determine users on the system.
	Comment: different responses to queries for existing and non existing data. authentication
	Classification: Processing:Information leak
CVE-2001-1406	process_bug.cgi in Bugzilla before 2.14 does not set the "groupset" bit when a bug is moved between product groups, which will cause the bug to have the old group's restrictions, which might not be as stringent.
	Comment: fails to change group acl when moved to other groups
	Classification: Access control:Authentication:Account lockout
CVE-2001-1475	SSH before 2.0, when using RC4 and password authentication, allows remote attackers to replay messages until a new server key (VK) is generated.
	Comment: insufficient replay protection
	Classification: Encryption:No replay protection
CVE-2001-1515	Macintosh clients, when using NT file system volumes on Windows 2000 SP1, create subdirectories and automatically modify the inherited NTFS permissions, which may cause the directories to have less restrictive permissions than intended.
	Comment: insecure default rights
	Classification: Access control:Authorization:Insecure permissions
CVE-2002-0011	Information leak in doeditvotes.cgi in Bugzilla before 2.14.1 may allow remote attackers to more easily conduct attacks on the login.

Table 13: Vulnerabilities identified as design flaws

CVE name	Data
	Comment: information leak in response to login request
	Classification: Processing:Information leak
CVE-2002-0027	Internet Explorer 5.5 and 6.0 allows remote attackers to read certain files and spoof the URL in the address bar by using the Document.open function to pass information between two frames from different domains, a new variant of the "Frame Domain Verification" vulnerability described in MS:MS01-058/CAN-2001-0874.
	Comment: origin validation, insufficient authorization
	Classification: Access control:Authorization:Missing
CVE-2002-0301	Citrix NFuse 1.6 allows remote attackers to bypass authentication and obtain sensitive information by directly calling launch.asp with invalid NFUSE_USER and NFUSE_PASSWORD parameters.
	Comment: authentication/authorization bypass
	Classification: Access control:Authentication:Insufficient
CVE-2002-0396	The web management server for Red-M 1050 (Bluetooth Access Point) does not use session-based credentials to authenticate users, which allows attackers to connect to the server from the same IP address as a user who has already established a session.
	Comment: no session management, insufficient authentication
	Classification: Access control:Authentication:Insufficient
CVE-2002-0409	orderdetails.aspx, as made available to Microsoft .NET developers as example code and demonstrated on www.ibuyspystore.com, allows remote attackers to view the orders of other users by modifying the OrderID parameter.
	Comment: no access control.
	Classification: Access control:Authorization:Missing
CVE-2002-0428	Check Point FireWall-1 SecuRemote/SecuClient 4.0 and 4.1 allows clients to bypass the "authentication timeout" by modifying the to_expire or expire values in the client's users.C configuration file.
	Comment: trust in client data,
	Classification: Processing:Using untrusted data
CVE-2002-0483	index.php for PHP-Nuke 5.4 and earlier allows remote attackers to determine the physical pathname of the web server when the file parameter is set to index.php, which triggers an error message that leaks the pathname.
	Comment:
	Classification: Processing:Information leak
CVE-2002-0542	mail in OpenBSD 2.9 and 3.0 processes a tilde ( ) escape character in a message even when it is not in interactive mode, which could allow local users to gain root privileges via calls to mail in cron.
	Comment: suid command execution hook. Not checking variable value
	Classification: Execution with other privileges:Insufficient access check
CVE-2002-0618	The Macro Security Model in Microsoft Excel 2000 and 2002 for Windows allows remote attackers to execute code in the Local Computer zone by embedding HTML scripts within an Excel workbook that contains an XSL stylesheet, aka "Excel XSL Stylesheet Script Execution".
	Comment: no compartementalize, execution without warning
	Classification: Access control:Authorization:Action without user confirmation
CVE-2002-0622	The Office Web Components (OWC) package installer for Microsoft Commerce Server 2000 allows remote attackers to execute commands by passing the commands as input to the OWC package installer, aka "OWC Package Command Execution".
	Comment: Self chosen command is taken as input

Table 13: Vulnerabilities identified as design flaws

CVE name	Data
	Classification: Access control:Authorization:Hook to execute programs or code
CVE-2002-0788	An interaction between PGP 7.0.3 with the "wipe deleted files" option, when used on Windows Encrypted File System (EFS), creates a cleartext temporary files that cannot be wiped or deleted due to strong permissions, which could allow certain local users or attackers with physical access to obtain cleartext information.
	Comment: ??? too restrictive rights
	Classification: Access control:Authorization:Insecure permissions
CVE-2002-0848	Cisco VPN 5000 series concentrator hardware 6.0.21.0002 and earlier, and 5.2.23.0003 and earlier, when using RADIUS with a challenge type of Password Authentication Protocol (PAP) or Challenge, sends the user password in cleartext in a validation retry request, which could allow remote attackers to steal passwords via sniffing.
	Comment: cleartext password in retry authentication request
	Classification: Encryption:Missing
CVE-2002-1020	The library feature for Adobe Content Server 3.0 allows a remote attacker to check out an eBook even when the maximum number of loans is exceeded by accessing the "Add to bookbag" feature when the server reports that no more copies are available.
	Comment: trusting client supplied data for calculation. insufficient restrictions. insufficient access validation
	Classification: Processing:Using untrusted data
CVE-2002-1288	The Microsoft Java implementation, as used in Internet Explorer, allows remote attackers to determine the current directory of the Internet Explorer process via the getAbsolutePath() method in a File() call.
	Comment: revealing to much information to untrusted code, no access control
	Classification: Access control:Authorization:Missing
CVE-2002-1534	Macromedia Flash Player allows remote attackers to read arbitrary files via XML script in a .swf file that is hosted on a remote SMB share.
	Comment: access validation, insufficient origin validation, insufficient compartementalization or security zone handling
	Classification: Access control:Authorization:Insufficient
CVE-2002-1558	Cisco ONS15454 and ONS15327 running ONS before 3.4 have an account for the VxWorks Operating System in the TCC, TCC+ and XTC that cannot be changed or disabled, which allows remote attackers to gain privileges by connecting to the account via Telnet.
	Comment: static default account/password
	Classification: Access control:Authentication:Static credentials
CVE-2002-1623	The design of the Internet Key Exchange (IKE) protocol, when using Aggressive Mode for shared secret authentication, does not encrypt initiator or responder identities during negotiation, which may allow remote attackers to determine valid usernames by (1) monitoring responses before the password is supplied or (2) sniffing, as originally reported for FireWall-1 SecuRemote.
	Comment: not all parts encrypted
	Classification: Encryption:Missing
CVE-2002-1637	Multiple components in Oracle 9i Application Server (9iAS) are installed with over 160 default usernames and passwords, including (1) SYS, (2) SYSTEM, (3) AQJAVA, (4) OWA, (5) IMAGEUSER, (6) USER1, (7) USER2, (8) PLSQL, (9) DEMO, (10) FINANCE, and many others, which allows attackers to gain privileges.
	Comment: Default account and password. required for some applications. user not forced to choose password when installed.

Table 13: Vulnerabilities identified as design flaws

CVE name	Data
	Classification: Miscellaneous
CVE-2002-1653	Farm9 Cryptcat, when started in server mode with the -e option, does not enable encryption, which allows clients to communicate without encryption despite intended configuration, and may allow remote attackers to sniff sensitive information.
	Comment: encryption not activated when told to do so.
	Classification: Encryption:Other weakness
CVE-2002-1697	Electronic Code Book (ECB) mode in VTun 2.0 through 2.5 uses a weak encryption algorithm that produces the same ciphertext from the same plaintext blocks, which could allow remote attackers to gain senstive information.
	Comment: weak encryption, ECB.
	Classification: Encryption:Using ECB mode
CVE-2002-1872	Microsoft SQL Server 6.0 through 2000, with SQL Authentication enabled, uses weak password encryption (XOR), which allows remote attackers to sniff and decrypt the password.
	Comment: weak password encryption authentication transfer
	Classification: Encryption:Other weakness
CVE-2002-2083	The Novell Netware client running on Windows 95 allows local users to bypass the login and open arbitrary files via the "What is this?" help feature, which can be launched from the Novell Netware login screen.
	Comment:
	Classification: Access control:Authentication:Insufficient
CVE-2002-2103	Apache before 1.3.24, when writing to the log file, records a spoofed hostname from the reverse lookup of an IP address, even when a double-reverse lookup fails, which allows remote attackers to hide the original source of activities.
	Comment: logging spoofed address, logging with incorrect data.
	Classification: Processing:Validation
CVE-2002-2122	Pointsec before 1.2 for PalmOS stores a user's PIN number in memory in plaintext, which allows a local attacker who steals an unlocked Palm to retrieve the PIN by dumping memory.
	Comment: password in plaintext in memory after use.
	Classification: Access control:Authentication:Plaintext credentials
CVE-2003-0501	The /proc filesystem in Linux allows local users to obtain sensitive information by opening various entries in /proc/self before executing a setuid program, which causes the program to fail to change the ownership and permissions of those entries.
	Comment: authorization does not protect all objects or access paths?
	Classification: Access control:Authorization:Insufficient
CVE-2003-0677	Cisco CSS 11000 routers on the CS800 chassis allow remote attackers to cause a denial of service (CPU consumption or reboot) via a large number of TCP SYN packets to the circuit IP address, aka "ONDM Ping failure."
	Comment:
	Classification: Miscellaneous
CVE-2003-0703	KisMAC before 0.05d trusts user-supplied variables to load arbitrary kernels or kernel modules, which allows local users to gain privileges via the $DRIVER_KEXT environment variable as used in (1) viha_driver.sh, (2) macjack_load.sh, or (3) airojack_load.sh, or (4) via "similar techniques" using exchangeKernel.sh.
	Comment: trusting shell variables
	Classification: Execution with other privileges:Trusting other component

Table 13: Vulnerabilities identified as design flaws

CVE name	Data
CVE-2003-1095	BEA WebLogic Server and Express 7.0 and 7.0.0.1, when using "memory" session persistence for web applications, does not clear authentication information when a web application is redeployed, which could allow users of that application to gain access without having to re-authenticate.
	Comment: fail to update cache after policy update. bypass of authentication
	Classification: Access control:Authentication:Insufficient
CVE-2003-1121	Services in ScriptLogic 4.01, and possibly other versions before 4.14, process client requests at raised privileges, which allows remote attackers to (1) modify arbitrary registry entries via the ScriptLogic RPC service (SLRPC) or (2) modify arbitrary configuration via the RunAdmin services (SLRAserver.exe and SLRAclient.exe).
	Comment: no access control, too many rights
	Classification: Execution with other privileges:Missing access check
CVE-2004-0135	The syssgi SGI_IOPROBE system call in IRIX 6.5.20 through 6.5.24 allows local users to gain privileges by reading and writing to kernel memory.
	Comment: no check for writes to kernel memory. no access control
	Classification: Access control:Authorization:Missing
CVE-2004-0162	Multiple content security gateway and antivirus products allow remote attackers to bypass content restrictions via MIME encapsulation that uses RFC822 comment fields, which may be interpreted as other fields by mail clients.
	Comment:
	Classification: Access control:Authorization:Insufficient
CVE-2004-0407	The HTML form upload capability in ColdFusion MX 6.1 does not reclaim disk space if an upload is interrupted, which allows remote attackers to cause a denial of service (disk consumption) by repeatedly uploading files and interrupting the uploads before they finish.
	Comment: resources not cleared
	Classification: Processing:Insufficient cleanup
CVE-2004-0526	Unknown versions of Internet Explorer and Outlook allow remote attackers to spoof a legitimate URL in the status bar via A HREF tags with modified "alt" values that point to the legitimate site, combined with an image map whose href points to the malicious site, which facilitates a "phishing" attack.
	Comment: display information from wrong source. hide real url destination
	Classification: Processing:Validation
CVE-2004-0593	Sygate Enforcer 3.5MR1 and earlier passes broadcast traffic before authentication, which could allow remote attackers to bypass filtering rules.
	Comment: some general traffic is allowed through without authentication
	Classification: Access control:Authentication:Insufficient
CVE-2004-0607	The eay_check_x509cert function in KAME Racoon successfully verifies certificates even when OpenSSL validation fails, which could allow remote attackers to bypass authentication.
	Comment: ignoring certificate validation errors. invalid certificates accepted
	Classification: Access control:Authentication:Insufficient
CVE-2004-0671	Brightmail Spamfilter 6.0 and earlier beta releases allows remote attackers to read mail from other users by modifying the id parameter in a viewMsgDetails.do request.
	Comment: missing authentication
	Classification: Access control:Authentication:Insufficient

Table 13: Vulnerabilities identified as design flaws

CVE name	Data
CVE-2004-0683	Symantec Norton AntiVirus 2002 and 2003 allows remote attackers to cause a denial of service (CPU consumption) via a compressed archive that contains a large number of directories.
	Comment:
	Classification: Processing:Resource amplification
CVE-2004-0727	Microsoft Internet Explorer 6.0.2800.1106 on Microsoft Windows XP SP2, and other versions including 5.01 and 5.5, allows remote web servers to bypass zone restrictions and execute arbitrary code in the local computer zone by redirecting a function to another function with the same name, as demonstrated by SimilarMethodNameRedir, aka the "Similar Method Name Redirection Cross Domain Vulnerability."
	Comment: insufficient authorization, zone handling
	Classification: Access control:Authorization:Insufficient
CVE-2004-0755	The FileStore capability in CGI::Session for Ruby before 1.8.1, and possibly PStore, creates files with insecure permissions, which can allow local users to steal session information and hijack sessions.
	Comment: failure to protect credentials, insufficient file permissions
	Classification: Access control:Authorization:Insecure permissions
CVE-2004-0835	MySQL 3.x before 3.23.59, 4.x before 4.0.19, 4.1.x before 4.1.2, and 5.x before 5.0.1, checks the CREATE/INSERT rights of the original table instead of the target table in an ALTER TABLE RENAME operation, which could allow attackers to conduct unauthorized activities.
	Comment: checking wrong acl
	Classification: Access control:Authorization:Insufficient
CVE-2004-1038	A design error in the IEEE1394 specification allows attackers with physical access to a device to read and write to sensitive memory using a modified FireWire/IEEE 1394 client, thus bypassing intended restrictions that would normally require greater degrees of physical access to exploit.
	Comment: no access control
	Classification: Access control:Authorization:Missing
CVE-2004-1157	Opera 7.x up to 7.54, and possibly other versions, allows remote attackers to spoof arbitrary web sites by injecting content from one window into a target window whose name is known but resides in a different domain, as demonstrated using a pop-up window on a trusted web site, aka the "window injection" vulnerability.
	Comment: insufficient origin check for frames. access control? security zone?
	Classification: Access control:Authorization:Insufficient
CVE-2004-1215	Kreed 1.05 and earlier allows remote attackers to cause a denial of service (server disconnect) via a long UDP packet, which causes a "message too long" socket error.
	Comment: improperly handling of error condition
	Classification: Processing:Validation
CVE-2004-1295	The slip_down function in slip.c for the uml_net program in uml-utilities 20030903, when uml_net is installed setuid root, does not verify whether the calling user has sufficient permission to disable an interface, which allows local users to cause a denial of service (network service disabled).
	Comment: too many privileges, no access control
	Classification: Execution with other privileges:Missing access check
CVE-2004-1313	The Smc.exe process in My Firewall Plus 5.0 build 1117, and possibly other versions, does not drop privileges before invoking help, which allows local users to gain privileges.
	Comment: execute external software with too much rights.
	Classification: Execution with other privileges:Trusting other component

Table 13: Vulnerabilities identified as design flaws

CVE name	Data
CVE-2004-1474	Symantec Enterprise Firewall/VPN Appliances 100, 200, and 200R running firmware before 1.63 and Gateway Security 320, 360, and 360R running firmware before 622 uses a default read/write SNMP community string, which allows remote attackers to alter the firewall's configuration file.
	Comment: default static community string
	Classification: Access control:Authentication:Static credentials
CVE-2004-1635	Bugzilla 2.17.1 through 2.18rc2 and 2.19 from cvs, when using the insidergroup feature, does not sufficiently protect private attachments when there are changes to the metadata, such as filename, description, MIME type, or review flags, which allows remote authenticated users to obtain sensitive information when (1) viewing the bug activity log or (2) receiving bug change notification mails.
	Comment: no access control
	Classification: Access control:Authorization:Insufficient
CVE-2004-1751	Ground Control II: Operation Exodus 1.0.0.7 and earlier allows remote servers to cause a denial of service (client or server crash) via a large packet, which generates a "Message too long" socket error that is treated as a critical error.
	Comment: improperly handling of eror condition
	Classification: Processing:Validation
CVE-2004-1884	Ipswitch WS_FTP Server 4.0.2 has a backdoor XXSESS_MGRYY username with a default password, which allows remote attackers to gain access.
	Comment: authentication, backdoor
	Classification: Access control:Authentication:Backdoor
CVE-2004-2135	cryptoloop on Linux kernel 2.6.x, when used on certain file systems with a block size 1024 or greater, has certain "IV computation" weaknesses that allow watermarked files to be detected without decryption.
	Comment: IV problem
	Classification: Encryption:Weak IV usage
CVE-2004-2144	Baal Smart Forms before 3.2 allows remote attackers to bypass authentication and obtain system access via a direct request to regadmin.php.
	Comment: no authentication, authentication bypass
	Classification: Access control:Authentication:Insufficient
CVE-2004-2393	Java Secure Socket Extension (JSSE) 1.0.3 through 1.0.3_2 does not properly validate the certificate chain of a client or server, which allows remote attackers to falsely authenticate peers for SSL/TLS.
	Comment: Fail to validate certificate chain
	Classification: Access control:Authentication:Insufficient
CVE-2004-2527	The local and remote desktop login screens in Microsoft Windows XP before SP2 and 2003 allow remote attackers to cause a denial of service (CPU and memory consumption) by repeatedly using the WinKey+"U" key combination, which causes multiple copies of Windows Utility Manager to be loaded more quickly than they can be closed when the copies detect that another instance is running.
	Comment: state problem
	Classification: Miscellaneous
CVE-2005-0143	Firefox before 1.0 and Mozilla before 1.7.5 display the SSL lock icon when an insecure page loads a binary file from a trusted site, which could facilitate phishing attacks.
	Comment: unsecure address displayed as secure.
	Classification: Processing:Validation

Table 13: Vulnerabilities identified as design flaws

CVE name	Data
CVE-2005-0230	Firefox 1.0 does not prevent the user from dragging an executable file to the desktop when it has an image/gif content type but has a dangerous extension such as .bat or .exe, which allows remote attackers to bypass the intended restriction and execute arbitrary commands via malformed GIF files that can still be parsed by the Windows batch file parser, aka "firedragging."
	Comment: allow wrong protocoll/format to be displayed. real format not same as what client says.
	Classification: Processing:Validation
CVE-2005-0316	WebWasher Classic 2.2.1 and 3.3, when running in server mode, does not properly drop CONNECT requests to the localhost from external systems, which could allow remote attackers to bypass intended access restrictions.
	Comment: proxy server allowing proxy connections to itself (127.0.0.1)
	Classification: Access control:Authorization:Insufficient
CVE-2005-0349	The production release of the UniversalAgent for UNIX in BrightStor ARCserve Backup 11.1 contains hard-coded credentials, which allows remote attackers to access the file system and possibly execute arbitrary commands.
	Comment: hard-coded user name and password
	Classification: Access control:Authentication:Static credentials
CVE-2005-0496	Arkeia Network Backup Client 5.x contains hard-coded credentials that effectively serve as a back door, which allows remote attackers to access the file system and possibly execute arbitrary commands.
	Comment: hardcoded credentials
	Classification: Access control:Authentication:Static credentials
CVE-2005-0591	Firefox before 1.0.1 allows remote attackers to spoof the (1) security and (2) download modal dialog boxes, which could be used to trick users into executing script or downloading and executing a file, aka "Firespoofing."
	Comment: hiding real action, visual
	Classification: Miscellaneous
CVE-2005-0744	The web GUI for Novell iChain 2.2 and 2.3 SP2 and SP3 allows attackers to hijack sessions and gain administrator privileges by (1) sniffing the connection on TCP port 51100 and replaying the authentication information or (2) obtaining and replaying the PCZQX02 authentication cookie from the browser.
	Comment: unsecure communication channel
	Classification: Encryption:Missing
CVE-2005-0871	calendar_scheduler.php in Topic Calendar 1.0.1 module for phpBB, when running on a Microsoft IIS server, allows remote attackers to obtain sensitive information via invalid parameters, which reveal the path in an error message.
	Comment: leaking sensitive information in error messages
	Classification: Processing:Information leak
CVE-2005-0918	The NPSVG3.dll ActiveX control for Adobe SVG Viewer 3.02 and earlier, when running on Internet Explorer, allows remote attackers to determine the existence of arbitrary files by setting the src property to the target filename and using Javascript to determine if the web page immediately stops loading, which indicates whether the file exists or not.
	Comment: timing based.
	Classification: Processing:Information leak
CVE-2005-1371	BPFTPServer service in BulletProof FTP Server 2.4.0.31 does not properly drop privileges before opening files through the Help menu, which allows local users to gain privileges.
	Comment: SUID, trusting executed code

Table 13: Vulnerabilities identified as design flaws

CVE name	Data
	Classification: Execution with other privileges:Trusting other component
CVE-2005-1817	Invision Power Board (IPB) 1.0 through 1.3 allows remote attackers to edit arbitrary forum posts via a direct request to index.php with modified parameters.
	Comment: no access control
	Classification: Access control:Authentication:Insufficient
CVE-2005-1905	The klif.sys driver in Kaspersky Labs Anti-Virus 5.0.227, 5.0.228, and 5.0.335 on Windows 2000 allows local users to gain privileges by modifying certain critical code addresses that are later accessed by privileged programs.
	Comment: execution of user supplied code in privileged code.
	Classification: Access control:Authentication:Insufficient
CVE-2005-2264	Firefox before 1.0.5 allows remote attackers to steal sensitive information by opening a malicious link in the Firefox sidebar using the _search target, then injecting script into other pages via a data: URL.
	Comment: validate image with content-type header, but uses URL file extension when saving
	Classification: Processing:Validation
CVE-2005-2424	The management interface for Siemens SANTIS 50 running firmware 4.2.8.0, and possibly other products including Ericsson HN294dp and Dynalink RTA300W, allows remote attackers to access the Telnet port without authentication via certain packets to the web interface that cause the interface to freeze.
	Comment: no authentication when failure happens
	Classification: Access control:Authentication:Insufficient
CVE-2005-2515	Quartz Composer Screen Saver in Mac OS X 10.4.2 allows local users to access links from the RSS Visualizer even when a password is required.
	Comment: authorization bypass. not checking state
	Classification: Access control:Authentication:Insufficient
CVE-2005-2620	grpWise.exe for Novell GroupWise client 5.5 through 6.5.2 stores the password in plaintext in memory, which allows attackers to obtain the password using a debugger or another mechanism to read process memory.
	Comment: password in plaintext in memory
	Classification: Access control:Authentication:Plaintext credentials
CVE-2005-2750	Software Update in Mac OS X 10.4.2, when the user marks all updates to be ignored, exits without asking the user to reset the status of the updates, which could prevent important, security-relevant updates from being installed.
	Comment: updates marked as skipped can not be unskipped
	Classification: Processing:Insufficient cleanup
CVE-2005-2798	sshd in OpenSSH before 4.2, when GSSAPIDelegateCredentials is enabled, allows GSSAPI credentials to be delegated to clients who log in using non-GSSAPI methods, which could cause those credentials to be exposed to untrusted users or hosts.
	Comment: unsafe use/sharing of credentials.
	Classification: Access control:Authentication:Insufficient
CVE-2005-2915	ezconfig.asp in Linksys WRT54G router 3.01.03, 3.03.6, non-default configurations of 2.04.4, and possibly other versions, uses weak encryption (XOR encoding with a fixed byte mask) for configuration information, which could allow attackers to decrypt the information and possibly re-encrypt it in conjunction with CVE-2005-2914.
	Comment: fixed encryption key
	Classification: Encryption:Other weakness

Table 13: Vulnerabilities identified as design flaws

CVE name	Data
CVE-2005-3034	Compuware DriverStudio Remote Control service (DSRsvc.exe) 2.7 and 3.0 beta 2 allows remote attackers to bypass authentication via a null session.
	Comment: insufficient authentication
	Classification: Access control:Authentication:Insufficient
CVE-2005-3321	chkstat in SuSE Linux 9.0 through 10.0 allows local users to modify permissions of files by creating a hardlink to a file from a world-writable directory, which can cause the link count to drop to 1 when the file is deleted or replaced, which is then modified by chkstat to use weaker permissions.
	Comment: insufficient checks before changing permission. chkstat sets permissions according to a chosen security level.
	Classification: Access control:Authorization:Insecure permissions
CVE-2005-3344	The default installation of Horde 3.0.4 contains an administrative account with a blank password, which allows remote attackers to gain access.
	Comment: password not forced to be set during installation,
	Classification: Miscellaneous
CVE-2005-4589	Spb Kiosk Engine 1.0.0.1 stores the administrator's passcode in the registry in plaintext, which allows local users to obtain the passcode.
	Comment: clear text credentials without access control
	Classification: Access control:Authentication:Plaintext credentials
CVE-2005-4697	The Microsoft Wireless Zero Configuration system (WZCS) allows local users to access WEP keys and pair-wise Master Keys (PMK) of the WPA pre-shared key via certain calls to the WZCQueryInterface API function in wzcsapi.dll.
	Comment: credentials should be write only, no access control.
	Classification: Access control:Authorization:Insufficient
CVE-2006-0236	GUI display truncation vulnerability in Mozilla Thunderbird 1.0.2, 1.0.6, and 1.0.7 allows user-complicit attackers to execute arbitrary code via an attachment with a filename containing a large number of spaces ending with a dangerous extension that is not displayed by Thunderbird, along with an inconsistent Content-Type header, which could be used to trick a user into downloading dangerous content by dragging or saving the attachment.
	Comment: visual, real file extension hided by long filename
	Classification: Processing:Validation

D Vulnerabilities identified as maybe design flaws

Table 14: Vulnerabilities identified as maybe design flaws

CVE name	Data
CVE-1999-0290	The WinGate telnet proxy allows remote attackers to cause a denial of service via a large number of connections to localhost.
	Comment: no resource usage controll
	Classification:
CVE-1999-0348	IIS ASP caching problem releases sensitive information when two virtual servers share the same physical directory.
	Comment: no authorization to data access. sharing data between processes
	Classification:
CVE-1999-0366	In some cases, Service Pack 4 for Windows NT 4.0 can allow access to network shares using a blank password, through a problem with a null NT hash value.
	Comment: not updating all credentials
	Classification:
CVE-1999-0380	SLMail 3.1 and 3.2 allows local users to access any file in the NTFS file system when the Remote Administration Service (RAS) is enabled by setting a user's Finger File to point to the target file, then running finger on the user.
	Comment: no authorization or access controll. configuration
	Classification:
CVE-1999-0468	Internet Explorer 5.0 allows a remote server to read arbitrary files on the client's file system using the Microsoft Scriptlet Component.
	Comment: Probably not. It is possible to paste a file location into an upload scriptlet componen byIf you add '
	Classification:
CVE-1999-0471	The remote proxy server in Winroute allows a remote attacker to reconfigure the proxy without authentication through the "cancel" button.
	Comment: cancel gives you access
	Classification:
CVE-1999-0725	When IIS is run with a default language of Chinese, Korean, or Japanese, it allows a remote attacker to view the source code of certain files, a.k.a. "Double Byte Code Page".
	Comment: URL include one multibyte char at the end. File is decleared to not need processing because its extension doesn't match, multibyte is stripped, file is delivered sans processing.
	Classification:
CVE-1999-0979	The SCO UnixWare privileged process system allows local users to gain root privileges by using a debugger such as gdb to insert traps into _init before the privileged process is executed.
	Comment: not following recommended restrictions, allowing access from debuggers
	Classification:
CVE-1999-1171	IPswitch WS_FTP allows local users to gain additional privileges and modify or add mail accounts by setting the "flags" registry key to 1920.
	Comment: no local protection of acl in registry.
	Classification:

Table 14: Vulnerabilities identified as maybe design flaws

CVE name	Data
CVE-1999-1234	LSA (LSASS.EXE) in Windows NT 4.0 allows remote attackers to cause a denial of service via a NULL policy handle in a call to (1) SamrOpenDomain, (2) SamrEnumDomainUsers, and (3) SamrQueryDomainInfo.
	Comment: insufficient validation of badly-formed structures in the implementation of MSRPC samr unmarshalling (xforce). Other references implementation?
	Classification:
CVE-1999-1380	Symantec Norton Utilities 2.0 for Windows 95 marks the TUNEOCX.OCX ActiveX control as safe for scripting, which allows remote attackers to execute arbitrary commands via the run option through malicious web pages that are accessed by browsers such as Internet Explorer 3.0.
	Comment: no authorization, no cage.
	Classification:
CVE-1999-1413	Solaris 2.4 before kernel jumbo patch -35 allows set-gid programs to dump core even if the real user id is not in the set-gid group, which allows local users to overwrite or create files at higher privileges by causing a core dump, e.g. through dmesg.
	Comment:
	Classification:
CVE-1999-1538	When IIS 2 or 3 is upgraded to IIS 4, ism.dll is inadvertently left in /scripts/iisadmin, which does not restrict access to the local machine and allows an unauthorized user to gain access to sensitive server information, including the Administrator's password.
	Comment: not cleaning up properly after upgrade
	Classification:
CVE-1999-1549	Lynx 2.x does not properly distinguish between internal and external HTML, which may allow a local attacker to read a "secure" hidden form value from a temporary file and craft a LYNXOPTIONS: URL that causes Lynx to modify the user's configuration file and execute commands.
	Comment: validation based on web page's title
	Classification:
CVE-2000-0249	The AIX Fast Response Cache Accelerator (FRCA) allows local users to modify arbitrary files via the configuration capability in the frcactrl program.
	Comment: suid not checking access
	Classification:
CVE-2000-0353	Pine 4.x allows a remote attacker to execute arbitrary commands via an index.html file which executes lynx and obtains a uudecoded file from a malicious web server, which is then executed by Pine.
	Comment: probably other. input validation in metamail?
	Classification:
CVE-2000-0375	The kernel in FreeBSD 3.2 follows symbolic links when it creates core dump files, which allows local attackers to modify arbitrary files.
	Comment:
	Classification:
CVE-2000-0582	Check Point FireWall-1 4.0 and 4.1 allows remote attackers to cause a denial of service by sending a stream of invalid commands (such as binary zeros) to the SMTP Security Server proxy.
	Comment:
	Classification:
CVE-2000-0614	Tnef program in Linux systems allows remote attackers to overwrite arbitrary files via TNEF encoded compressed attachments which specify absolute path names for the decompressed output.
	Comment: no check or question if file already exist
	Classification:

Table 14: Vulnerabilities identified as maybe design flaws

CVE name	Data
CVE-2000-0716	WorldClient email client in MDaemon 2.8 includes the session ID in the referer field of an HTTP request when the user clicks on a URL, which allows the visited web site to hijcak the session ID and read the user's email.
	Comment: exposure of security credential
	Classification:
CVE-2000-0873	netstat in AIX 4.x.x does not properly restrict access to the -Zi option, which allows local users to clear network interface statistics and possibly hide evidence of unusual network activities.
	Comment:
	Classification:
CVE-2000-0958	HotJava Browser 3.0 allows remote attackers to access the DOM of a web page by opening a javascript: URL in a named window.
	Comment:
	Classification:
CVE-2000-1003	NETBIOS client in Windows 95 and Windows 98 allows a remote attacker to cause a denial of service by changing a file sharing service to return an unknown driver type, which causes the client to crash.
	Comment: not checking if driver is real
	Classification:
CVE-2000-1013	The setlocale function in FreeBSD 5.0 and earlier, and possibly other OSes, allows local users to read arbitrary files via the LANG environmental variable.
	Comment:
	Classification:
CVE-2000-1025	eWave ServletExec JSP/Java servlet engine, versions 3.0C and earlier, allows remote attackers to cause a denial of service via a URL that contains the "/servlet/" string, which invokes the ServletExec servlet and causes an exception if the servlet is already running.
	Comment: no access controll. Insufficient error check when binding to a socket.
	Classification:
CVE-2000-1215	The default configuration of Lotus Domino server 5.0.8 includes system information (version, operating system, and build date) in the HTTP headers of replies, which allows remote attackers to obtain sensitive information.
	Comment:
	Classification:
CVE-2000-1227	Windows NT 4.0 and Windows 2000 hosts allow remote attackers to cause a denial of service (unavailable connections) by sending multiple SMB SMBnegprots requests but not reading the response that is sent back.
	Comment:
	Classification:
CVE-2001-0004	IIS 5.0 and 4.0 allows remote attackers to read the source code for executable web server programs by appending "
	Comment: failure to check filetype before parsing.
	Classification:
CVE-2001-0465	TurboTax saves passwords in a temporary file when a user imports investment tax information from a financial institution, which could allow local users to obtain sensitive information.
	Comment:
	Classification:

Table 14: Vulnerabilities identified as maybe design flaws

CVE name	Data
CVE-2001-0712	The rendering engine in Internet Explorer determines the MIME type independently of the type that is specified by the server, which allows remote servers to automatically execute script which is placed in a file whose MIME type does not normally support scripting, such as text (.txt), JPEG (.jpg), etc.
	Comment: trying to recover from incorrect protocol. Ignoring protocol. trusting client/user/peer supplied data
	Classification:
CVE-2001-0766	Apache on MacOS X Client 10.0.3 with the HFS+ file system allows remote attackers to bypass access restrictions via a URL that contains some characters whose case is not matched by Apache's filters.
	Comment: Another implementation is vulnerable, but installation on a case sensitive file system is not.
	Classification:
CVE-2001-0942	dbsnmp in Oracle 8.1.6 and 8.1.7 uses the ORACLE_HOME environment variable to find and execute the dbsnmp program, which allows local users to execute arbitrary programs by pointing the ORACLE_HOME to an alternate directory that contains a malicious version of dbsnmp.
	Comment: Privileged program running code from user supplied directory
	Classification:
CVE-2001-1008	Java Plugin 1.4 for JRE 1.3 executes signed applets even if the certificate is expired, which could allow remote attackers to conduct unauthorized activities via an applet that has been signed by an expired certificate.
	Comment: is it only this spesific combination that fails?
	Classification:
CVE-2001-1064	Cisco 600 series routers running CBOS 2.0.1 through 2.4.2ap allows remote attackers to cause a denial of service via multiple connections to the router on the (1) HTTP or (2) telnet service, which causes the router to become unresponsive and stop forwarding packets.
	Comment: not limiting resources
	Classification:
CVE-2001-1322	xinetd 2.1.8 and earlier runs with a default umask of 0, which could allow local users to read or modify files that are created by an application that runs under xinetd but does not set its own safe umask.
	Comment: insecure default rights on files created. Distribution dependent? References talk of "some distributions vulnerable"
	Classification:
CVE-2001-1431	Nokia Firewall Appliances running IPSO 3.3 and VPN-1/FireWall-1 4.1 Service Pack 3, IPSO 3.4 and VPN-1/FireWall-1 4.1 Service Pack 4, and IPSO 3.4 or IPSO 3.4.1 and VPN-1/FireWall-1 4.1 Service Pack 5, when SYN Defender is configured in Active Gateway mode, does not properly rewrite the third packet of a TCP three-way handshake to use the NAT IP address, which allows remote attackers to gain sensitive information.
	Comment:
	Classification:
CVE-2001-1446	Find-By-Content in Mac OS X 10.0 through 10.0.4 creates world-readable index files named .FBCIndex in every directory, which allows remote attackers to learn the contents of files in web accessible directories.
	Comment:
	Classification:
CVE-2001-1459	OpenSSH 2.9 and earlier does not initiate a Pluggable Authentication Module (PAM) session if commands are executed with no pty, which allows local users to bypass resource limits (rlimits) set in pam.d.
	Comment: not initializing resources via all access paths
	Classification:

Table 14: Vulnerabilities identified as maybe design flaws

CVE name	Data
CVE-2001-1564	setrlimit in HP-UX 10.01, 10.10, 10.24, 10.20, 11.00, 11.04 and 11.11 does not properly enforce core file size on processes after setuid or setgid privileges are dropeed, which could allow local users to cause a denial of service by exhausting available disk space.
	Comment: Probably not. Checking rlimit when dumping core should be part of the design
	Classification:
CVE-2002-0129	efax 0.9 and earlier, when installed setuid root, allows local users to read arbitrary files via the -d option, which prints the contents of the file in a warning message.
	Comment: missing access control on file access, suid. suid root not needed?
	Classification:
CVE-2002-0153	Internet Explorer 5.1 for Macintosh allows remote attackers to bypass security checks and invoke local AppleScripts within a specific HTML element, aka the "Local Applescript Invocation" vulnerability.
	Comment: why isn't windows version affected, applescript? Allowing automatic execution of peer supplied commands in URL. no access control on file execution. trusting data from untrusted zone
	Classification:
CVE-2002-0190	Microsoft Internet Explorer 5.01, 5.5 and 6.0 allows remote attackers to execute arbitrary code under fewer security restrictions via a malformed web page that requires NetBIOS connectivity, aka "Zone Spoofing through Malformed Web Page" vulnerability.
	Comment: depends on what the malformed page does. no compartementalize.
	Classification:
CVE-2002-0344	Symantec LiveUpdate 1.5 and earlier in Norton Antivirus stores usernames and passwords for a local LiveUpdate server in cleartext in the registry, which may allow remote attackers to impersonate the LiveUpdate server.
	Comment: cleartext password registry, no protection of credentials
	Classification:
CVE-2002-0810	Bugzilla 2.14 before 2.14.2, and 2.16 before 2.16rc2, directs error messages from the syncshadowdb command to the HTML output, which could leak sensitive information, including plaintext passwords, if syncshadowdb fails.
	Comment: revealing too much information in error messages
	Classification:
CVE-2002-0978	Microsoft File Transfer Manager (FTM) ActiveX control before 4.0 allows remote attackers to upload or download arbitrary files to arbitrary locations via a man-in-the-middle attack with modified TGT and TGN parameters in a call to the "Persist" function.
	Comment: unsure of the nature of flaw. no authorization of data. trusting peer supplied data.
	Classification:
CVE-2002-1016	Adobe eBook Reader allows a user to bypass restrictions for copy, print, lend, and give operations by backing up key data files, performing the operations, and restoring the original data files.
	Comment: insufficient access control, insufficient restrictions. trust in client supplied data? Impossible to prevent?
	Classification:

Table 14: Vulnerabilities identified as maybe design flaws

CVE name	Data
CVE-2002-1937	Symantec Firewall/VPN Appliance 100 through 200R hardcodes the administrator's MAC address inside the firewall's configuration, which allows remote attackers to spoof the administrator's MAC address and perform an ARP poisoning man-in-the-middle attack to obtain the administrator's password.
	Comment: no encrypted communication
	Classification:
CVE-2003-0066	The rxvt terminal emulator 2.7.8 and earlier allows attackers to modify the window title via a certain character escape sequence and then insert it back to the command line in the user's terminal, e.g. when the user views a file containing the malicious sequence, which could allow the attacker to execute arbitrary commands.
	Comment: no sanitizing of input(output?) data
	Classification:
CVE-2003-0189	The authentication module for Apache 2.0.40 through 2.0.45 on Unix does not properly handle threads safely when using the crypt_r or crypt functions, which allows remote attackers to cause a denial of service (failed Basic authentication with valid usernames and passwords) when a threaded MPM is used.
	Comment:
	Classification:
CVE-2003-0226	Microsoft Internet Information Services (IIS) 5.0 and 5.1 allows remote attackers to cause a denial of service via a long WebDAV request with a (1) PROPFIND or (2) SEARCH method, which generates an error condition that is not properly handled.
	Comment: probably buffer overflow?
	Classification:
CVE-2003-0447	The Custom HTTP Errors capability in Internet Explorer 5.01, 5.5 and 6.0 allows remote attackers to execute script in the Local Zone via an argument to shdocvw.dll that causes a "javascript:" link to be generated.
	Comment:
	Classification:
CVE-2003-0567	Cisco IOS 11.x and 12.0 through 12.2 allows remote attackers to cause a denial of service (traffic block) by sending a particular sequence of IPv4 packets to an interface on the device, causing the input queue on that interface to be marked as full.
	Comment:
	Classification:
CVE-2003-0740	Stunnel 4.00, and 3.24 and earlier, leaks a privileged file descriptor returned by listen(), which allows local users to hijack the Stunnel server.
	Comment: probably not. Too detailed. API misuse?
	Classification:
CVE-2003-1124	Unknown vulnerability in Sun Management Center (SunMC) 2.1.1, 3.0, and 3.0 Revenue Release (RR), when installed and run by root, allows local users to create or modify arbitrary files.
	Comment: SUID, files with writeable directories
	Classification:
CVE-2004-0134	cpr (libcpr) in SGI IRIX before 6.5.25 allows local users to gain privileges by loading a user provided library while restarting the checkpointed process.
	Comment: executing user provided code.
	Classification:

Table 14: Vulnerabilities identified as maybe design flaws

CVE name	Data
CVE-2004-0395	The xatitv program in the gatos package does not properly drop root privileges when the configuration file does not exist, which allows local users to execute arbitrary commands via shell metacharacters in a system call.
	Comment: SUID input validation?
	Classification:
CVE-2004-0609	rssh 2.0 through 2.1.x expands command line arguments before entering a chroot jail, which allows remote authenticated users to determine the existence of files in a directory outside the jail.
	Comment:
	Classification:
CVE-2004-0621	admin.php in Newsletter ZWS allows remote attackers to gain administrative privileges via a list_user operation with the ulevel parameter set to 1 (administrator level), which lists all users and their passwords.
	Comment: can be design if the ulevel argument is meant to be there, else it probably is implementation if programmed with register_globals=on.
	Classification:
CVE-2004-0685	Certain USB drivers in the Linux 2.4 kernel use the copy_to_user function on uninitialized structures, which could allow local users to obtain sensitive information by reading memory that was not cleared from previous usage.
	Comment: missing memset to clear memory before use.
	Classification:
CVE-2004-0704	Unknown vulnerability in (1) duplicates.cgi and (2) buglist.cgi in Bugzilla 2.16.x before 2.16.6, 2.18 before 2.18rc1, when configured to hide products, allows remote attackers to view hidden products.
	Comment: Variable not checked for products you have access to. All products are displayed.
	Classification:
CVE-2004-0894	LSASS (Local Security Authority Subsystem Service) of Windows 2000 Server and Windows Server 2003 does not properly validate connection information, which allows local users to gain privileges via a specially-designed program.
	Comment:
	Classification:
CVE-2004-0909	Mozilla Firefox before the Preview Release, Mozilla before 1.7.3, and Thunderbird before 0.8 may allow remote attackers to trick users into performing unexpected actions, including installing software, via signed scripts that request enhanced abilities using the enablePrivilege parameter, then modify the meaning of certain security-relevant dialog messages.
	Comment: visual, attacker able to produce text in dialog box
	Classification:
CVE-2004-1116	The init scripts in Great Internet Mersenne Prime Search (GIMPS) 23.9 and earlier execute user-owned programs with root privileges, which allows local users to gain privileges by modifying the programs.
	Comment: probably not. Distribution spesific
	Classification:
CVE-2004-1144	Unknown vulnerability in the 32bit emulation code in Linux 2.4 on AMD64 systems allows local users to gain privileges.
	Comment: missing return value check?
	Classification:
CVE-2004-1296	The (1) eqn2graph and (2) pic2graph scripts in groff 1.18.1 allow local users to overwrite arbitrary files via a symlink attack on temporary files.
	Comment: race condition?
	Classification:

Table 14: Vulnerabilities identified as maybe design flaws

CVE name	Data
CVE-2004-1557	MyWebServer 1.0.3 allows remote attackers to bypass authentication, modify configuration, and read arbitrary files via a direct HTTP request to (1) /admin or (2) ServerProperties.html.
	Comment: no authentication.can be fixed by configuring authentication on web server?
	Classification:
CVE-2004-2006	Trend Micro OfficeScan 3.0 - 6.0 has default permissions of "Everyone Full Control" on the installation directory and registry keys, which allows local users to disable virus protection.
	Comment: setting more restricted ACL's removes some functionality - ability to see which pattern file is installed, or to run a manual scan of PC
	Classification:
CVE-2004-2068	fetchnews in leafnode 1.9.47 and earlier allows remote attackers to cause a denial of service (process hang) via an emptry NNTP news article with missing mandatory headers.
	Comment: no timeout
	Classification:
CVE-2004-2638	The Admin Access With Levels plugin in osCommerce 1.5.1 allows remote attackers to access files in the "admin/" directory by modifying the in_login parameter to a non-zero value.
	Comment:
	Classification:
CVE-2005-0035	The Acrobat web control in Adobe Acrobat and Acrobat Reader 7.0 and earlier, when used with Internet Explorer, allows remote attackers to determine the existence of arbitrary files via the LoadFile ActiveX method.
	Comment: different response depending on existens/non-existence of file
	Classification:
CVE-2005-0148	Thunderbird before 0.9, when running on Windows systems, uses the default handler when processing javascript: links, which invokes Internet Explorer and may expose the Thunderbird user to vulnerabilities in the version of Internet Explorer that is installed on the user's system. NOTE: since the invocation between multiple products is a common practice, and the vulnerabilities inherent in multi-product interactions are not easily enumerable, this issue might be REJECTED in the future.
	Comment: does not use default handler for URLs. insecure default configuration?
	Classification:
CVE-2005-0440	ELOG before 2.5.7 allows remote attackers to bypass authentication and download a configuration file that contains a sensitive write password via a modified URL.
	Comment: no authentication before download
	Classification:
CVE-2005-1002	logwebftbs2000.exe in Logics Software File Transfer (LOG-FT) allows remote attackers to read arbitrary files via modified (1) VAR_FT_LANG and (2) VAR_FT_TMPL parameters.
	Comment:
	Classification:
CVE-2005-1220	Shoutbox SCRIPT 3.0.2 and earlier allows remote attackers to obtain sensitive information via a direct request to db/settings.dat, which displays usernames and password hashes.
	Comment:
	Classification:

Table 14: Vulnerabilities identified as maybe design flaws

CVE name	Data
CVE-2005-1383	The OHS component 1.0.2 through 10.x, when UseWebcacheIP is disabled, in Oracle Application Server allows remote attackers to bypass HTTP Server mod_access restrictions via a request to the webcache TCP port 7778.
	Comment: authorization, all access paths are not checked. There is no information on whether the UseWebCacheIP has always been there or have just been added.
	Classification:
CVE-2005-1522	The imap4d server for GNU Mailutils 0.5 and 0.6, and other versions before 0.6.90, allows authenticated remote users to cause a denial of service (CPU consumption) via a large range value in the FETCH command.
	Comment: maximum range should be checked against real maximum value
	Classification:
CVE-2005-1604	PHP Advanced Transfer Manager (phpATM) 1.21 allows remote attackers to upload arbitrary files via filenames containing multiple file extensions, as demonstrated using a filename ending in "php.ns", which allows execution of arbitrary PHP code.
	Comment: possible to execute uploaded programs
	Classification:
CVE-2005-1616	viewforum.php in Ultimate PHP Board (UPB) 1.8 through 1.9.6 allows remote attackers to obtain sensitive information via an invalid (1) id or possibly (2) postorder parameter, which reveals the path in an error message when a file can not be opened.
	Comment:
	Classification:
CVE-2005-1647	Gurgens (GASoft) Guest Book 2.1 stores the db/Genid.dat database file under the web document root with insufficient access control, which allows remote attackers to obtain and decrypt usernames and passwords.
	Comment:
	Classification:
CVE-2005-1650	The web mail service in Woppoware PostMaster 4.2.2 (build 3.2.5) generates different error messages depending on whether a user exists or not, which allows remote attackers to determine valid usernames.
	Comment:
	Classification:
CVE-2005-2211	Backup Manager 0.5.8a creates temporary files insecurely, which allows local users to conduct unauthorized file operations when a user is burning a CDR.
	Comment: SUID? temporary files
	Classification:
CVE-2005-2843	Helpdesk software Hesk 0.92 does not properly verify usernames and passwords, which allows remote attackers to bypass authentication via a direct request to admin_main.php.
	Comment:
	Classification:
CVE-2005-3177	CHKDSK in Microsoft Windows 2000 before Update Rollup 1 for SP4, Windows XP, and Windows Server 2003, when running in fix mode, does not properly handle security descriptors if the master file table contains a large number of files or if the descriptors do not satisfy certain NTFS conventions, which could cause ACLs for some files to be reverted to less secure defaults, or cause security descriptors to be removed.
	Comment: miscalculation? Variable type?
	Classification:

Table 14: Vulnerabilities identified as maybe design flaws

CVE name	Data
CVE-2005-3434	Archilles Newsworld before 1.5.0-rc1 stores (1) account.nwd and (2) session.nwd under the web root with insufficient access control, which allows remote attackers to obtain sensitive information such as usernames, hashed passwords, and session IDs, and gain privileges.
	Comment:
	Classification:
CVE-2005-3899	The automatic update feature in Google Talk allows remote attackers to cause a denial of service (CPU and memory consumption) by poisoning a target's DNS cache and causing a large update file to be sent, which consumes large amounts of CPU and memory during the signature verification, aka BenjiBug.
	Comment: no server identification?
	Classification:
CVE-2005-4013	PHP Web Statistik 1.4 stores the stat.cfg file under the web root with insufficient access control, which allows remote attackers to obtain sensitive information such as statistics and the log directory location, possibly including the logdb.dta file.
	Comment:
	Classification:
CVE-2005-4690	Six Apart Movable Type 3.16 allows local users with blog-creation privileges to create or overwrite arbitrary files of certain types (such as HTML and image files) by selecting an arbitrary directory as a blog's top-level directory. NOTE: this issue can be used in conjunction with CVE-2005-3102 to create or overwrite arbitrary files of all types.
	Comment:
	Classification:
CVE-2006-0153	427BB 2.2 and 2.2.1 verifies authentication credentials based on the username, authenticated, and usertype cookies, which allows remote attackers to bypass authentication by using a valid username and usertype and setting the authenticated cookie.
	Comment:
	Classification:

E Vulnerabilities identified as not design flaws

Table 15: Vulnerabilities identified as other type of flaws

CVE name	Data
CVE-1999-0015	Teardrop IP denial of service.
	Comment: calculating the size of buffer to hold fragments
CVE-1999-0049	Csetup under IRIX allows arbitrary file creation or overwriting.
	Comment: no check of access control if specified DEBUG file already exist
CVE-1999-0236	ScriptAlias directory in NCSA and Apache httpd allowed attackers to read CGI programs.
CVE-1999-0278	In IIS, remote attackers can obtain source code for ASP files by appending "::$DATA" to the URL.
CVE-1999-0281	Denial of service in IIS using long URLs.
CVE-1999-0289	The Apache web server for Win32 may provide access to restricted files when a . (dot) is appended to a requested URL.
CVE-1999-0462	suidperl in Linux Perl does not check the nosuid mount option on file systems, allowing local users to gain root access by placing a setuid script in a mountable file system, e.g. a CD-ROM or floppy disk.
	Comment: buffer overflow
CVE-1999-0501	A Unix account has a guessable password.
	Comment: default password
CVE-1999-0518	A NETBIOS/SMB share password is guessable.
CVE-1999-0582	A Windows NT account policy has inappropriate, security-critical settings for lockout, e.g. lockout duration, lockout after bad logon attempts, etc.
CVE-1999-0606	An incorrect configuration of the EZMall 2000 shopping cart CGI program "mall2000.cgi" could disclose private information.
	Comment: files created/data stored in insecure location (web area?). Can be configured?
CVE-1999-0627	The rexd service is running, which uses weak authentication that can allow an attacker to execute commands.
CVE-1999-0692	The default configuration of the Array Services daemon (arrayd) disables authentication, allowing remote users to gain root privileges.
CVE-1999-0695	The Sybase PowerDynamo personal web server allows attackers to read arbitrary files through a .. (dot dot) attack.
CVE-1999-0706	Linux xmonisdn package allows local users to gain root privileges by modifying the IFS or PATH environmental variables.
CVE-1999-0771	The web components of Compaq Management Agents and the Compaq Survey Utility allow a remote attacker to read arbitrary files via a .. (dot dot) attack.
CVE-1999-0788	Arkiea nlservd allows remote attackers to conduct a denial of service.
CVE-1999-0828	UnixWare pkg commands such as pkginfo, pkgcat, and pkgparam allow local users to read arbitrary files via the dacread permission.
CVE-1999-0835	Denial of service in BIND named via malformed SIG records.
CVE-1999-0844	Denial of service in MDaemon WorldClient and WebConfig services via a long URL.
CVE-1999-0846	Denial of service in MDaemon 2.7 via a large number of connection attempts.
CVE-1999-0849	Denial of service in BIND named via maxdname.
CVE-1999-0890	iHTML Merchant allows remote attackers to obtain sensitive information or execute commands via a code parsing error.

Table 15: Vulnerabilities identified as other type of flaws

CVE name	Data
CVE-1999-0919	A memory leak in a Motorola CableRouter allows remote attackers to conduct a denial of service via a large number of telnet connections.
CVE-1999-0929	Novell NetWare with Novell-HTTP-Server or YAWN web servers allows remote attackers to conduct a denial of service via a large number of HTTP GET requests.
CVE-1999-0933	TeamTrack web server allows remote attackers to read arbitrary files via a .. (dot dot) attack.
CVE-1999-0947	AN-HTTPd provides example CGI scripts test.bat, input.bat, input2.bat, and envout.bat, which allow remote attackers to execute commands via shell metacharacters.
CVE-1999-1053	guestbook.pl cleanses user-inserted SSI commands by removing text between "<!–" and "–>" separators, which allows remote attackers to execute arbitrary commands when guestbook.pl is run on Apache 1.3.9 and possibly other versions, since Apache allows other closing sequences besides "–>".
CVE-1999-1108	** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-1999-1107. Reason: This candidate is a duplicate of CVE-1999-1107. Notes: All CVE users should reference CVE-1999-1107 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.
CVE-1999-1180	O'Reilly WebSite 1.1e and Website Pro 2.0 allows remote attackers to execute arbitrary commands via shell metacharacters in an argument to (1) args.cmd or (2) args.bat.
CVE-1999-1226	Netscape Communicator 4.7 and earlier allows remote attackers to cause a denial of service, and possibly execute arbitrary commands, via a long certificate key.
CVE-1999-1249	movemail in HP-UX 10.20 has insecure permissions, which allows local users to gain privileges.
CVE-1999-1308	Certain programs in HP-UX 10.20 do not properly handle large user IDs (UID) or group IDs (GID) over 60000, which could allow local users to gain privileges.
CVE-1999-1331	netcfg 2.16-1 in Red Hat Linux 4.2 allows the Ethernet interface to be controlled by users on reboot when an option is set, which allows local users to cause a denial of service by shutting down the interface.
CVE-1999-1387	Windows NT 4.0 SP2 allows remote attackers to cause a denial of service (crash), possibly via malformed inputs or packets, such as those generated by a Linux smbmount command that was compiled on the Linux 2.0.29 kernel but executed on Linux 2.0.25.
CVE-1999-1422	The default configuration of Slackware 3.4, and possibly other versions, includes . (dot, the current directory) in the PATH environmental variable, which could allow local users to create Trojan horse programs that are inadvertently executed by other users.
CVE-1999-1490	xosview 1.5.1 in Red Hat 5.1 allows local users to gain root access via a long HOME environmental variable.
CVE-1999-1573	Multiple unknown vulnerabilities in the "r-cmnds" (1) remshd, (2) rexecd, (3) rlogind, (4) rlogin, (5) remsh, (6) rcp, (7) rexec, and (8) rdist for HP-UX 10.00 through 11.00 allow attackers to gain privileges or access files.
CVE-1999-1581	Memory leak in Simple Network Management Protocol (SNMP) agent (snmp.exe) for Windows NT 4.0 before Service Pack 4 allows remote attackers to cause a denial of service (memory consumption) via a large number of SNMP packets with Object Identifiers (OIDs) that cannot be decoded.

Table 15: Vulnerabilities identified as other type of flaws

CVE name	Data
CVE-2000-0009	The bna_pass program in Optivity NETarchitect uses the PATH environmental variable for finding the "rm" program, which allows local users to execute arbitrary commands.
	Comment: suid,
CVE-2000-0024	IIS does not properly canonicalize URLs, potentially allowing remote attackers to bypass access restrictions in third-party software via escape characters, aka the "Escape Character Parsing" vulnerability.
CVE-2000-0033	InterScan VirusWall SMTP scanner does not properly scan messages with malformed attachments.
CVE-2000-0056	IMail IMONITOR status.cgi CGI script allows remote attackers to cause a denial of service with many calls to status.cgi.
CVE-2000-0073	Buffer overflow in Microsoft Rich Text Format (RTF) reader allows attackers to cause a denial of service via a malformed control word.
CVE-2000-0149	Zeus web server allows remote attackers to view the source code for CGI programs via a null character (
CVE-2000-0174	StarOffice StarScheduler web server allows remote attackers to read arbitrary files via a .. (dot dot) attack.
CVE-2000-0185	RealMedia RealServer reveals the real IP address of a Real Server, even if the address is supposed to be private.
CVE-2000-0207	SGI InfoSearch CGI program infosrch.cgi allows remote attackers to execute commands via shell metacharacters.
CVE-2000-0212	InterAccess TelnetID Server 4.0 allows remote attackers to conduct a denial of service via malformed terminal client configuration information.
CVE-2000-0213	The Sambar server includes batch files ECHO.BAT and HELLO.BAT in the CGI directory, which allow remote attackers to execute commands via shell metacharacters.
CVE-2000-0259	The default permissions for the Cryptography\Offload registry key used by the OffloadModExpo in Windows NT 4.0 allows local users to obtain compromise the cryptographic keys of other users.
CVE-2000-0264	Panda Security 3.0 with registry editing disabled allows users to edit the registry and gain privileges by directly executing a .reg file or using other methods.
CVE-2000-0274	The Linux trustees kernel patch allows attackers to cause a denial of service by accessing a file or directory with a long name.
CVE-2000-0314	traceroute in NetBSD 1.3.3 and Linux systems allows local users to flood other systems by providing traceroute with a large waittime (-w) option, which is not parsed properly and sets the time delay for sending packets to zero.
CVE-2000-0319	mail.local in Sendmail 8.10.x does not properly identify the .\n string which identifies the end of message text, which allows a remote attacker to cause a denial of service or corrupt mailboxes via a message line that is 2047 characters long and ends in .\n.
CVE-2000-0338	Concurrent Versions Software (CVS) uses predictable temporary file names for locking, which allows local users to cause a denial of service by creating the lock directory before it is created for use by a legitimate CVS user.
CVE-2000-0344	The knfsd NFS server in Linux kernel 2.2.x allows remote attackers to cause a denial of service via a negative size value.
CVE-2000-0365	Red Hat Linux 6.0 installs the /dev/pts file system with insecure modes, which allows local users to write to other tty devices.
CVE-2000-0393	The KDE kscd program does not drop privileges when executing a program specified in a user's SHELL environmental variable, which allows the user to gain privileges by specifying an alternate program to execute.
	Comment: sguid, some distributions distribute without sguid.

Table 15: Vulnerabilities identified as other type of flaws

CVE name	Data
CVE-2000-0421	The process_bug.cgi script in Bugzilla allows remote attackers to execute arbitrary commands via shell metacharacters.
CVE-2000-0424	The CGI counter 4.0.7 by George Burgyan allows remote attackers to execute arbitrary commands via shell metacharacters.
CVE-2000-0431	Cobalt RaQ2 and RaQ3 does not properly set the access permissions and ownership for files that are uploaded via FrontPage, which allows attackers to bypass cgiwrap and modify files.
CVE-2000-0470	Allegro RomPager HTTP server allows remote attackers to cause a denial of service via a malformed authentication request.
CVE-2000-0497	IBM WebSphere server 3.0.2 allows a remote attacker to view source code of a JSP program by requesting a URL which provides the JSP extension in upper case.
	Comment: NTFS is case-insensitive, but WebSphere configuration is. Add JSP to WebSphere config
CVE-2000-0513	CUPS (Common Unix Printing System) 1.04 and earlier allows remote attackers to cause a denial of service by authenticating with a user name that does not exist or does not have a shadow password.
CVE-2000-0524	Microsoft Outlook and Outlook Express allow remote attackers to cause a denial of service by sending email messages with blank fields such as BCC, Reply-To, Return-Path, or From.
CVE-2000-0528	Net Tools PKI Server does not properly restrict access to remote attackers when the XUDA template files do not contain absolute pathnames for other files.
CVE-2000-0576	Oracle Web Listener for AIX versions 4.0.7.0.0 and 4.0.8.1.0 allows remote attackers to cause a denial of service via a malformed URL.
CVE-2000-0634	The web administration interface for CommuniGate Pro 3.2.5 and earlier allows remote attackers to read arbitrary files via a .. (dot dot) attack.
CVE-2000-0660	The WDaemon web server for WorldClient 2.1 allows remote attackers to read arbitrary files via a .. (dot dot) attack.
CVE-2000-0661	WircSrv IRC Server 5.07s allows remote attackers to cause a denial of service via a long string to the server port.
CVE-2000-0664	AnalogX SimpleServer:WWW 1.06 and earlier allows remote attackers to read arbitrary files via a modified .. (dot dot) attack that uses the
CVE-2000-0670	The cvsweb CGI script in CVSWeb 1.80 allows remote attackers with write access to a CVS repository to execute arbitrary commands via shell metacharacters.
CVE-2000-0693	pgxconfig in the Raptor GFX configuration tool uses a relative path name for a system call to the "cp" program, which allows local users to execute arbitrary commands by modifying their path to point to an alternate "cp" program.
	Comment: use of system without full path.
CVE-2000-0697	The administration interface for the dwhttpd web server in Solaris AnswerBook2 allows interface users to remotely execute commands via shell metacharacters.
CVE-2000-0705	ntop running in web mode allows remote attackers to read arbitrary files via a .. (dot dot) attack.
CVE-2000-0732	Worm HTTP server allows remote attackers to cause a denial of service via a long URL.
CVE-2000-0734	eEye IRIS 1.01 beta allows remote attackers to cause a denial of service via a large number of UDP connections.
CVE-2000-0837	FTP Serv-U 2.5e allows remote attackers to cause a denial of service by sending a large number of null bytes.
CVE-2000-1019	Search engine in Ultraseek 3.1 and 3.1.10 (aka Inktomi Search) allows remote attackers to cause a denial of service via a malformed URL.

Table 15: Vulnerabilities identified as other type of flaws

CVE name	Data
CVE-2000-1050	Allaire JRun 3.0 http servlet server allows remote attackers to directly access the WEB-INF directory via a URL request that contains an extra "/" in the beginning of the request (aka the "extra leading slash").
CVE-2000-1066	The getnameinfo function in FreeBSD 4.1.1 and earlier, and possibly other operating systems, allows a remote attacker to cause a denial of service via a long DNS hostname.
CVE-2000-1073	csstart program in iCal 2.1 Patch 2 searches for the cshttpd program in the current working directory, which allows local users to gain root privileges by creating a Trojan Horse cshttpd program in a directory and calling csstart from that directory.
CVE-2000-1083	The xp_showcolv function in SQL Server and Microsoft SQL Server Desktop Engine (MSDE) does not properly restrict the length of a buffer before calling the srv_paraminfo function in the SQL Server API for Extended Stored Procedures (XP), which allows an attacker to cause a denial of service or execute arbitrary commands, aka the "Extended Stored Procedure Parameter Parsing" vulnerability.
CVE-2000-1151	Baxter IRC client in BeOS r5 pro and earlier allows remote attackers to conduct a denial of service via a message that contains a long URL.
CVE-2000-1153	PostMaster 1.0 in BeOS r5 pro and earlier allows remote attackers to conduct a denial of service via a message that contains a long URL.
CVE-2000-1168	IBM HTTP Server 1.3.6 (based on Apache) allows remote attackers to cause a denial of service and possibly execute arbitrary commands via a long GET request.
CVE-2001-0017	Memory leak in PPTP server in Windows NT 4.0 allows remote attackers to cause a denial of service via a malformed data packet, aka the "Malformed PPTP Packet Stream" vulnerability.
CVE-2001-0024	simplestmail.cgi CGI program by Leif Wright allows remote attackers to execute arbitrary commands via shell metacharacters in the MyEmail parameter.
CVE-2001-0040	APC UPS daemon, apcupsd, saves its process ID in a world-writable file, which allows local users to kill an arbitrary process by specifying the target process ID in the apcupsd.pid file.
CVE-2001-0051	IBM DB2 Universal Database version 6.1 creates an account with a default user name and password, which allows remote attackers to gain access to the databasse.
	Comment: password not changed
CVE-2001-0066	Secure Locate (slocate) allows local users to corrupt memory via a malformed database file that specifies an offset value that accesses memory outside of the intended buffer.
CVE-2001-0083	Windows Media Unicast Service in Windows Media Services 4.0 and 4.1 does not properly shut down some types of connections, producing a memory leak that allows remote attackers to cause a denial of service via a series of severed connections, aka the "Severed Windows Media Server Connection" vulnerability.
CVE-2001-0087	itetris/xitetris 1.6.2 and earlier trusts the PATH environmental variable to find and execute the gunzip program, which allows local users to gain root privileges by changing their PATH so that it points to a malicious gunzip program.
CVE-2001-0088	common.inc.php in phpWebLog 0.4.2 does not properly initialize the $CONF array, which inadvertently sets the password to a single character, allowing remote attackers to easily guess the SiteKey and gain administrative privileges to phpWebLog.
CVE-2001-0151	IIS 5.0 allows remote attackers to cause a denial of service via a series of malformed WebDAV requests.

Table 15: Vulnerabilities identified as other type of flaws

CVE name	Data
CVE-2001-0166	Macromedia Shockwave Flash plugin version 8 and earlier allows remote attackers to cause a denial of service via malformed tag length specifiers in a SWF file.
CVE-2001-0170	glibc 2.1.9x and earlier does not properly clear the RESOLV_HOST_CONF, HOSTALIASES, or RES_OPTIONS environmental variables when executing setuid/setgid programs, which could allow local users to read arbitrary files.
	Comment: missing comma
CVE-2001-0189	Directory traversal vulnerability in LocalWEB2000 HTTP server allows remote attackers to read arbitrary commands via a .. (dot dot) attack in an HTTP GET request.
CVE-2001-0231	Directory traversal vulnerability in newsdesk.cgi in News Desk 1.2 allows remote attackers to read arbitrary files via a .. in the "t" parameter.
CVE-2001-0239	Microsoft Internet Security and Acceleration (ISA) Server 2000 Web Proxy allows remote attackers to cause a denial of service via a long web request with a specific type.
CVE-2001-0263	Gene6 G6 FTP Server 2.0 (aka BPFTP Server 2.10) allows attackers to read file attributes outside of the web root via the (1) SIZE and (2) MDTM commands when the "show relative paths" option is not enabled.
CVE-2001-0275	Moby Netsuite Web Server 1.02 allows remote attackers to cause a denial of service, and possibly execute arbitrary commands, via a long HTTP request.
CVE-2001-0346	Handle leak in Microsoft Windows 2000 telnet service allows attackers to cause a denial of service by starting a large number of sessions and terminating them.
CVE-2001-0365	Eudora before 5.1 allows a remote attacker to execute arbitrary code, when the 'Use Microsoft Viewer' and 'allow executables in HTML content' options are enabled, via an HTML email message containing Javascript, with ActiveX controls and malicious code within IMG tags.
CVE-2001-0441	Buffer overflow in (1) wrapping and (2) unwrapping functions of slrn news reader before 0.9.7.0 allows remote attackers to execute arbitrary commands via a long message header.
CVE-2001-0457	man2html before 1.5-22 allows remote attackers to cause a denial of service (memory exhaustion).
CVE-2001-0483	Configuration error in Axent Raptor Firewall 6.5 allows remote attackers to use the firewall as a proxy to access internal web resources when the http.noproxy Rule is not set.
CVE-2001-0498	Transparent Network Substrate (TNS) over Net8 (SQLNet) in Oracle 8i 8.1.7 and earlier allows remote attackers to cause a denial of service via a malformed SQLNet connection request with a large offset in the header extension.
CVE-2001-0545	IIS 4.0 with URL redirection enabled allows remote attackers to cause a denial of service (crash) via a malformed request that specifies a length that is different than the actual length.
CVE-2001-0563	ElectroSystems Engineering Inc. ElectroComm 2.0 and earlier allows a remote attacker to create a denial of service via large (> 160000 character) strings sent to port 23.
CVE-2001-0602	Lotus Domino R5 prior to 5.0.7 allows a remote attacker to create a denial of service via repeated (>400) URL requests for DOS devices.
CVE-2001-0694	Directory traversal vulnerability in WFTPD 3.00 R5 allows a remote attacker to view arbitrary files via a dot dot attack in the CD command.
CVE-2001-0912	Packaging error for expect 8.3.3 in Mandrake Linux 8.1 causes expect to search for its libraries in the /home/snailtalk directory before other directories, which could allow a local user to gain root privileges.

Table 15: Vulnerabilities identified as other type of flaws

CVE name	Data
CVE-2001-1002	The default configuration of the DVI print filter (dvips) in Red Hat Linux 7.0 and earlier does not run dvips in secure mode when dvips is executed by lpd, which could allow remote attackers to gain privileges by printing a DVI file that contains malicious commands.
CVE-2001-1044	Basilix Webmail 0.9.7beta, and possibly other versions, stores *.class and *.inc files under the document root and does not restrict access, which could allows remote attackers to obtain sensitive information such as MySQL passwords and usernames from the mysql.class file.
CVE-2001-1122	Windows NT 4.0 SP 6a allows a local user with write access to winnt/system32 to cause a denial of service (crash in lsass.exe) by running the NT4ALL exploit program in 'SPECIAL' mode.
	Comment: users don't have write access to winnt/system by default.
CVE-2001-1158	Check Point VPN-1/FireWall-1 4.1 base.def contains a default macro, accept_fw1_rdp, which can allow remote attackers to bypass intended restrictions with forged RDP (internal protocol) headers to UDP port 259 of arbitrary hosts.
CVE-2001-1183	PPTP implementation in Cisco IOS 12.1 and 12.2 allows remote attackers to cause a denial of service (crash) via a malformed packet.
CVE-2001-1273	The "mxcsr P4" vulnerability in the Linux kernel before 2.2.17-14, when running on certain Intel CPUs, allows local users to cause a denial of service (system halt).
CVE-2001-1417	AOL Instant Messenger (AIM) 4.7 allows remote attackers to cause a denial of service (application hang or crash) via a buddy icon GIF file whose length and width values are larger than the actual image data.
CVE-2001-1421	AOL Instant Messenger (AIM) 4.7 and earlier allows remote attackers to cause a denial of service (application crash) via a large number of different fonts followed by an HTML HR tag.
CVE-2001-1426	Alcatel Speed Touch running firmware KHDSAA.108 and KHDSAA.132 through KHDSAA.134 has a TFTP server running without a password, which allows remote attackers to change firmware versions or the device's configurations.
CVE-2001-1438	Handspring Visor 1.0 and 1.0.1 with the VisorPhone Springboard module installed allows remote attackers to cause a denial of service (PalmOS crash and VisorPhone database corruption) by sending a large or crafted SMS image.
CVE-2001-1552	ssdpsrv.exe in Windows ME allows remote attackers to cause a denial of service by sending multiple newlines in a Simple Service Discovery Protocol (SSDP) message. NOTE: multiple replies to the original post state that the problem could not be reproduced.
CVE-2002-0036	Integer signedness error in MIT Kerberos V5 ASN.1 decoder before krb5 1.2.5 allows remote attackers to cause a denial of service via a large unsigned data element length, which is later used as a negative value.
CVE-2002-0142	CGI handler in John Roy Pi3Web for Windows 2.0 beta 1 and 2 allows remote attackers to cause a denial of service (crash) via a series of requests whose physical path is exactly 260 characters long and ends in a series of . (dot) characters.
CVE-2002-0254	ICQ 2001b Build 3659 allows remote attackers to cause a denial of service (crash) via a malformed picture that contains large height and width values, which causes the crash when viewed in Userdetails.
CVE-2002-0291	Dino's Webserver 1.2 allows remote attackers to cause a denial of service (CPU consumption) and possibly execute arbitrary code via several large HTTP requests within a short time.
CVE-2002-0293	FTP service in Alcatel OmniPCX 4400 allows the "halt" user to gain root privileges by modifying root's .profile file.

Table 15: Vulnerabilities identified as other type of flaws

CVE name	Data
CVE-2002-0294	Alcatel 4400 installs the /chetc/shutdown command with setgid privileges, which allows many different local users to shut down the system.
CVE-2002-0358	MediaMail and MediaMail Pro in SGI IRIX 6.5.16 and earlier allows local users to force the program to dump core via certain arguments, which could allow the users to read sensitive data or gain privileges.
CVE-2002-0400	ISC BIND 9 before 9.2.1 allows remote attackers to cause a denial of service (shutdown) via a malformed DNS packet that triggers an error condition that is not properly handled when the rdataset parameter to the dns_message_findtype() function in message.c is not NULL.
CVE-2002-0465	Directory traversal vulnerability in filemanager.asp for Hosting Controller 1.4.1 and earlier allows remote attackers to read and modify arbitrary files, and execute commands, via a .. (dot dot) in the OpenPath parameter.
CVE-2002-0630	The Telnet service for Polycom ViewStation before 7.2.4 allows remote attackers to cause a denial of service (crash) via long or malformed ICMP packets.
CVE-2002-0661	Directory traversal vulnerability in Apache 2.0 through 2.0.39 on Windows, OS2, and Netware allows remote attackers to read arbitrary files and execute commands via .. (dot dot) sequences containing \ (backslash) characters.
CVE-2002-0856	SQL*NET listener for Oracle Net Oracle9i 9.0.x and 9.2 allows remote attackers to cause a denial of service (crash) via certain debug requests that are not properly handled by the debugging feature.
CVE-2002-0924	CGIScript.net csNews.cgi allows remote authenticated users to execute arbitrary Perl code via terminating quotes and metacharacters in text fields of the "Advanced Settings" capability.
CVE-2002-0957	The default configuration of BlackICE Agent 3.1.eal and 3.1.ebh has a high tcp.maxconnections setting, which could allow remote attackers to cause a denial of service (memory consumption) via a large number of connections to the BlackICE system that consumes more resources than intended by the user.
	Comment: insecure default network setting
CVE-2002-1030	Race condition in Performance Pack in BEA WebLogic Server and Express 5.1.x, 6.0.x, 6.1.x and 7.0 allows remote attackers to cause a denial of service (crash) via a flood of data and connections.
CVE-2002-1041	Unknown vulnerability in DCE (1) SMIT panels and (2) configuration commands, possibly related to relative pathnames.
CVE-2002-1062	Signedness error in Thomas Hauck Jana Server 2.x through 2.2.1, and 1.4.6 and earlier, allows remote attackers to execute arbitrary code via long (1) Username, (2) Password, or (3) Hostname entries.
CVE-2002-1135	modsecurity.php 1.10 and earlier, in phpWebSite 0.8.2 and earlier, allows remote attackers to execute arbitrary PHP source code via an inc_prefix parameter that points to the malicious code.
	Comment: input validation? no authorization. php include
CVE-2002-1153	IBM Websphere 4.0.3 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via an HTTP request with long HTTP headers, such as "Host".
CVE-2002-1220	BIND 8.3.x through 8.3.3 allows remote attackers to cause a denial of service (termination due to assertion failure) via a request for a subdomain that does not exist, with an OPT resource record with a large UDP payload size.
CVE-2002-1245	Maped in LuxMan 0.41 uses the user-provided search path to find and execute the gzip program, which allows local users to modify /dev/mem and gain privileges via a modified PATH environment variable that points to a Trojan horse gzip program.

Table 15: Vulnerabilities identified as other type of flaws

CVE name	Data
	Comment: executes gzip without using full path.
CVE-2002-1293	The Microsoft Java implementation, as used in Internet Explorer, provides a public load0() method for the CabCracker class (com.ms.vm.loader.CabCracker), which allows remote attackers to bypass the security checks that are performed by the load() method.
CVE-2002-1373	Signed integer vulnerability in the COM_TABLE_DUMP package for MySQL 3.23.x before 3.23.54 allows remote attackers to cause a denial of service (crash or hang) in mysqld by causing large negative integers to be provided to a memcpy call.
CVE-2002-1384	Integer overflow in pdftops, as used in Xpdf 2.01 and earlier, xpdf-i, and CUPS before 1.1.18, allows local users to execute arbitrary code via a ColorSpace entry with a large number of elements, as demonstrated by cups-pdf.
CVE-2002-1387	The spray mode in traceroute-nanog (aka traceroute-ng) may allow local users to overwrite arbitrary memory locations via an array index overflow using the nprobes (number of probes) argument.
CVE-2002-1417	Directory traversal vulnerability in Novell NetBasic Scripting Server (NSN) for Netware 5.1 and 6, and Novell Small Business Suite 5.1 and 6, allows remote attackers to read arbitrary files via a URL containing a "..
CVE-2002-1444	The Google toolbar 1.1.60, when running on Internet Explorer 5.5 and 6.0, allows remote attackers to cause a denial of service (crash with an exception in oleaut32.dll) via malicious HTML, possibly related to small width and height parameters or an incorrect call to the Google.Search() function.
CVE-2002-1501	The MPS functionality in Enterasys SSR8000 (Smart Switch Router) before firmware 8.3.0.10 allows remote attackers to cause a denial of service (crash) via multiple port scans to ports 15077 and 15078.
CVE-2002-1510	xdm, with the authComplain variable set to false, allows arbitrary attackers to connect to the X server if the xdm auth directory does not exist.
	Comment: default value not according to manual
CVE-2002-1531	The administrative web interface (STEMWADM) for SurfControl SuperScout Email Filter allows remote attackers to cause a denial of service (crash) via an HTTP request without a Content-Length parameter.
CVE-2002-1601	The Connectables feature in Adobe PhotoDeluxe 3.1 prepends the Adobe directory to the CLASSPATH environment variable, which allows applets to run with higher privileges and remote attackers to gain privileges via an HTML e-mail message or a web page.
	Comment: access control, insufficient compartementalization. Applets with extensions can be downloaded. Applets executed from filesystem have more rights than applets loaded from the network. Not configuration error because removing path from CLASSPATH breaks functionality
CVE-2002-1718	Microsoft Internet Information Server (IIS) 5.1 may allow remote attackers to view the contents of a Frontpage Server Extension (FPSE) file, as claimed using an HTTP request for colegal.htm that contains .. (dot dot) sequences.
CVE-2002-1737	Astaro Security Linux 2.016 creates world-writable files and directories, which allows local users to overwrite arbitrary files.
CVE-2002-1743	AOL ICQ 2002a Build 3722 allows remote attackers to cause a denial of service (crash) via a malformed .hpf file.
CVE-2002-1782	The default configuration of University of Washington IMAP daemon (wu-imapd), when running on a system that does not allow shell access, allows a local user with a valid IMAP account to read arbitrary files as that user.

Table 15: Vulnerabilities identified as other type of flaws

CVE name	Data
	Comment: If users are not allowed shell access, some configuration must be done on the OS server itself, and the imap server should be configured in a more restrictive way. If shell access is allowed, then this realy is not a flaw.
CVE-2002-1833	The default configurations for DocuTech 6110 and DocuTech 6115 have a default administrative password of (1) "service!" on Solaris 8.0 or (2) "administ" on Windows NT , which allows remote attackers to gain privileges.
CVE-2002-1861	Sybase Enterprise Application Server 4.0, when running on Windows, allows remote attackers to retrieve files in the WEB-INF directory, which contains Java class files and configuration information, via a request to the WEB-INF directory with a trailing dot ("WEB-INF.").
CVE-2002-1873	Microsoft Exchange 2000, when used with Microsoft Remote Procedure Call (MSRPC), allows remote attackers to cause a denial of service (crash or memory consumption) via malformed MSRPC calls.
CVE-2002-1886	TightAuction 3.0 stores config.inc under the web document root with insufficient access control, which allows remote attackers to obtain the database username and password.
CVE-2002-1887	PHP remote code injection vulnerability in customize.php for phpMyNewsletter 0.6.10 allows remote attackers to execute arbitrary PHP code via the l parameter.
	Comment: not checking if included file is a valid file to include. php include
CVE-2002-1909	Click2Learn Ingenium Learning Management System 5.1 and 6.1 stores the hashed administrative password in a config.txt file under the htdocs directory, which allows remote attackers to obtain the administrative password.
CVE-2002-1921	The default configuration of MySQL 3.20.32 through 3.23.52, when running on Windows, does set the bind address to the loopback interface, which allows remote attackers to connect to the database.
CVE-2002-2006	The default installation of Apache Tomcat 4.0 through 4.1 and 3.0 through 3.3.1 allows remote attackers to obtain the installation path and other sensitive system information via the (1) SnoopServlet or (2) TroubleShooter example servlets.
CVE-2002-2138	RFC-NETBIOS in HP Advanced Server/9000 B.04.05 through B.04.09, when running HP-UX 11.00 or 11.11, allows remote attackers to cause a denial of sevrice (panic) via a malformed UDP packet on port 139.
CVE-2003-0012	The data collection script for Bugzilla 2.14.x before 2.14.5, 2.16.x before 2.16.2, and 2.17.x before 2.17.3 sets world-writable permissions for the data/mining directory when it runs, which allows local users to modify or delete the data.
	Comment: perl code if (! -d) should be if -d $dir)
CVE-2003-0058	MIT Kerberos V5 Key Distribution Center (KDC) before 1.2.5 allows remote authenticated attackers to cause a denial of service (crash) on KDCs within the same realm via a certain protocol request that causes a null dereference.
CVE-2003-0148	The default installation of MSDE via McAfee ePolicy Orchestrator 2.0 through 3.0 allows attackers to execute arbitrary code via a series of steps that (1) obtain the database administrator username and encrypted password in a configuration file from the ePO server using a certain request, (2) crack the password due to weak cryptography, and (3) use the password to pass commands through xp_cmdshell.

Table 15: Vulnerabilities identified as other type of flaws

CVE name	Data
CVE-2003-0163	decrypt_msg for the Gaim-Encryption GAIM plugin 1.15 and earlier does not properly validate a message length parameter, which allows remote attackers to cause a denial of service (crash) via a negative length, which overwrites arbitrary heap memory with a zero byte.
CVE-2003-0225	The ASP function Response.AddHeader in Microsoft Internet Information Server (IIS) 4.0 and 5.0 does not limit memory requests when constructing headers, which allow remote attackers to generate a large header to cause a denial of service (memory consumption) with an ASP page.
CVE-2003-0296	The IMAP Client for Evolution 1.2.4 allows remote malicious IMAP servers to cause a denial of service and possibly execute arbitrary code via certain large literal size values that cause either integer signedness errors or integer overflow errors.
CVE-2003-0300	The IMAP Client for Sylpheed 0.8.11 allows remote malicious IMAP servers to cause a denial of service (crash) via certain large literal size values that cause either integer signedness errors or integer overflow errors.
CVE-2003-0322	Integer overflow in BitchX IRC client 1.0-0c19 and earlier allows remote malicious IRC servers to cause a denial of service (crash).
CVE-2003-0326	Integer overflow in parse_decode_path() of slocate may allow attackers to execute arbitrary code via a LOCATE_PATH with a large number of ":" (colon) characters, whose count is used in a call to malloc.
CVE-2003-0328	EPIC IRC Client (EPIC4) pre2.002, pre2.003, and possibly later versions, allows remote malicious IRC servers to cause a denial of service (crash) and possibly execute arbitrary code via a CTCP request from a large nickname, which causes an incorrect length calculation.
CVE-2003-0398	Vignette StoryServer 4 and 5, and Vignette V/5 and V/6, with the SSI EXEC feature enabled, allows remote attackers to execute arbitrary code via a text variable to a Vignette Application that is later displayed.
CVE-2003-0403	Vignette StoryServer 5 and Vignette V/5 allows remote attackers to read and modify license information, and cause a denial of service (service halt) by directly accessing the /vgn/license template.
CVE-2003-0405	Vignette StoryServer 5 and Vignette V/6 allows remote attackers to execute arbitrary TCL code via (1) an HTTP query or cookie which is processed in the NEEDS command, or (2) an HTTP Referrer that is processed in the VALID_PATHS command.
CVE-2003-0417	Directory traversal vulnerability in Son hServer 0.2 allows remote attackers to read arbitrary files via ".|." (modified dot-dot) sequences.
CVE-2003-0499	Mantis 0.17.5 and earlier stores its database password in cleartext in a world-readable configuration file, which allows local users to perform unauthorized database operations.
CVE-2003-0518	The screen saver in MacOS X allows users with physical access to cause the screen saver to crash and gain access to the underlying session via a large number of characters in the password field, possibly triggering a buffer overflow.
CVE-2003-0539	skk (Simple Kana to Kanji conversion program) 12.1 and earlier, and the ddskk package which is based on skk, creates temporary files insecurely, which allows local users to overwrite arbitrary files.
CVE-2003-0541	gtkhtml before 1.1.10, as used in Evolution, allows remote attackers to cause a denial of service (crash) via a malformed message that causes a null pointer dereference.
CVE-2003-0551	The STP protocol implementation in Linux 2.4.x does not properly verify certain lengths, which could allow attackers to cause a denial of service.

Table 15: Vulnerabilities identified as other type of flaws

CVE name	Data
CVE-2003-0574	Unknown vulnerability in SGI IRIX 6.5.x through 6.5.20, and possibly earlier versions, allows local users to cause a core dump in scheme and possibly gain privileges via certain environment variables, a different vulnerability than CVE-2001-0797 and CVE-1999-0028.
CVE-2003-0581	X Fontserver for Truetype fonts (xfstt) 1.4 allows remote attackers to cause a denial of service and possibly execute arbitrary code via a (1) FS_QueryXExtents8 or (2) FS_QueryXBitmaps8 packet, and possibly other types of packets, with a large num_ranges value, which causes an out-of-bounds array access.
CVE-2003-0695	Multiple "buffer management errors" in OpenSSH before 3.7.1 may allow attackers to cause a denial of service or execute arbitrary code using (1) buffer_init in buffer.c, (2) buffer_free in buffer.c, or (3) a separate function in channels.c, a different vulnerability than CVE-2003-0693.
CVE-2003-0696	The getipnodebyname() API in AIX 5.1 and 5.2 does not properly close sockets, which allows attackers to cause a denial of service (resource exhaustion).
CVE-2003-0730	Multiple integer overflows in the font libraries for XFree86 4.3.0 allow local or remote attackers to cause a denial of service or execute arbitrary code via heap-based and stack-based buffer overflow attacks.
CVE-2003-0778	saned in sane-backends 1.0.7 and earlier, and possibly later versions, does not properly allocate memory in certain cases, which could allow attackers to cause a denial of service (memory consumption).
CVE-2003-0791	The Script.prototype.freeze/thaw functionality in Mozilla 1.4 and earlier allows attackers to execute native methods by modifying the string used as input to the script.thaw JavaScript function, which is then deserialized and executed.
CVE-2003-0792	Fetchmail 6.2.4 and earlier does not properly allocate memory for long lines, which allows remote attackers to cause a denial of service (crash) via a certain email.
CVE-2003-0853	An integer overflow in ls in the fileutils or coreutils packages may allow local users to cause a denial of service or execute arbitrary code via a large -w value, which could be remotely exploited via applications that use ls, such as wu-ftpd.
CVE-2003-0861	Integer overflows in (1) base64_encode and (2) the GD library for PHP before 4.3.3 have unknown impact and unknown attack vectors.
CVE-2003-0961	Integer overflow in the do_brk function for the brk system call in Linux kernel 2.4.22 and earlier allows local users to gain root privileges.
CVE-2003-0989	tcpdump before 3.8.1 allows remote attackers to cause a denial of service (infinite loop) via certain ISAKMP packets, a different vulnerability than CVE-2004-0057.
CVE-2003-1084	Monit 1.4 to 4.1 allows remote attackers to cause a denial of service (daemon crash) via an HTTP POST request with a negative Content-Length field.
CVE-2003-1091	Integer overflow in MP3Broadcaster for Apple QuickTime/Darwin Streaming Server 4.1.3 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via malformed ID3 tags in MP3 files.
CVE-2003-1109	The Session Initiation Protocol (SIP) implementation in multiple Cisco products including IP Phone models 7940 and 7960, IOS versions in the 12.2 train, and Secure PIX 5.2.9 to 6.2.2 allows remote attackers to cause a denial of service and possibly execute arbitrary code via crafted INVITE messages, as demonstrated by the OUSPG PROTOS c07-sip test suite.

Table 15: Vulnerabilities identified as other type of flaws

CVE name	Data
CVE-2003-1111	The Session Initiation Protocol (SIP) implementation in multiple dynamicsoft products including y and certain demo products for AppEngine allows remote attackers to cause a denial of service or execute arbitrary code via crafted INVITE messages, as demonstrated by the OUSPG PROTOS c07-sip test suite.
CVE-2003-1113	The Session Initiation Protocol (SIP) implementation in IPTel SIP Express Router 0.8.9 and earlier allows remote attackers to cause a denial of service and possibly execute arbitrary code via crafted INVITE messages, as demonstrated by the OUSPG PROTOS c07-sip test suite.
CVE-2003-1114	The Session Initiation Protocol (SIP) implementation in Mediatrix Telecom VoIP Access Devices and Gateways running SIPv2.4 and SIPv4.3 firmware allows remote attackers to cause a denial of service or execute arbitrary code via crafted INVITE messages, as demonstrated by the OUSPG PROTOS c07-sip test suite.
CVE-2003-1115	The Session Initiation Protocol (SIP) implementation in Nortel Networks Succession Communication Server 2000, when using SIP-T, allows remote attackers to cause a denial of service and possibly execute arbitrary code via crafted INVITE messages, as demonstrated by the OUSPG PROTOS c07-sip test suite.
CVE-2003-1163	hash.c in Ganglia gmond 2.5.3 allows remote attackers to cause a denial of service (segmentation fault) via a UDP packet that contains a single-byte name string, which is used as an out-of-bounds array index.
CVE-2003-1198	connection.c in Cherokee web server before 0.4.6 allows remote attackers to cause a denial of service via an HTTP POST request without a Content-Length header field.
CVE-2004-0033	admin.php in PHPGEDVIEW 2.61 allows remote attackers to obtain sensitive information via an action parameter with a phpinfo command.
CVE-2004-0093	XFree86 4.1.0 allows remote attackers to cause a denial of service and possibly execute arbitrary code via an out-of-bounds array index when using the GLX extension and Direct Rendering Infrastructure (DRI).
CVE-2004-0094	Integer signedness errors in XFree86 4.1.0 allow remote attackers to cause a denial of service and possibly execute arbitrary code when using the GLX extension and Direct Rendering Infrastructure (DRI).
CVE-2004-0119	The Negotiate Security Software Provider (SSP) interface in Windows 2000, Windows XP, and Windows Server 2003, allows remote attackers to cause a denial of service (crash from null dereference) or execute arbitrary code via a crafted SPNEGO NegTokenInit request during authentication protocol selection.
CVE-2004-0154	rpc.mountd in nfs-utils after 1.0.3 and before 1.0.6 allows attackers to cause a denial of service (crash) via an NFS mount of a directory from a client whose reverse DNS lookup name is different from the forward lookup name.
CVE-2004-0183	TCPDUMP 3.8.1 and earlier allows remote attackers to cause a denial of service (crash) via ISAKMP packets containing a Delete payload with a large number of SPI's, which causes an out-of-bounds read, as demonstrated by the Striker ISAKMP Protocol Test Suite.
CVE-2004-0247	The client and server of Chaser 1.50 and earlier allow remote attackers to cause a denial of service (crash via exception) via a UDP packet with a length field that is greater than the actual data length, which causes Chaser to read unexpected memory.
CVE-2004-0382	Unknown vulnerability in the CUPS printing system in Mac OS X 10.3.3 and Mac OS X 10.2.8 with unknown impact, possibly related to a configuration file setting.

Table 15: Vulnerabilities identified as other type of flaws

CVE name	Data
CVE-2004-0414	CVS 1.12.x through 1.12.8, and 1.11.x through 1.11.16, does not properly handle malformed "Entry" lines, which prevents a NULL terminator from being used and may lead to a denial of service (crash), modification of critical program data, or arbitrary code execution.
CVE-2004-0504	Ethereal 0.10.3 allows remote attackers to cause a denial of service (crash) via certain SIP messages between Hotsip servers and clients.
CVE-2004-0506	The SPNEGO dissector in Ethereal 0.9.8 to 0.10.3 allows remote attackers to cause a denial of service (crash) via unknown attack vectors that cause a null pointer dereference.
CVE-2004-0525	HP Integrated Lights-Out (iLO) 1.10 and other versions before 1.55 allows remote attackers to cause a denial of service (hang) by accessing iLO using the TCP/IP reserved port zero.
CVE-2004-0571	Microsoft Word for Windows 6.0 Converter does not properly validate certain data lengths, which allows remote attackers to execute arbitrary code via a .wri, .rtf, and .doc file sent by email or malicious web site, aka "Table Conversion Vulnerability," a different vulnerability than CVE-2004-0901.
CVE-2004-0599	Multiple integer overflows in the (1) png_read_png in pngread.c or (2) png_handle_sPLT functions in pngrutil.c or (3) progressive display image reading capability in libpng 1.2.5 and earlier allow remote attackers to cause a denial of service (application crash) via a malformed PNG image.
CVE-2004-0608	The Unreal Engine, as used in DeusEx 1.112fm and earlier, Devastation 390 and earlier, Mobile Forces 20000 and earlier, Nerf Arena Blast 1.2 and earlier, Postal 2 1337 and earlier, Rune 107 and earlier, Tactical Ops 3.4.0 and earlier, Unreal 1 226f and earlier, Unreal II XMP 7710 and earlier, Unreal Tournament 451b and earlier, Unreal Tournament 2003 2225 and earlier, Unreal Tournament 2004 before 3236, Wheel of Time 333b and earlier, and X-com Enforcer, allows remote attackers to execute arbitrary code via a UDP packet containing a secure query with a long value, which overwrites memory.
CVE-2004-0642	Double-free vulnerabilities in the error handling code for ASN.1 decoders in the (1) Key Distribution Center (KDC) library and (2) client library for MIT Kerberos 5 (krb5) 1.3.4 and earlier may allow remote attackers to execute arbitrary code.
CVE-2004-0657	Integer overflow in the NTP daemon (NTPd) before 4.0 causes the NTP server to return the wrong date/time offset when a client requests a date/time that is more than 34 years away from the server's time.
CVE-2004-0674	Enterasys XSR-1800 series Security Routers, when running firmware 7.0.0.0 and using Policy-Based Routing, allow remote attackers to cause a denial of service (crash) via a packet with the IP record route option set.
CVE-2004-0745	LHA 1.14 and earlier allows attackers to execute arbitrary commands via a directory with shell metacharacters in its name.
CVE-2004-0754	Integer overflow in Gaim before 0.82 allows remote attackers to cause a denial of service and possibly execute arbitrary code via the size variable in Groupware server messages.
CVE-2004-0816	Integer underflow in the firewall logging rules for iptables in Linux before 2.6.8 allows remote attackers to cause a denial of service (application crash) via a malformed IP packet.
CVE-2004-0832	The (1) ntlm_fetch_string and (2) ntlm_get_string functions in Squid 2.5.6 and earlier, with NTLM authentication enabled, allow remote attackers to cause a denial of service (application crash) via an NTLMSSP packet that causes a negative value to be passed to memcpy.

Table 15: Vulnerabilities identified as other type of flaws

CVE name	Data
CVE-2004-0900	The DHCP Server service for Microsoft Windows NT 4.0 Server and Terminal Server Edition does not properly validate the length of certain messages, which allows remote attackers to execute arbitrary code via a malformed DHCP message, aka the "DHCP Request Vulnerability."
CVE-2004-0919	The syscons CONS_SCRSHOT ioctl in FreeBSD 5.x allows local users to read arbitrary kernel memory via (1) negative coordinates or (2) large coordinates.
CVE-2004-0957	Unknown vulnerability in MySQL 3.23.58 and earlier, when a local user has privileges for a database whose name includes a "_" (underscore), grants privileges to other databases that have similar names, which can allow the user to conduct unauthorized activities.
CVE-2004-0959	rfc1867.c in PHP before 5.0.2 allows local users to upload files to arbitrary locations via a PHP script with a certain MIME header that causes the "$_FILES" array to be modified.
CVE-2004-0988	Integer overflow on Apple QuickTime before 6.5.2, when running on Windows systems, allows remote attackers to cause a denial of service (memory consumption) via certain inputs that cause a large memory operation.
CVE-2004-1066	The cmdline pseudofiles in (1) procfs on FreeBSD 4.8 through 5.3, and (2) linprocfs on FreeBSD 5.x through 5.3, do not properly validate a process argument vector, which allows local users to cause a denial of service (panic) or read portions of kernel memory. NOTE: this candidate might be SPLIT into 2 separate items in the future.
	Comment: pointer derefferenced
CVE-2004-1072	The binfmt_elf loader (binfmt_elf.c) in Linux kernel 2.4.x up to 2.4.27, and 2.6.x up to 2.6.8, may create an interpreter name string that is not NULL terminated, which could cause strings longer than PATH_MAX to be used, leading to buffer overflows that allow local users to cause a denial of service (hang) and possibly execute arbitrary code.
CVE-2004-1149	Computer Associates eTrust EZ Antivirus 7.0.0 to 7.0.4, including 7.0.1.4, installs its files with insecure permissions (ACLs), which allows local users to gain privileges by replacing critical programs with malicious ones, as demonstrated using VetMsg.exe.
	Comment: configuration
CVE-2004-1176	Buffer underflow in extfs.c in Midnight Commander (mc) 4.5.55 and earlier allows remote attackers to cause a denial of service and possibly execute arbitrary code.
CVE-2004-1224	Off-by-one error in the mtr_curses_keyaction function for mtr 0.55 through 0.65 allows local users to hijack raw sockets, as demonstrated using the "s" keybinding, which leaves a buffer without a NULL terminator.
CVE-2004-1354	The Solaris Management Console (SMC) in Sun Solaris 8 and 9 generates different 404 error messages when a file does not exist versus when a file exists but is otherwise inacessible, which could allow remote attackers to obtain sensitive information in conjunction with a directory traversal (..) attack.
CVE-2004-1435	Multiple versions of Cisco ONS 15327, ONS 15454, and ONS 15454 SDH, including 4.6(0) and 4.6(1), 4.5(x), 4.1(0) to 4.1(3), 4.0(0) to 4.0(2), and earlier versions, allows remote attackers to cause a denial of service (control card reset) via a large number of TCP connections with an invalid response instead of the final ACK (TCP-ACK).
CVE-2004-1539	Halo: Combat Evolved 1.05 and earlier allows remote game servers to cause a denial of service (client crash) via a long value in a game server reply, which triggers a NULL dereference.

Table 15: Vulnerabilities identified as other type of flaws

CVE name	Data
CVE-2004-1642	WFTPD Pro Server 3.21 allows remote authenticated users to cause a denial of service (crash) via a series of long MLIST commands.
CVE-2004-1688	Pigeon Server 3.02.0143 and earlier allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a long login name sent to port 3103.
CVE-2004-1744	Easy File Sharing (EFS) Webserver 1.25 allows remote attackers to cause a denial of service (CPU consumption or crash) via many large HTTP requests.
CVE-2004-1749	Attack Mitigator IPS 5500 3.11.008, and possibly other versions, when configured in a one-armed routing configuration, allows remote attackers to cause a denial of service (CPU consumption) via a large number of HTTP requests.
CVE-2004-1766	The default installation of NetScreen-Security Manager before Feature Pack 1 does not enable encryption for communication with devices running ScreenOS 5.0, which allows remote attackers to obtain sensitive information via sniffing.
CVE-2004-1808	Extcompose in metamail does not verify the output file before writing to it, which allows local users to overwrite arbitrary files via a symlink attack.
	Comment: symlink
CVE-2004-1833	The admin.ib file in Borland Interbase 7.1 for Linux has default world writable permissions, which allows local users to gain database administrative privileges.
CVE-2004-1850	The Rage 1.01 and earlier allows remote attackers to cause a denial of service (infinite loop) via a TCP packet with the port and IP address set to zero.
CVE-2004-2032	Netgear RP114 allows remote attackers to bypass the keyword based URL filtering by requesting a long URL, as demonstrated using a large number of
CVE-2004-2045	The HTTP administration interface on Conceptronic CADSLR1 ADSL router running firmware 3.04n allows remote attackers to cause a denial of service (device reboot) via an HTTP request with a long username.
CVE-2004-2075	Sophos Anti-Virus 3.78 allows remote attackers to cause a denial of service (infinite loop) via a MIME header that is not properly terminated.
CVE-2004-2081	The samiftp.dll library in Sami FTP Server 1.1.3 allows local users to cause a denial of service (pmsystem.exe crash) by issuing (1) a CD command with a tilde ( ) character or dot dot (/../) or (2) a GET command for an unavailable file.
CVE-2004-2126	The upgrade for BlackICE PC Protection 3.6 and earlier sets insecure permissions for .INI files such as (1) blackice.ini, (2) firewall.ini, (3) protect.ini, or (4) sigs.ini, which allows local users to modify BlackICE configuration or possibly execute arbitrary code by exploiting vulnerabilities in the .INI parsers.
CVE-2004-2169	Application Access Server (A-A-S) 1.0.37 and earlier allows remote authenticated users to cause a denial of service (application crash) via a long file request.
CVE-2004-2249	Unknown vulnerability in the "access code" in SecureEditor before 0.1.2 has unknown impact and attack vectors, possibly involving a bypass of IP address restrictions.
CVE-2004-2353	BugPort before 1.099 stores its configuration file (conf/config.conf) under the web document root with a file extension that is not normally parsed by web servers, which allows remote attackers to obtain sensitive information.

Table 15: Vulnerabilities identified as other type of flaws

CVE name	Data
CVE-2004-2517	myServer 0.7.1 allows remote attackers to cause a denial of service (crash) via a long HTTP POST request in a View=Logon operation to index.html.
CVE-2004-2583	SMTP service in SmarterTools SmarterMail 1.6.1511 and 1.6.1529 allows remote attackers to cause a denial of service (CPU consumption) via a large number of simultaneous open connections to TCP port 25.
CVE-2004-2650	Spooler in Apache Foundation James 2.2.0 allows local users to cause a denial of service (memory consumption) by triggering various error conditions in the retrieve function, which prevents a lock from being released and causes a memory leak.
CVE-2005-0023	gnome-pty-helper in GNOME libzvt2 and libvte4 allows local users to spoof the logon hostname via a modified DISPLAY environment variable. NOTE: the severity of this issue has been disputed.
CVE-2005-0055	Internet Explorer 5.01, 5.5, and 6 does not properly validate buffers when handling certain DHTML methods including the createControlRange Javascript function, which allows remote attackers to execute arbitrary code, aka the "DHTML Method Heap Memory Corruption Vulnerability."
CVE-2005-0118	helvis 1.8h2_1 and earlier stores recovery files in world readable directories with world readable permissions, which allows local users to read the recovered files of other users.
CVE-2005-0122	** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2005-0975. Reason: This candidate is a duplicate of CVE-2005-0975. Notes: All CVE users should reference CVE-2005-0975 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.
CVE-2005-0133	ClamAV 0.80 and earlier allows remote attackers to cause a denial of service (clamd daemon crash) via a ZIP file with malformed headers.
CVE-2005-0192	Directory traversal vulnerability in the parsing of Skin file names in RealPlayer 10.5 (6.0.12.1040) and earlier allows remote attackers to read arbitrary files via a .. (dot dot) in an RJS filename.
CVE-2005-0229	CitrusDB 0.3.5 and earlier stores the newfile.txt temporary data file under the web root, which allows remote attackers to steal credit card information via a direct request to newfile.txt.
CVE-2005-0369	Armagetron 0.2.6.0 and earlier and Armagetron Advanced 0.2.7.0 earlier allows remote attackers to cause a denial of service (application crash) via a packet with a large (1) descriptor ID or (2) claim_id, which exceeds the boundaries of an array.
CVE-2005-0398	The KAME racoon daemon in ipsec-tools before 0.5 allows remote attackers to cause a denial of service (crash) via malformed ISAKMP packets.
CVE-2005-0400	The ext2_make_empty function call in the Linux kernel before 2.6.11.6 does not properly initialize memory when creating a block for a new directory entry, which allows local users to obtain potentially sensitive information by reading the block.
	Comment: leak of information, no clearing of memory to be written to disk
CVE-2005-0568	Soldier of Fortune II 1.03 gold allows remote attackers to cause a denial of service (application crash) via a large cl_guid value, which results in an invalid pointer dereference.
CVE-2005-0579	nxagent in FreeNX before 0.2.8 does not properly handle when the XAUTHORITY environment variable is not set, which allows local users to access the X server without X authentication.

Table 15: Vulnerabilities identified as other type of flaws

CVE name	Data
CVE-2005-0639	Multiple vulnerabilities in xli before 1.17 may allow remote attackers to execute arbitrary code via "buffer management errors" from certain image properties, some of which may be related to integer overflows in PPM files.
CVE-2005-0655	auraCMS 1.5 allows remote attackers to obtain sensitive information via an HTTP request with an invalid id parameter to (1) teman.php, (2) hal.php, or (3) arsip.php, which reveals the path in a PHP error message.
CVE-2005-0712	Mac OS X before 10.3.8 users world-writable permissions for certain directories, which may allow local users to gain privileges, possibly via the receipt cache or ColorSync profiles.
CVE-2005-0808	Apache Tomcat before 5.x allows remote attackers to cause a denial of service (application crash) via a crafted AJP12 packet to TCP port 8007.
CVE-2005-0815	Multiple "range checking flaws" in the ISO9660 filesystem handler in Linux 2.6.11 and earlier may allow attackers to cause a denial of service or corrupt memory via a crafted filesystem.
CVE-2005-0865	Samsung ADSL Modem SMDK8947v1.2 uses default passwords for the (1) root, (2) admin, or (3) user users, which allows remote attackers to gain privileges via Telnet or an HTTP request to adsl.cgi.
	Comment: default password not changed
CVE-2005-0958	Format string vulnerability in the log_do function in log.c for YepYep mtftpd 0.0.3, when the statistics option is enabled, allows remote attackers to execute arbitrary code via the CWD command.
CVE-2005-0965	The gaim_markup_strip_html function in Gaim 1.2.0, and possibly earlier versions, allows remote attackers to cause a denial of service (application crash) via a string that contains malformed HTML, which causes an out-of-bounds read.
CVE-2005-0973	Unknown vulnerability in the setsockopt system call in Mac OS X 10.3.9 and earlier allows local users to cause a denial of service (memory exhaustion) via crafted arguments.
CVE-2005-0975	Integer signedness error in the parse_machfile function in the mach-o loader (mach_loader.c) for the Darwin Kernel as used in Mac OS X 10.3.7, and other versions before 10.3.9, allows local users to cause a denial of service (CPU consumption) via a crafted mach-o header.
CVE-2005-0998	The Web_Links module for PHP-Nuke 7.6 allows remote attackers to obtain sensitive information via an invalid show parameter, which triggers a division by zero PHP error that leaks the full pathname of the server.
CVE-2005-1020	Secure Shell (SSH) 2 in Cisco IOS 12.0 through 12.3 allows remote attackers to cause a denial of service (device reload) (1) via a username that contains a domain name when using a TACACS+ server to authenticate, (2) when a new SSH session is in the login phase and a currently logged in user issues a send command, or (3) when IOS is logging messages and an SSH session is terminated while the server is sending data.
CVE-2005-1106	PictureViewer in QuickTime for Windows 6.5.2 allows remote attackers to cause a denial of service (application crash) via a GIF image with the maximum depth start value, possibly triggering an integer overflow.
CVE-2005-1123	Monkey daemon (monkeyd) before 0.9.1 allows remote attackers to cause a denial of service (memory corruption) via a request for a zero byte file.
CVE-2005-1229	Directory traversal vulnerability in cpio 2.6 and earlier allows remote attackers to write to arbitrary directories via a .. (dot dot) in a cpio file.
CVE-2005-1235	auction_my_auctions.php in phpbb-Auction 1.2m and earlier allows remote attackers to obtain sensitive information via an invalid mode parameter, which leaks the full path in a PHP error message.

Table 15: Vulnerabilities identified as other type of flaws

CVE name	Data
CVE-2005-1264	Raw character devices (raw.c) in the Linux kernel 2.6.x call the wrong function before passing an ioctl to the block device, which crosses security boundaries by making kernel address space accessible from user space, a similar vulnerability to CVE-2005-1589.
CVE-2005-1347	** UNVERIFIABLE ** NOTE: this issue describes a problem that can not be independently verified as of 20050421. Adobe Acrobat reader (AcroRd32.exe) 6.0 and earlier allows remote attackers to cause a denial of service ("Invalid-ID-Handle-Error" error) and modify memory beginning at a particular address, possibly allowing the execution of arbitrary code, via a crafted PDF file. NOTE: the vendor has stated that the reporter refused to provide sufficient details to confirm the issue. In addition, due to the lack of details in the original advisory, an independent verification is not possible. Finally, the reliability of the original reporter is unknown. This item has only been assigned a CVE identifier for tracking purposes, and to serve as a concrete example of the newly defined UNVERIFIABLE and PRERELEASE content decisions in CVE, which must be discussed by the Editorial Board. Without additional details or independent verification by reliable sources, it is highly likely that this item will be REJECTED.
CVE-2005-1369	The (1) it87 and (2) via686a drivers in I2C for Linux 2.6.x before 2.6.11.8, and 2.6.12 before 2.6.12-rc2, create the sysfs "alarms" file with write permissions, which allows local users to cause a denial of service (CPU consumption) by attempting to write to the file, which does not have an associated store function.
CVE-2005-1456	Multiple unknown vulnerabilities in the (1) DHCP and (2) Telnet dissectors in Ethereal before 0.10.11 allow remote attackers to cause a denial of service (abort).
CVE-2005-1465	Unknown vulnerability in the NCP dissector in Ethereal before 0.10.11 allow remote attackers to cause a denial of service (long loop).
CVE-2005-1601	MRO Maximo Self Service 4 and 5 stores certain information under the web document root using file extensions that are not processed by Tomcat, which allows remote attackers to obtain sensitive information via a direct request for the file, such as MXServer.properties.
CVE-2005-1698	PostNuke 0.750 and 0.760RC3 allows remote attackers to obtain sensitive information via a direct request to (1) theme.php or (2) Xanthia.php in the Xanthia module, (3) user.php, (4) thelang.php, (5) text.php, (6) html.php, (7) menu.php, (8) finclude.php, or (9) button.php in the pnblocks directory in the Blocks module, (10) config.php in the NS-Multisites (aka Multisites) module, or (11) xmlrpc.php, which reveals the path in an error message.
CVE-2005-1709	Unknown vulnerability in Blue Coat Reporter before 7.1.2 allows remote unauthenticated attackers to add a license.
CVE-2005-1711	Gibraltar Firewall 2.2 and earlier, when using the ClamAV update to 0.81 for Squid, uses a defunct ClamAV method to scan memory for viruses, which does not return an error code and prevents viruses from being detected.
	Comment: programmer using wrong function call
CVE-2005-1746	The cluster cookie parsing code in BEA WebLogic Server 7.0 through Service Pack 5 attempts to contact any host or port specified in a cookie, even when it is not in the cluster, which allows remote attackers to cause a denial of service (cluster slowdown) via modified cookies.
CVE-2005-1792	Memory leak in Windows Management Instrumentation (WMI) service allows attackers to cause a denial of service (memory consumption and crash) by creating security contexts more quickly than they can be cleared from the RPC cache.

Table 15: Vulnerabilities identified as other type of flaws

CVE name	Data
CVE-2005-1852	Multiple integer overflows in libgadu, as used in Kopete in KDE 3.2.3 to 3.4.1, ekg before 1.6rc3, GNU Gadu, CenterICQ, Kadu, and other packages, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via an incoming message.
CVE-2005-2099	The Linux kernel before 2.6.12.5 does not properly destroy a keyring that is not instantiated properly, which allows local users or remote attackers to cause a denial of service (kernel oops) via a keyring with a payload that is not empty, which causes the creation to fail, leading to a null dereference in the keyring destructor.
CVE-2005-2100	The rw_vm function in usercopy.c in the 4GB split patch for the Linux kernel in Red Hat Enterprise Linux 4 does not perform proper bounds checking, which allows local users to cause a denial of service (crash).
CVE-2005-2394	show_news.php in CuteNews 1.3.6 allows remote attackers to obtain the full path of the server via an invalid archive parameter.
CVE-2005-2446	** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2005-2369. Reason: This candidate is a duplicate of CVE-2005-2369. Notes: All CVE users should reference CVE-2005-2369 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.
CVE-2005-2479	Quick 'n Easy FTP Server 3.0 allows remote attackers to cause a denial of service (application crash or CPU consumption) via a long USER command.
CVE-2005-2483	Eval injection vulnerability in Karrigell before 2.1.8 allows remote attackers to execute arbitrary Python code via modified arguments to a Karrigell services (.ks) script, which can reference functions from libraries that are used by that script.
CVE-2005-2538	FlatNuke 2.5.5 and possibly earlier versions allows remote attackers to obtain sensitive information via (1) a null byte or (2) an MS-DOS device name such as AUX, CON, PRN, COM1, or LPT1 in the mod parameter.
CVE-2005-2570	FunkBoard 0.66CF, and possibly earlier versions, allows remote attackers to obtain sensitive information via a direct request to forums.php, which reveals the path in an error message.
CVE-2005-2602	Mozilla Thunderbird 1.0 and Firefox 1.0.6 allows remote attackers to obfuscate URIs via a long URI, which causes the address bar to go blank and could facilitate phishing attacks.
	Comment: address bar text should not be white by design
CVE-2005-2671	** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2005-2041. Reason: This candidate is a duplicate of CVE-2005-2041. Notes: All CVE users should reference CVE-2005-2041 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.
CVE-2005-2725	The inputtrap utility in QNX RTOS 6.1.0, 6.3, and possibly earlier versions does not properly check permissions when the -t flag is specified, which allows local users to read arbitrary files.
CVE-2005-2753	Integer overflow in Apple QuickTime before 7.0.3 allows user-complicit attackers to execute arbitrary code via a crafted MOV file that causes a sign extension of the length element in a Pascal style string.
CVE-2005-2754	Integer overflow in Apple QuickTime before 7.0.3 allows user-complicit attackers to execute arbitrary code via a crafted MOV file with "Improper movie attributes."
CVE-2005-2804	Integer overflow in the registry parsing code in GroupWise 6.5.3, and possibly earlier version, allows remote attackers to cause a denial of service (application crash) via a large TCP/IP port in the Windows registry key.

Table 15: Vulnerabilities identified as other type of flaws

CVE name	Data
CVE-2005-2872	The ipt_recent kernel module (ipt_recent.c) in Linux kernel before 2.6.12, when running on 64-bit processors such as AMD64, allows remote attackers to cause a denial of service (kernel panic) via certain attacks such as SSH brute force, which leads to memset calls using a length based on the u_int32_t type, acting on an array of unsigned long elements, a different vulnerability than CVE-2005-2873.
	Comment: integer size error?
CVE-2005-2912	Linksys WRT54G router allows remote attackers to cause a denial of service (CPU consumption and server hang) via an HTTP POST request with a negative Content-Length value.
CVE-2005-2937	** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2005-3663, CVE-2005-3664. Reason: this candidate was intended for one issue, but multiple advisories used this candidate for different issues. Notes: All CVE users should consult CVE-2005-3663 and CVE-2005-3664 to determine which ID is appropriate. All references and descriptions in this candidate have been removed to prevent accidental usage.
CVE-2005-3167	Incomplete blacklist vulnerability in MediaWiki before 1.4.11 does not properly remove certain CSS inputs (HTML inline style attributes) that are processed as active content by Internet Explorer, which allows remote attackers to conduct cross-site scripting (XSS) attacks.
CVE-2005-3195	** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2005-3178. Reason: this candidate is a duplicate of CVE-2005-3178; the duplicate arose from a pre-candidate that was not deleted during the editing phase. Notes: All CVE users should reference CVE-2005-3178 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.
CVE-2005-3277	The LPD service in HP-UX 10.20 11.11 (11i) and earlier allows remote attackers to execute arbitrary code via shell metacharacters ("“" or single backquote) in a request that is not properly handled when an error occurs, as demonstrated by killing the connection, a different vulnerability than CVE-2002-1473.
CVE-2005-3297	Multiple integer overflows in OpenWBEM on SuSE Linux 9 allow remote attackers to execute arbitrary code via unknown vectors.
CVE-2005-3330	The _httpsrequest function in Snoopy 1.2, as used in products such as (1) MagpieRSS, (2) WordPress, (3) Ampache, and (4) Jinzora, allows remote attackers to execute arbitrary commands via shell metacharacters in an HTTPS URL to an SSL protected web page, which is not properly handled by the fetch function.
CVE-2005-3331	viewpatch in mgdiff 1.0 allows local users to overwrite arbitrary files via a symlink attack on temporary files.
CVE-2005-3492	FlatFrag 0.3 and earlier allows remote attackers to cause a denial of service (crash) by sending an NT_CONN_OK command from a client that is not connected, which triggers a null dereference.
CVE-2005-3569	INSO service in IBM DB2 Content Manager before 8.2 Fix Pack 10 on AIX allows attackers to cause a denial of service (application crash) via unknown attack vectors involving LZH files.
CVE-2005-3717	The telnet daemon in UTStarcom F1000 VOIP WIFI Phone s2.0 running VxWorks 5.5.1 with kernel WIND 2.6 has a default username "target" and password "password", which allows remote attackers to gain full access to the system.
CVE-2005-3732	The Internet Key Exchange version 1 (IKEv1) implementation (isakmp_agg.c) in racoon in ipsec-tools before 0.6.3, when running in aggressive mode, allows remote attackers to cause a denial of service (null dereference and crash) via crafted IKE packets, as demonstrated by the PROTOS ISAKMP Test Suite for IKEv1.

Table 15: Vulnerabilities identified as other type of flaws

CVE name	Data
CVE-2005-4077	Multiple off-by-one errors in the cURL library (libcurl) 7.11.2 through 7.15.0 allow local users to trigger a buffer overflow and cause a denial of service or bypass PHP security restrictions via certain URLs that (1) are malformed in a way that prevents a terminating null byte from being added to either a hostname or path buffer, or (2) contain a "?" separator in the hostname portion, which causes a "/" to be prepended to the resulting string.
CVE-2005-4153	Mailman 2.1.4 through 2.1.6 allows remote attackers to cause a denial of service via a message that causes the server to "fail with an Overflow on bad date data in a processed message," a different vulnerability than CVE-2005-3573.
CVE-2005-4156	Unspecified vulnerability in Mambo 4.5 (1.0.0) through 4.5 (1.0.9), with magic_quotes_gpc disabled, allows remote attackers to read arbitrary files and possibly cause a denial of service via a query string that ends with a NULL character.
CVE-2005-4210	Opera before 8.51, when running on Windows with Input Method Editor (IME) installed, allows remote attackers to cause a denial of service (persistent application crash) by bookmarking a site with a long title.
CVE-2005-4216	The Administration Service (FMSAdmin.exe) in Macromedia Flash Media Server 2.0 r1145 allows remote attackers to cause a denial of service (application crash) via a malformed request with a single character to port 1111.
CVE-2005-4261	Unspecified vulnerability in Positive Software Corporation CP+ (cpplus) before 2.5.5 allows attackers to has unknown impact and attack vectors, related to "a possible security flaw caused by a bug in Perl." NOTE: unless CP+ includes its own copy of Perl with CVE-2005-3962, this is a different vulnerability than CVE-2005-3962; however, there is insufficient information to be sure.
CVE-2005-4269	mshtml.dll in Microsoft Windows XP, Server 2003, and Internet Explorer 6.0 SP1 allows attackers to cause a denial of service (access violation) by causing mshtml.dll to process button-focus events at the same time that a document is reloading, as seen in Microsoft Office InfoPath 2003 by repeatedly clicking the "Delete" button in a repeating section in a form. NOTE: the normal operation of InfoPath appears to involve a local user without any privilege boundaries, so this might not be a vulnerability in InfoPath. If no realistic scenarios exist for this problem in other products, then perhaps it should be excluded from CVE.
CVE-2005-4278	Untrusted search path vulnerability in Perl before 5.8.7-r1 on Gentoo Linux allows local users in the portage group to gain privileges via a malicious shared object in the Portage temporary build directory, which is part of the RUNPATH.
CVE-2005-4279	Untrusted search path vulnerability in Qt-UnixODBC before 3.3.4-r1 on Gentoo Linux allows local users in the portage group to gain privileges via a malicious shared object in the Portage temporary build directory, which is part of the RUNPATH.
CVE-2005-4280	Untrusted search path vulnerability in CMake before 2.2.0-r1 on Gentoo Linux allows local users in the portage group to gain privileges via a malicious shared object in the Portage temporary build directory, which is part of the RUNPATH.
CVE-2005-4443	Untrusted search path vulnerability in Gauche before 0.8.6-r1 on Gentoo Linux allows local users in the portage group to gain privileges via a malicious shared object in the Portage temporary build directory, which is part of the RUNPATH.

Table 15: Vulnerabilities identified as other type of flaws

CVE name	Data
CVE-2005-4503	httprint v202, and possibly other versions before v301, allows remote attackers to cause a denial of service (crash) via a long Server field in an HTTP response.
CVE-2005-4695	Symantec Brightmail AntiSpam 6.0 build 1 and 2 allows remote attackers to cause a denial of service (bmserver component termination) via malformed MIME messages.
CVE-2006-0023	Microsoft Windows XP SP1 and SP2 before August 2004, and possibly other operating systems and versions, uses insecure default ACLs that allow the Authenticated Users group to gain privileges by modifying critical configuration information for the (1) Simple Service Discovery Protocol (SSDP) and (2) Universal Plug and Play Device Host (UPnP) services. NOTE: the (3) NetBT and (4) SCardSvr already required privileged access to exploit.
CVE-2006-0118	Unspecified vulnerability in IBM Lotus Notes and Domino Server before 6.5.5, when running on AIX, allows attackers to cause a denial of service (deep recursion leading to stack overflow and crash) via long formulas.
CVE-2006-0138	aMSN (aka Alvaro's Messenger) allows remote attackers to cause a denial of service (client hang and termination of client's instant-messaging session) by repeatedly sending crafted data to the default file-transfer port (TCP 6891).
CVE-2006-0340	Unspecified vulnerability in Stack Group Bidding Protocol (SGBP) support in Cisco IOS 12.0 through 12.4 running on various Cisco products, when SGBP is enabled, allows remote attackers on the local network to cause a denial of service (device hang and network traffic loss) via a crafted UDP packet to port 9900.
CVE-2006-0467	Unspecified vulnerability in Pioneers (formerly gnocatan) before 0.9.49 allows remote attackers to cause a denial of service (application crash) via long chat messages.
CVE-2006-0525	Multiple Adobe products, including (1) Photoshop CS2, (2) Illustrator CS2, and (3) Adobe Help Center, install a large number of .EXE and .DLL files with write-access permission for the Everyone group, which allows local users to gain privileges via Trojan horse programs.
CVE-2006-0579	Multiple integer overflows in (1) the new_demux_packet function in demuxer.h and (2) the demux_asf_read_packet function in demux_asf.c in MPlayer 1.0pre7try2 and earlier allow remote attackers to execute arbitrary code via an ASF file with a large packet length value. NOTE: the provenance of this information is unknown; portions of the details are obtained from third party information.
CVE-2006-0634	Borland C++Builder 6 (BCB6) with Update Pack 4 Enterprise edition (ent_upd4) evaluates the "i>sizeof(int)" expression to false when i equals -1, which might introduce integer overflow vulnerabilities into applications that could be exploited by context-dependent attackers.
CVE-2006-0830	The scripting engine in Internet Explorer allows remote attackers to cause a denial of service (resource consumption) and possibly execute arbitrary code via a web page that contains a recurrent call to an infinite loop in Javascript or VBscript, which consumes the stack, as demonstrated by resetting the "location" variable within the loop.

F Vulnerabilities identified as unknown type

Table 16: Vulnerabilities identified as unknown type

CVE name	Data
CVE-1999-0213	libnsl in Solaris allowed an attacker to perform a denial of service of rpcbind.
CVE-1999-0447	Local users can gain privileges using the debug utility in the MPE/iX operating system.
CVE-1999-0588	A filter in a router or firewall allows unusual fragmented packets.
CVE-1999-1034	Vulnerability in login in AT&T System V Release 4 allows local users to gain privileges.
CVE-1999-1061	HP Laserjet printers with JetDirect cards, when configured with TCP/IP, can be configured without a password, which allows remote attackers to connect to the printer and change its IP address or disable logging.
CVE-1999-1121	The default configuration for UUCP in AIX before 3.2 allows local users to gain root privileges.
CVE-1999-1136	Vulnerability in Predictive on HP-UX 11.0 and earlier, and MPE/iX 5.5 and earlier, allows attackers to compromise data transfer for Predictive messages (using e-mail or modem) between customer and Response Center Predictive systems.
CVE-1999-1145	Vulnerability in Glance programs in GlancePlus for HP-UX 10.20 and earlier allows local users to access arbitrary files and gain privileges.
CVE-1999-1300	Vulnerability in accton in Cray UNICOS 6.1 and 6.0 allows local users to read arbitrary files and modify system accounting configuration.
CVE-1999-1415	Vulnerability in /usr/bin/mail in DEC ULTRIX before 4.2 allows local users to gain privileges.
CVE-2000-0233	SuSE Linux IMAP server allows remote attackers to bypass IMAP authentication and gain privileges.
CVE-2000-0237	Netscape Enterprise Server with Web Publishing enabled allows remote attackers to list arbitrary directories via a GET request for the /publisher directory, which provides a Java applet that allows the attacker to browse the directories.
CVE-2000-1099	Java Runtime Environment in Java Development Kit (JDK) 1.2.2_05 and earlier can allow an untrusted Java class to call into a disallowed class, which could allow an attacker to escape the Java sandbox and conduct unauthorized activities.
CVE-2000-1102	PTlink IRCD 3.5.3 and PTlink Services 1.8.1 allow remote attackers to cause a denial of service (server crash) via "mode +owgscfxeb" and "oper" commands.
CVE-2000-1206	Vulnerability in Apache httpd before 1.3.11, when configured for mass virtual hosting using mod_rewrite, or mod_vhost_alias in Apache 1.3.9, allows remote attackers to retrieve arbitrary files.
CVE-2001-0177	WebMaster ConferenceRoom 1.8.1 allows remote attackers to cause a denial of service via a buddy relationship between the IRC server and a server clone.
CVE-2001-0195	sash before 3.4-4 in Debian Linux does not properly clone /etc/shadow, which makes it world-readable and could allow local users to gain privileges via password cracking.
	Comment: only debian? Why should a shell clone /etc/shadow? Built in chpasswd?

Table 16: Vulnerabilities identified as unknown type

CVE name	Data
CVE-2001-0444	Cisco CBOS 2.3.0.053 sends output of the "sh nat" (aka "show nat") command to the terminal of the next user who attempts to connect to the router via telnet, which could allow that user to obtain sensitive information.
CVE-2001-0688	Broker FTP Server 5.9.5.0 allows a remote attacker to cause a denial of service by repeatedly issuing an invalid CD or CWD ("CD . .") command.
CVE-2001-0709	Microsoft IIS 4.0 and before, when installed on a FAT partition, allows a remote attacker to obtain source code of ASP files via a URL encoded with Unicode.
	Comment: Probably deployment.
CVE-2001-0720	Internet Explorer 5.1 for Macintosh on Mac OS X allows remote attackers to execute arbitrary commands by causing a BinHex or MacBinary file type to be downloaded, which causes the files to be executed if automatic decoding is enabled.
CVE-2001-1097	Cisco routers and switches running IOS 12.0 through 12.2.1 allows a remote attacker to cause a denial of service via a flood of UDP packets.
CVE-2002-0357	Unknown vulnerability in rpc.passwd in the nfs.sw.nis subsystem of SGI IRIX 6.5.15 and earlier allows local users to gain root privileges.
CVE-2002-0528	Watchguard SOHO firewall 5.0.35 unpredictably disables certain IP restrictions for customized services that were set before the administrator upgrades to 5.0.35, which could allow remote attackers to bypass the intended access control rules.
CVE-2002-1269	Unknown vulnerability in NetInfo Manager application in Mac OS X 10.2.2 allows local users to access restricted parts of a filesystem.
CVE-2003-0366	lyskom-server 2.0.7 and earlier allows unauthenticated users to cause a denial of service (CPU consumption) via a large query.
CVE-2003-0428	Unknown vulnerability in the DCERPC (DCE/RPC) dissector in Ethereal 0.9.12 and earlier allows remote attackers to cause a denial of service (memory consumption) via a certain NDR string.
CVE-2003-0631	VMware GSX Server 2.5.1 build 4968 and earlier, and Workstation 4.0 and earlier, allows local users to gain root privileges via certain enivronment variables that are used when launching a virtual machine session.
	Comment: SUID, no information on input validation or code hook
CVE-2003-1188	Unichat allows remote attackers to cause a denial of service (crash) by adding extra chat characters (avatars) and logging in to a chat room, as demonstrated using duplicate ACTOR entries in u2res000.rit.
CVE-2004-0088	The System Configuration subsystem in Mac OS 10.2.8 allows local users to modify network settings, a different vulnerability than CVE-2004-0087.
CVE-2004-0654	Unknown vulnerability in the Basic Security Module (BSM), when configured to audit either the Administrative (ad) or the System-Wide Administration (as) audit class in Solaris 7, 8, and 9, allows local users to cause a denial of service (kernel panic).
CVE-2004-0684	WebSphere Edge Component Caching Proxy in WebSphere Edge Server 5.02, with the JunctionRewrite directive enabled, allows remote attackers to cause a denial of service via an HTTP GET request without any parameters.
CVE-2004-0924	NetInfo Manager on Mac OS X 10.3.x through 10.3.5, after an initial root login, reports the root account as being disabled, even when it has not.
CVE-2004-2244	The XML parser in Oracle 9i Application Server Release 2 9.0.3.0 and 9.0.3.1, 9.0.2.3 and earlier, and Release 1 1.0.2.2 and 1.0.2.2.2, and Database Server Release 2 9.2.0.1 and later, allows remote attackers to cause a denial of service (CPU and memory consumption) via a SOAP message containing a crafted DTD.

Table 16: Vulnerabilities identified as unknown type

CVE name	Data
CVE-2004-2481	MyProxy 6.58 allows remote authenticated users in the Users Tab to connect to arbitrary hosts from the MyProxy server, possibly bypassing access restrictions, by connecting to the proxy and issuing a CONNECT command.
CVE-2005-0721	PHP remote code injection vulnerability in modules.php in eXPerience2 allows remote attackers to execute arbitrary PHP code by modifying the file parameter to reference a URL on a remote web server that contains the code.
CVE-2005-0954	Windows Explorer and Internet Explorer in Windows 2000 SP1 allows remote attackers to cause a denial of service (CPU consumption) via a malformed Windows Metafile (WMF) file.
CVE-2005-1409	PostgreSQL 7.3.x through 8.0.x gives public EXECUTE access to certain character conversion functions, which allows unprivileged users to call those functions with malicious values, with unknown impact, aka the "Character conversion vulnerability."
CVE-2005-1609	Unknown vulnerability in Sun StorEdge 6130 Arrays (SE6130) with serial numbers between 0451AWF00G and 0513AWF00J allows local users and remote attackers to delete data.
CVE-2005-1719	Unknown vulnerability in ALWIL avast! antivirus 4 (4.6.6230) and earlier, when running on Windows NT 4.0, does not properly detect certain viruses.
CVE-2005-4680	Sophos Anti-Virus before 4.02, 4.5.x before 4.5.9, 4.6.x before 4.6.9, and 5.x before 5.1.4 allow remote attackers to hide arbitrary files and data via crafted ARJ archives, which are not properly scanned.
	Comment: does the crafting break the ARJ format rules?
CVE-2006-0045	crawl before 4.0.0 does not securely call programs when saving and loading games, which allows local users to gain privileges.
	Comment: suid files, input validation or execution of programs by design?
CVE-2006-0307	The DM Primer in the DM Deployment Common Component in Computer Associates (CA) BrightStor Mobile Backup r4.0, BrightStor ARCserve Backup for Laptops & Desktops r11.0, r11.1, r11.1 SP1, Unicenter Remote Control 6.0, 6.0 SP1, CA Desktop Protection Suite r2, CA Server Protection Suite r2, and CA Business Protection Suite r2 allows remote attackers to cause a denial of service (CPU consumption and log file consumption) via unspecified "unrecognized network messages" that are not properly handled.

G Programs to work with National Vulnerability Database

G.1 nvd-parse.py

A program to parse the xml files from National Vulnerability Database and insert the data into a local database.

```
#!/usr/bin/python

import sys
import site
from xml.sax import make_parser
from xml.sax.handler import feature_namespaces
from xml.sax import saxutils
from xml.sax import ContentHandler

import MySQLdb

#print sys.getdefaultencoding()
#site.setencoding()

class nvdParser(ContentHandler):

    #def __init__(self, search_name):
    def __init__(self):
        # Save the name we're looking for
        #self.search_name = normalize_whitespace(search_name)



        self.entryType = ''
        self.entryName = ''
        self.entrySeq = ''
        self.entryDiscovered = ''
        self.entryPublished = ''
        self.entryModified = ''
        self.entrySeverity = ''
        self.entryCVSS_score = ''
        self.entryCVSS_vector = ''
        self.descriptSource = ''
        self.descript = ''

        self.refs = []
        self.vulnType = []

        self.vulnTypes = {'access': 0, 'inputbound': 0, 'inputbuffer': 0,
                          'design': 0, 'exception': 0, 'env': 0,
                          'config': 0, 'race': 0, 'other': 0}


        # Initialize the flag to false
        self.inDescript = 0
        self.inRef = 0
```

```
    def startElement(self, name, attrs):
#        if self.entryName == 'CVE-1999-1180':
#            print 'Start element:', name



        if name == 'entry':

            self.refs = []
            #self.vulnTypes = []
            self.vulnTypes = {'access': 0, 'inputbound': 0, 'inputbuffer': 0,
                        'design': 0, 'exception': 0, 'env': 0,
                        'config': 0, 'race': 0, 'other': 0}



            self.entryType = attrs.get('type')
            self.entryName = attrs.get('name')
            self.entrySeq = attrs.get('seq')
            self.entryDiscovered = attrs.get('discovered')
            self.entryPublished = attrs.get('published')
            self.entryModified = attrs.get('modified')
            self.entrySeverity = attrs.get('severity')
            self.entryCVSS_score = attrs.get('CVSS_score')
            self.entryCVSS_vector = attrs.get('CVSS_vector')

            #print 'Starting element:', name, type, cvename, seq
#            print '*****************************************************'

        elif name == 'desc':
            self.descCount = 0

        elif name == 'descript':

            self.descriptSource = attrs.get('source')
            self.inDescript = 1
            self.descript = ''

        elif name == 'vuln_types':
            self.inVulnTypes = 1


        elif name == 'input':
            if self.inVulnTypes == 1:
                if attrs.get('buffer') == '1':
                    self.vulnTypes['inputbuffer'] = 1
                elif attrs.get('bound') == '1':
                    self.vulnTypes['inputbound'] = 1
        elif name == 'access':
            if self.inVulnTypes == 1:
                self.vulnTypes['access'] = 1
        elif name == 'design':
            if self.inVulnTypes == 1:
                self.vulnTypes['design'] = 1
        elif name == 'exception':
            if self.inVulnTypes == 1:
                self.vulnTypes['exception'] = 1
```

```
        elif name == 'env':
            if self.inVulnTypes == 1:
                self.vulnTypes['env'] = 1
        elif name == 'config':
            if self.inVulnTypes == 1:
                self.vulnTypes['config'] = 1
        elif name == 'race':
            if self.inVulnTypes == 1:
                self.vulnTypes['race'] = 1
        elif name == 'other':
            if self.inVulnTypes == 1:
                self.vulnTypes['other'] = 1

        elif name == 'ref':
            self.inRef = 1

            self.refSource = attrs.get('source')
            self.refUrl = attrs.get('url')
            self.refSig = attrs.get('sig')
            self.refAdv = attrs.get('adv')
            self.refPatch = attrs.get('patch')

            self.refTxt = ''




    def endElement(self, name):
        #        print "End element  :", name

        if name == 'entry':
            c=2
##            print self.entryName, self.descript
##            print self.entryName
##            print self.descript
            ## if len(self.vulnTypes) > 0:
##                  for vulnType in self.vulnTypes:
##                      print vulnType

##             if len(self.refs) > 0:
##                 for ref in self.refs:
##                     print ref

            #print "\n"



            nvd_dbc.execute("""INSERT INTO entry (type, name, seq,
                           discovered, published, modified, severity,
                           CVSS_score, CVSS_vector, source,description,
                           inputbuffer, inputbound, access, design, exception,
                           env, config, race, other)
                           values (%s, %s, %s, %s, %s, %s, %s, %s, %s, %s, %s,
                           %s, %s, %s, %s, %s, %s, %s, %s, %s)""",
                           (self.entryType, self.entryName, self.entrySeq,
                           self.entryDiscovered, self.entryPublished,
                            self.entryModified, self.entrySeverity,
                            self.entryCVSS_score, self.entryCVSS_vector,
```

```
                            self.descriptSource, self.descript,
                            self.vulnTypes['inputbuffer'],
                            self.vulnTypes['inputbound'],
                            self.vulnTypes['access'],
                            self.vulnTypes['design'],
                            self.vulnTypes['exception'],
                            self.vulnTypes['env'],
                            self.vulnTypes['config'],
                            self.vulnTypes['race'],
                            self.vulnTypes['other']
                            ))

            if len(self.refs) > 0:
                for ref in self.refs:
                    #print ref
                    nvd_dbc.execute("""INSERT INTO ref (seq, source, url, sig, adv, patch, text)
                            values (%s, %s, %s, %s, %s, %s, %s)""",
                            (self.entrySeq, ref[0], ref[1], ref[2], ref[3], ref[4], ref[5].encode('utf-8')))

        elif name == 'descript':

            self.inDescript = 0


        elif name == 'vuln_types':

            self.inVulnTypes = 0



        elif name == 'ref':

            self.refs.append([self.refSource,
                              self.refUrl,
                              self.refSig,
                              self.refAdv,
                              self.refPatch,
                              self.refTxt])
            self.inRef = 0




    def characters(self, ch):

        if self.inDescript:
            self.descript = self.descript + ch

        if self.inRef:
            self.refTxt = self.refTxt + ch



nvd_db=MySQLdb.connect(user='nvd', passwd="???????????",db="nvd")
nvd_dbc=nvd_db.cursor()

# Create a parser
parser = make_parser()
```

```
# Tell the parser we are not interested in XML namespaces
parser.setFeature(feature_namespaces, 0)

# Create the handler
dh = nvdParser()

# Tell the parser to use our handler
parser.setContentHandler(dh)

# Parse the input
#parser.parse('file://nvd/nvdcve-recent.xml')
parser.parse('file://nvdcve-2002.xml')
parser.parse('file://nvdcve-2003.xml')
parser.parse('file://nvdcve-2004.xml')
parser.parse('file://nvdcve-2005.xml')
parser.parse('file://nvdcve-2006.xml')
```

G.2 nvd-manage.py

A program used to sample vulnerabilities from the local copy of National Vulnerability Database.

```
#!/usr/bin/python

import sys
import getopt
import MySQLdb

import random
import time
import os.path

#from types import *

def main():
    try:
        opts, args = getopt.getopt(sys.argv[1:], "ht:n:co:u:", ["help", "type=", "checkout",
                                                                "output=", "update="])
    except getopt.GetoptError:
        # print help information and exit:
        #usage()
        print "Unknown argument."

        sys.exit(2)

    type = None
    verbose = False
    number = 10
    checkout = False

    nvddir = "/srv/vulnerability-collections/nvd/study/"

    for o, a in opts:
        if o in ("-h", "--help"):
```

```
            #usage()
            print """
            -h, --help: This info
            -t, --type= inutbuffer|inputbound|access|design|exception|env|config|race
            |other
            -n number: number of vulnerabilities wanted
            -c, --checkout: Mark vulnerabilities in database as checked out
            -o, --output: not implemented\n
            """

            sys.exit()

        if o in ("-t", "--type"):
            if a in ("inputbuffer", "inputbound", "access", "design", "exception",
                     "env", "config", "race", "other"):
                type = a
            else:
                print "Does not recognize type: %s" % a
                sys.exit()

        if o == "-n":
            number = int(a)


        if o in ("-c", "--checkout"):
            checkout = True

        if o in ("-o", "--output"):
            if a in ("html", "text", "all"):
                output = a

        if o in ("-u", "--update"):
            fname = a
#            updateDB(fname)
            sys.exit()
    print "type:", type
    print "number: ", number
    print "checkout: ", checkout

    nvd_db=MySQLdb.connect(user='nvd', passwd="????????????",db="nvd")
    nvd_dbc=nvd_db.cursor()

    if type in ("inputbuffer", "inputbound", "access", "design", "exception",
                "env", "config", "race", "other"):
        sqlquery = """SELECT seq FROM entry
                      WHERE %s = 1 AND th_state = 'none'""" % type
        #print nvd_dbc.info;
        nvd_dbc.execute(sqlquery)
    else:
        sqlquery = """SELECT seq FROM entry
                      WHERE th_state = 'none'"""

        nvd_dbc.execute(sqlquery)

    unchecked = nvd_dbc.fetchall()

    selected = []
```

```
    #print unchecked[number][0]
    if len(unchecked) < number:
        number = len(unchecked)

    for i in range(number):
#        print unchecked[random.randint(0, len(unchecked))][0]
        selected.append(unchecked[random.randint(0, len(unchecked))][0])

    entry = []
    entries = []

    #
    # fetch references for the selected entries
    #
    for i in selected:
        nvd_dbc.execute("""SELECT * FROM entry WHERE seq = %s""", (i,))
        res = nvd_dbc.fetchone()

        entry = list(res)

        nvd_dbc.execute("""SELECT * FROM ref WHERE seq = %s""", (i,))
        res = nvd_dbc.fetchall()

        entry.append(res)

        entries.append(entry)

    #
    # output to files
    #

#    print entries
    entries.sort()

    datetime = time.localtime()

    if checkout:
        fname = "my-nvd-%s%02d%02d%02d%02d" % (datetime[0], datetime[1], datetime[2],
                                               datetime[3], datetime[4])
        print "Saving to %s." % (nvddir + fname + ".txt/html")

    else:
        fname = "my-nvd-example"
        print "Saving to %s. If you want to check out, use -c option" % fname

    if os.path.isfile(nvddir + fname + ".txt") and checkout:
        sys.exit("File %s exist" % (nvddir + fname + ".txt"))
    else:
        txtfile = open(nvddir + fname + ".txt", 'w')

    if os.path.isfile(nvddir + fname + ".html") and checkout:
       sys.exit("file %s exist" % (nvddir + fname + ".html"))

    else:
        htmlfile = open(nvddir + fname + ".html", 'w')
```

```
    #
    # output text file
    #
    for i in entries:
        txtfile.write("%s n: \n" % i[1])
        txtfile.write("%s Desc: %s\n" % (i[1], i[10]))
        txtfile.write("\n")


    #
    # output html file
    #
    htmlfile.write("""<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
    "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<link href="nvd_style.css" rel="stylesheet" type="text/css" />

</head>
<body>
<div class="leftbar">
<div class="leftbar_text">NVD</div>
</div>
<div class="rightbar"> """)



    for i in entries:

        htmlfile.write("""<div class="rightbar_title">%s%s<a style="color : #f6f0d0;"
            href="http://nvd.nist.gov/nvd.cfm?cvename=%s"<strong>NVD</strong></a>
            <a style="color : #f6f0d0;"href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=%s"
                <strong>CVE</strong></a> </div>\n""" % (i[1], " "*100, i[1], i[1]))

        htmlfile.write("""%s <p> </p>\n""" % (i[10],))

        refs = i[22]

        for ref in refs:
            htmlfile.write("""<a href="%s" target="_blank">%s</a><p></p>\n""" % (ref[2],
            ref[2]))

        htmlfile.write("""<p> </p>\n""")

    htmlfile.write("""</div></body>\n""")

    # mark as checked out in database
    if checkout:
        for i in entries:
            nvd_dbc.execute("""UPDATE entry SET th_state = 'examining' WHERE seq = %s""",
            (i[2],))


if __name__ == "__main__":
    main()
```