



Year-end Report for 2006*

System Access is Top Impact for 2006

The exploit impact possible in the most Secunia advisories published this year is “System impact”, encompassing system compromise and code execution. What does this mean for you? Find out on page 2.

Zero-day bugs infest Microsoft Office

This year was particularly difficult for Microsoft, as ten 0-day vulnerabilities were discovered in their software, six in MS Office alone. Know more about these kinds of attacks on page 6.

Secunia Research Updates

Secunia discovered 75 vulnerabilities this year, a substantial increase from 2005, thanks to a beefed-up security team, and a little library file called “unacev2.dll”. See what else happened with Secunia Research this year on page 9.

Software Inspector: 38.4% of Detected Applications are Insecure

More than a third of all scanned applications by the Secunia Software Inspector were revealed to be insecure versions, corresponding to more than 250,000 installed software. Find out more about on page 13.

Vulnerability Statistics

Secunia published over 5,000 advisories this year. Find out the numbers on Secunia advisories this year in terms of impact and criticality on page 15.

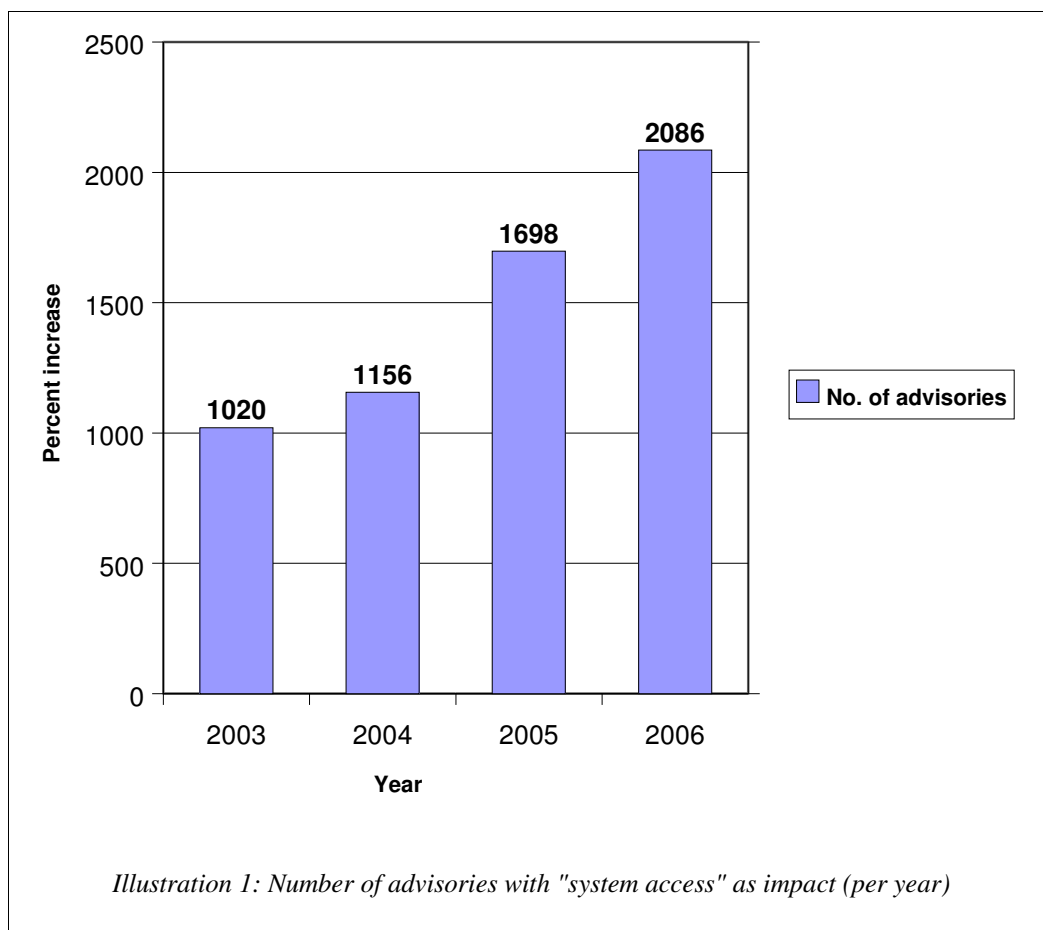
** The information contained within this year-end report covers the period*

from 1 January 2006 to 19 December 2006.

1

System Access is Top Impact for 2006

For 2006, the number one impact for vulnerability exploits was “system access”. What exactly does this term mean, and what does it imply? What is its impact to you, as a system administrator, a top-level manager, a government employee, or even as a home user?



The figure above, gathered from the thousands of vulnerability reports published by Secunia annually, clearly shows a rise in system access. In 2003, when Secunia first started collecting vulnerability intelligence, the end-of-year number of advisories with “system access” as the impact, was 1,020. For 2004, it was 1,156 (an increase of 13%); for 2005, it was 1,698 (an increase of almost 50%). As of this writing, current figures are at 2,086, tagging the increase of advisories at almost 25%.

** The information contained within this year-end report covers the period*

from 1 January 2006 to 19 December 2006.

When a software vulnerability is exploited in such a way as to give the attacker system access to the hacked computer or network, it's basically the same as having your laptop stolen without even noticing it. At once, all the information you have in your computer is suddenly accessible to someone else.

The thousands of vulnerabilities this year that may potentially allow system access were found in a diverse set of products: Internet browsers, mail servers, archiving applications, and media players are only some on the list. Why the diversity? To quote a hungry wolf, "All the more to see you with, my dear".

What hackers want to see, in this case, is the contents of your computer or your network: the installed programs, the users, the confidential information. And not merely to see them either; a hacker with system access can copy the entire contents of your hard drive, add users to the system, or install programs that you know nothing about.

How a hacker is able to exploit the vulnerability depends on the application. Some vulnerabilities, such as those for browsers or client-based applications (media players, instant messaging tools), usually require some sort of user interaction, through social engineering methods. For example, last February, an exploit for Macromedia's (now Adobe) Shockwave player required that users with Shockwave installed in their browsers visit a particular website in which the exploit code was housed. Once they opened the website in their browsers, the vulnerability was exploited.

The figure on the following page shows the software with the greatest number of advisories capable of allowing "system access". Microsoft Office XP and Office 2000 lead with 16 advisories each; while the rest of the list is littered with other Office editions and applications. IE 6.x and 5.01 have 12 and 11 respectively, while Mozilla 1.x has 7.

From the graph, it is worth noting that almost all the applications listed (except for the Novell Open Enterprise Server) are client-based applications, the preferred playground of social engineering tactics. End-users are guaranteed to be present in more computers than, say, server applications, so the pool of possible victims of exploitation is larger.

convenience of online transactions, allowing a hacker to have system access can have serious consequences.

Hence the rise in exploits aiming for “system access”. Knowledge is power, as the old saying goes, but in some instances power translates very loudly to currency. The pool of information found in computers is too much for web criminals to ignore, and the fact that vulnerabilities exist that are easy to exploit (using tools readily downloadable from the Internet) is an opportunity that very few resist.

“System access” may help explain a few tangible phenomena: the appearance of perfect digital copies of movies burned into pirated DVDs even before they’re premiered in theatres. That shopping splurge on Amazon reflected in your credit card bill that you don’t remember going on. And even, if rumours are to be believed, US military secrets such as personnel files from a black market in Afghanistan [2].

Still, software vulnerabilities that may potentially allow system access of unauthorised users are software vulnerabilities just the same. The best practice to prevent such attacks can also help prevent attacks that have other impacts to a computer or network. For companies, user awareness going beyond the “don’t open email attachments” kind is recommended, as is proper training and security tools for IT personnel. Several applications are available in the market that help collect and disseminate vulnerability information that can stop attacks before they even have the chance to happen. Secunia has several corporate solutions for vulnerability management across an entire network. To know more about what Secunia has to offer in the way of enterprise solutions, please visit <http://corporate.secunia.com>.

For home users, fussy as it may seem, there is an urgent need to be vigilant about the software that you use, and vendor-released updates that curb security bugs. There are also several tools freely available on the Internet that can help you organise your software information so that you get up-to-date alerts on new releases, such as the Secunia Software Inspector. To use the Secunia Software Inspector to check the vulnerability status of your most-used applications, please visit http://secunia.com/software_inspector.

[1] <http://www.nysun.com/article/44133>

[2] <http://www.engadget.com/2006/04/13/flash-drives-containing-us-military-secrets-for-sale-next-to-afg/>

Zero-day bugs infest Microsoft Office

Ten vulnerabilities were discovered in various Microsoft applications via zero-day attacks this year, six in Microsoft Office alone. Zero-day attacks are characterised by the active exploitation of a vulnerability before its public disclosure. The exploit code can then be used by hackers to create malware, which they then send out via email, or upload to websites that they entice users to visit.

Advisory name	Date published
Microsoft Word Unspecified Code Execution Vulnerability	2006-12-11
Microsoft Word Memory Corruption Vulnerabilities	2006-12-06
Microsoft XMLHTTP ActiveX Control Code Execution Vulnerability	2006-11-04
Microsoft Visual Studio WMI Object Broker ActiveX Control Code Execution	2006-11-01
Microsoft Vector Graphics Rendering Library Buffer Overflow	2006-09-19
Microsoft Word Code Execution Vulnerabilities	2006-09-05
Microsoft Visual Basic for Applications Buffer Overflow	2006-08-08
Microsoft PowerPoint Code Execution Vulnerabilities	2006-07-14
Microsoft Excel Multiple Code Execution Vulnerabilities	2006-06-16
Microsoft Word Malformed Object Pointer Vulnerability	2006-05-19

Table 1: 0-day Secunia Advisories for 2006

Of the six in Microsoft Office, four are for MS Word, one for MS Excel, and one for PowerPoint. The other vulnerabilities were located in XMLHTTP, Visual Studio, Visual Basic, and in the Vector Graphics Rendering library. Successful exploitation of the vulnerabilities may result in the execution of arbitrary code.

In the case of the most recent Word 0-day vulnerabilities, malware discovered in the wild that used them were found to be mostly Trojan downloaders, which can be configured to automatically download any file from the Internet. It's the use of the word "any" that should be cause for concern. It can mean a password-cracker, a snooping program, a tool that records all keystrokes and screenshots; you name it, there's software and hacking toolkits available for it.

With malware and security attacks veering away from the call for infamy, and into the darker, seedier world of hacking-for-profit, the trend has shifted from spreading to as many computers as possible, or making as big a splash as possible, to discreetly stealing sensitive information from specific, limited targets.

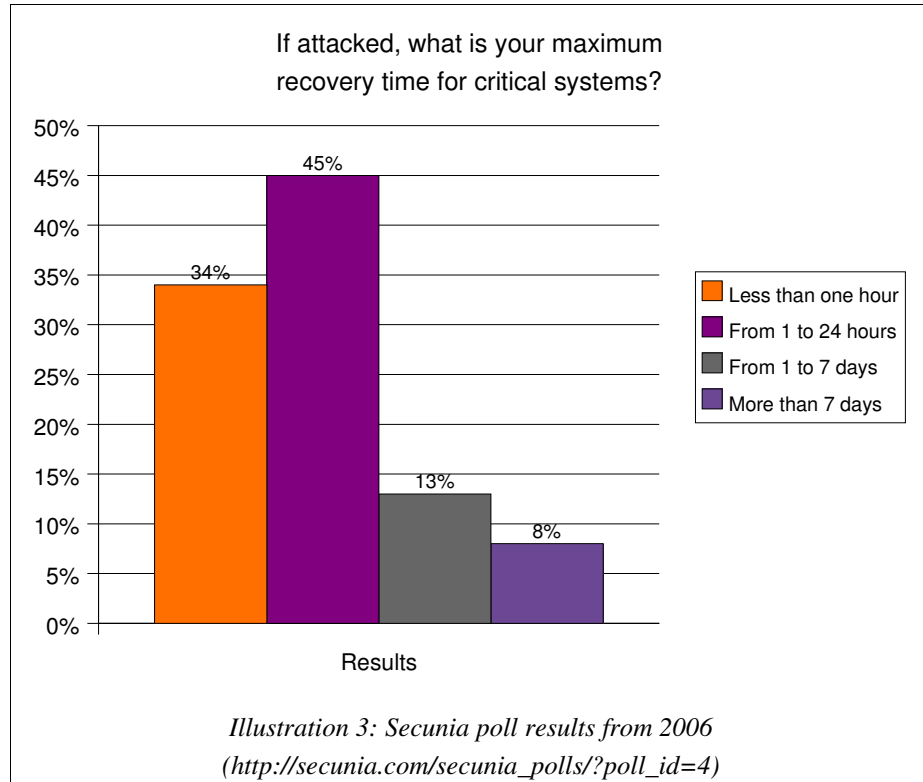
** The information contained within this year-end report covers the period*

from 1 January 2006 to 19 December 2006.

Microsoft used the exact same terms to explain the attack vector of the latest MS Word 0-day vulnerabilities. It would be erroneous to think that the words “specific” and “limited” are no cause for concern. On the contrary, opening a Word document that you receive in your email, and finding out that various password-stealing Trojans have infiltrated your system arguably has a much bigger impact than having your computer conk out for a couple of hours and having the tech guys patch it up and fix it.

In the case of widespread virus attacks, security researchers had plenty of malware samples to study. Their behaviour and infection methods were fixed, and comprehensive signatures could be developed to identify them.

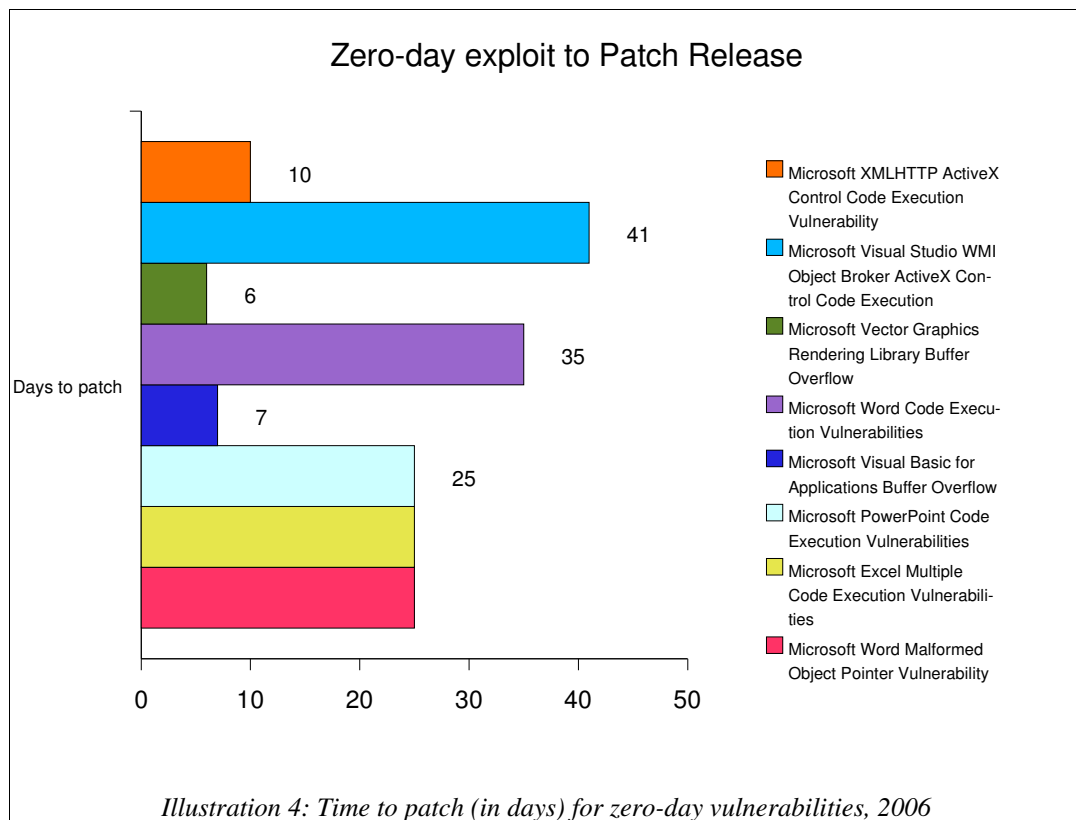
But for limited targeted attacks, the samples are few and far between. Information about such attacks for 0-day vulnerabilities are often hard to come by, as researchers often don't have enough samples to take an in-depth look at. And so, victims of such an attack, if they are even aware of such an attack taking place, often have to assume the worst: the attack may have yielded your social security number, your banking details, your network username and password, or any other sensitive information that you house in your computer, to a malicious person.



* The information contained within this year-end report covers the period from 1 January 2006 to 19 December 2006.

According to a poll conducted this year by Secunia on its community web site, the maximum recovery time that most users were willing to spend when their systems are attacked was between 0 to 24 hours.

Unfortunately, this scenario has not been visible in this year's attacks. Of the nine 0-day vulnerabilities, the fastest-released patch (for VML) took six days, while it took 41 days to patch the Visual Studio vulnerability. In addition, the latest two Word vulnerabilities remain unpatched to this day.



For 0-days attacks, the most important currency is information. On a corporate level, IT support personnel are advised to organise vulnerability information in such a way as to effectively obtain, process, and disseminate information within their IT infrastructure. Secunia has several enterprise solutions available for this exact task. To know more about Secunia and our corporate products, please visit <http://corporate.secunia.com/>.

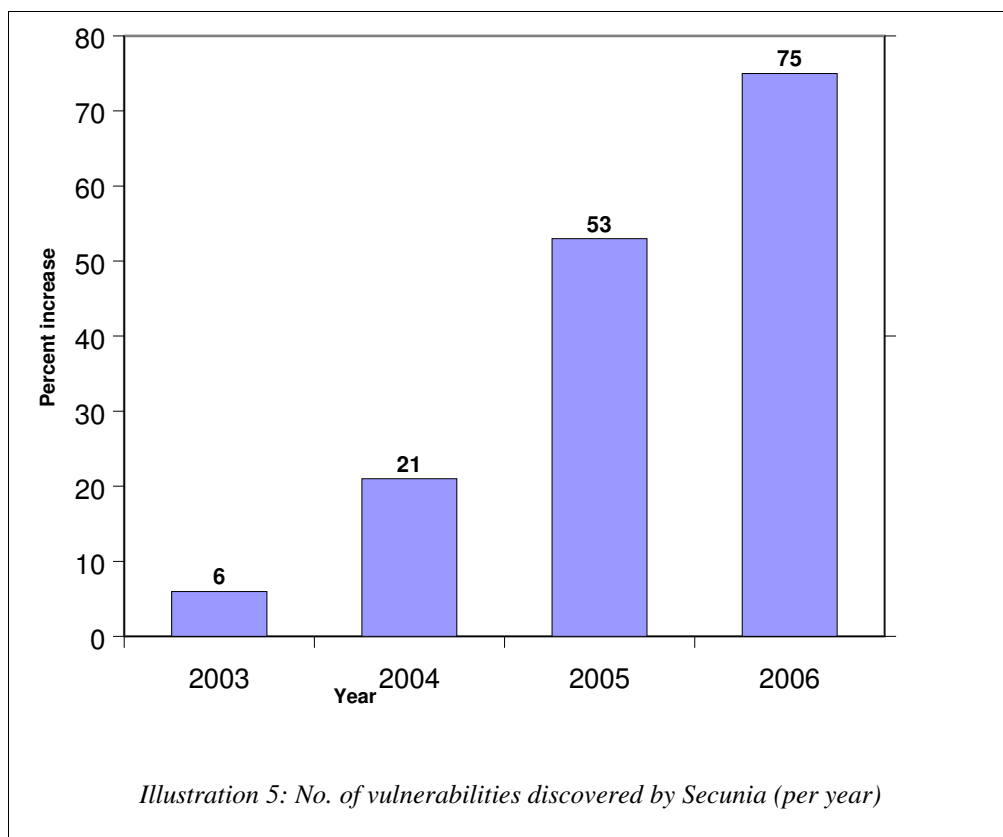
** The information contained within this year-end report covers the period*

from 1 January 2006 to 19 December 2006.

Secunia Research Updates

This year, Secunia Research was responsible for the discovery of seventy-five vulnerabilities, seventy of which have been publicly disclosed, and five of which are pending disclosure and are currently being coordinated with the vendor.

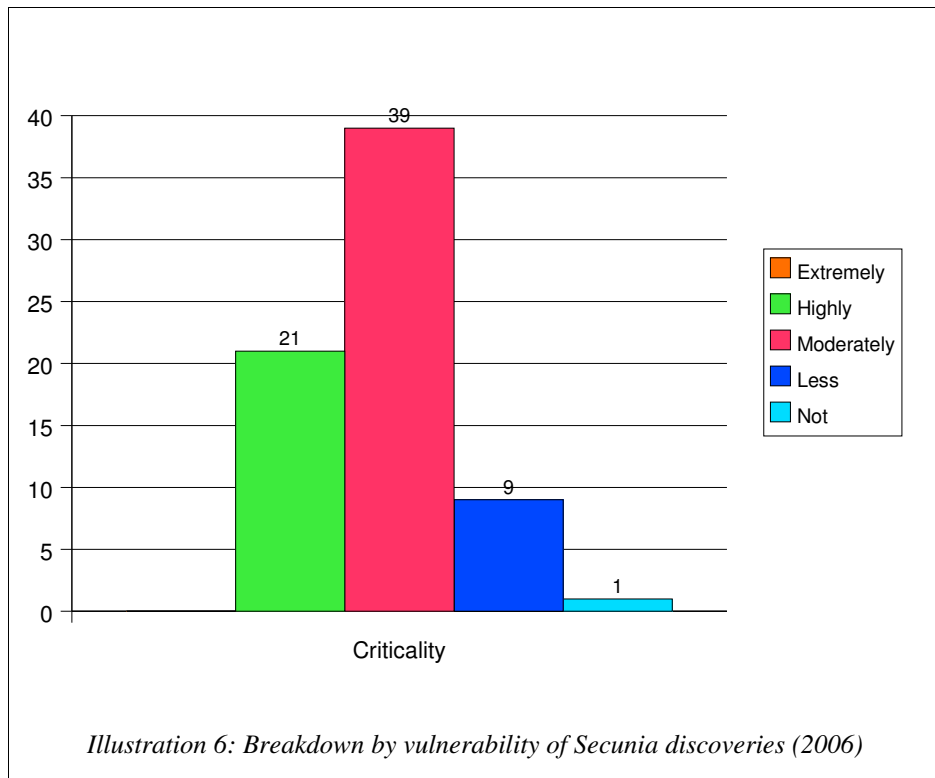
These figures represent an all-time high from last year, in which fifty-three discoveries were published by the year end.



Among the vulnerabilities discovered by Secunia this year, 21 were deemed “highly critical”, 39 were “moderately critical”, 9 were “less critical”, and 1 was tagged as “not critical”. For more information on how Secunia distinguishes the criticality of a vulnerability, please visit http://secunia.com/about_secunia_advisories/.

** The information contained within this year-end report covers the period*

from 1 January 2006 to 19 December 2006.



Carsten Eiram, a Senior Security Analyst with Secunia, credits two factors for this year's record. One was the discovery in late 2005 of a vulnerability in “unacev2.dll”, a DLL file that's part of the UNACE Dynamic Link Library. Back in September 2005, a Secunia researcher had discovered a vulnerability in this file as it was used in the ALZip archive application.

The vulnerable file was part of a library commonly used in archiving applications to decompress ACE files. As a matter of fact, before 2005 ended, two more archiving applications were found to contain the same DLL file.

In early 2006, Secunia Research established their File Signatures database, that currently contains over 100,000 rules that can be used to identify files from over 4,000 applications. Because “unacev2.dll” was used in three known archiving applications, Secunia researchers decided to try out the File Signatures database in the hopes of discovering other vulnerable tools. They were correct.

From May to September of 2006, as their database grew in number, Secunia Research discovered the vulnerable DLL in fifteen more archiving tools. With the sheer number of software being developed daily by programmers, the task of manually keeping

** The information contained within this year-end report covers the period*

from 1 January 2006 to 19 December 2006.

track of and detecting the file could have been daunting. Instead, by dipping into the pool of Secunia technology, researchers were able to provide vulnerability information without breaking a sweat.

Table 2: List of Secunia-discovered vulnerabilities due to "unacev2.dll" buffer overflow

Advisory Name	Date of Disclosure
ALZip ACE Archive Handling Buffer Overflow	2005-09-07
WinRAR Format String and Buffer Overflow Vulnerabilities	2005-10-11
ZipGenius Multiple Archive Handling Buffer Overflow	2005-10-21
Servant Salamander unacev2.dll Buffer Overflow Vulnerability	2006-04-28
WinHKI unacev2.dll Buffer Overflow Vulnerability	2006-05-01
ExtractNow unacev2.dll Buffer Overflow Vulnerability	2006-05-02
Anti-Trojan unacev2.dll Buffer Overflow Vulnerability	2006-05-08
PowerArchiver unacev2.dll Buffer Overflow Vulnerability	2006-05-08
Where Is It unacev2.dll Buffer Overflow Vulnerability	2006-05-09
FilZip unacev2.dll Buffer Overflow Vulnerability	2006-05-15
Eazel unacev2.dll Buffer Overflow Vulnerability	2006-05-17
IZArc unacev2.dll Buffer Overflow Vulnerability	2006-05-17
Rising Antivirus unacev2.dll Buffer Overflow Vulnerability	2006-05-30
AutoMate unacev2.dll Buffer Overflow Vulnerability	2006-06-07
BitZipper unacev2.dll Buffer Overflow Vulnerability	2006-07-17
ZipTV ARJ Archive Handling and unacev2.dll Buffer Overflows	2006-09-07

The other factor that contributed to the success of Secunia Research this year was the development of new Secunia technologies. This year saw the launch of the File Signatures database (as discussed earlier), Binary Analysis, and Exploit Code development.

Binary analysis is a technology specially developed for security vendors and partners who are particularly conscious about the exact cause of software vulnerabilities. Secunia researchers specialising in disassembling and debugging take an in-depth look at vulnerabilities for critical and popular software, peering into the source code and determining the practical exploitability of a software flaw, and if necessary, creating exploit codes or proof-of-concept (PoC) codes for it. As a result, security vendors can create more generic rules to identify the same vulnerability in exploits created in the future. Secunia researchers also have the opportunity to discover more vulnerabilities as their in-depth perspective allows them to carefully scrutinize every line of code.

** The information contained within this year-end report covers the period*

from 1 January 2006 to 19 December 2006. 11

Security clients who opt to take advantage of Secunia's Exploit Code development tools are privy to the PoCs developed in-house by Secunia that aim to prove the actual impact of vulnerabilities.

To carry out these tasks, Secunia has added several well-trained researchers and engineers to the team. Secunia users can thus expect improvements in existing products, and more discovered vulnerabilities. Secunia aims to not only be the leading provider of vulnerability intelligence, but also the leading provider of in-depth vulnerability analysis.

Software Inspector: 38.4% of Detected Applications are Insecure

Secunia launched the Software Inspector on its community website last November. The Secunia Software Inspector is a free, specially designed application that can detect what software you have on your computer, if you have the latest available version for that software, and if not, how you can upgrade to the latest version.

Computer users are always reminded that vulnerabilities exist in the programmes that they use; vulnerabilities that can potentially result in lost data, program failure, or even criminal activities, like computer access by unauthorized users, phishing attacks, or information theft. But with the dozens of programs installed in the average computer, trying to keep up with each upgrade is practically impossible. To do so would require that one check vendor websites regularly, and surf the Internet for news on software vulnerabilities. Unless you're a network administrator, this task just isn't very practical.

Hence, Secunia developed the Software Inspector. What takes several hours on the Internet only takes the Software Inspector a few seconds to do.

The Software Inspector detects the most popular software that fall under the following categories:

- Internet browsers
- Internet browser plug-ins
- Instant Messaging clients
- Email clients
- Media players
- Windows updates

To detect what software you have on your computer, Secunia uses its File Signature technology, which is composed of carefully programmed rules used to identify installed applications, and their exact versions on Windows-based systems.

To detect if your software version is the latest non-vulnerable version available from the vendor, the Software Inspector uses Secunia Advisory Intelligence technology, which Secunia has been providing to the global IT community for over four years.

Use of the Secunia Software Inspector is absolutely free. In addition, users who sign

up for the Referral Programme are allowed access to additional data on Software Inspector statistics, such as the most popular software, or upgrade figures for a certain product.

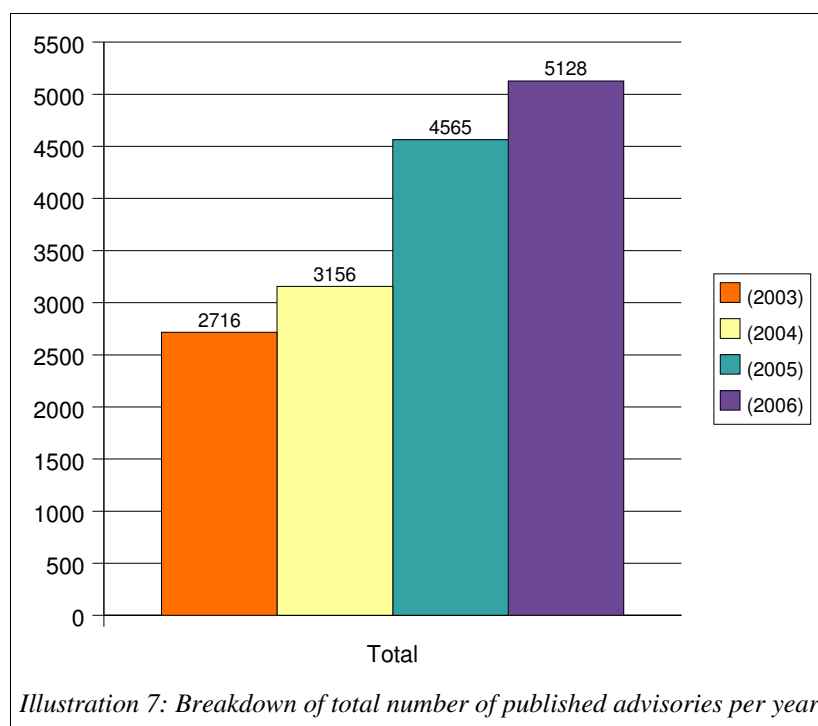
From over 700,000 applications detected, about 38.4% were insecure versions. For more detailed statistics, please visit: http://secunia.com/software_inspector_statistics/

Users are also encouraged to spread word of the Secunia Software Inspector on their websites – after all, it was designed with the primary goal of emphasizing how important it is to make sure that you run secure software on your computers. To know more about Secunia and our solutions for open communities and the media, please go to <http://secunia.com>.

The Secunia Software Inspector can be accessed at:
http://secunia.com/software_inspector

Vulnerability Statistics

Total Number of Published Advisories



This year, Secunia published over five thousand advisories bringing the total number of advisories in Secunia's vulnerability intelligence database to more than 15,500. Vulnerability advisories can be viewed at <http://secunia.com>, which has had over 5 million unique visitors this year alone. The most viewed advisories for the year are shown below.

Advisory ID	Advisory Title
22477	Internet Explorer 7 "mhtml:" Redirection Information Disclosure
18680	Microsoft Internet Explorer "createTextRange()" Code Execution
19521	Internet Explorer Window Loading Race Condition Vulnerability
18963	Mac OS X File Association Meta Data Shell Script Execution
18255	Microsoft Windows WMF "SETABORTPROC" Arbitrary Code Execution
20153	Microsoft Word Malformed Object Pointer Vulnerability
19738	Internet Explorer "mhtml:" Redirection Disclosure of Sensitive Information
19631	Firefox Multiple Vulnerabilities
21910	Internet Explorer Multiple Vulnerabilities
18700	Firefox Multiple Vulnerabilities

Table 3: Most popular advisories for 2006

** The information contained within this year-end report covers the period
from 1 January 2006 to 19 December 2006.*

Criticality

For 2006, almost all advisories were either highly, moderately, or less critical; leaving the most dangerous and least dangerous vulnerabilities at a minimum.

The criticality for a certain vulnerability is based on Secunia's assessment of the vulnerability's possible impact on a system or network, the availability of a vendor-issued solution or patch, the description of workarounds if available, and if an exploit exists for the vulnerability.

Secunia uses a rating system containing five different levels of criticality:

Extremely Critical

This level is typically used for remotely exploitable vulnerabilities, which can lead to system compromise. Successful exploitation of the vulnerability does not normally require any interaction, and the vulnerability is already being actively exploited (or exploits are publicly available). These vulnerabilities can e.g. exist in services like FTP, HTTP, and SMTP or in certain client systems like email programs or browsers.

Highly Critical

This level is typically used for remotely exploitable vulnerabilities, which can lead to system compromise. Successful exploitation of the vulnerability does not normally require any interaction but there are no known exploits available at the time of disclosure. Such vulnerabilities can exist in services like FTP, HTTP, and SMTP or in client systems like email programs or browsers.

Moderately Critical

Typically used for remotely exploitable Denial of Service vulnerabilities against services like FTP, HTTP, and SMTP, and for vulnerabilities, which allows system compromises but require user interaction. This rating is also used for vulnerabilities allowing system compromise on LANs in services like SMB, RPC, NFS, LPD and similar services, which are not intended for use over the Internet.

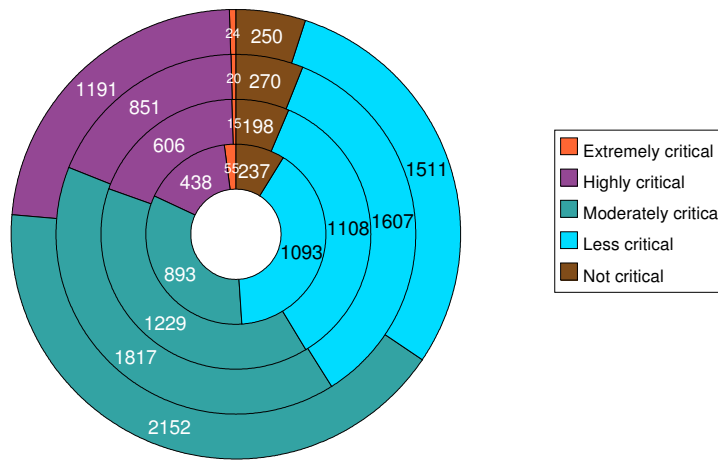
Less Critical

Typically used for cross-site scripting vulnerabilities and privilege escalation vulnerabilities. This rating is also used for vulnerabilities allowing exposure of sensitive data to local users.

Not Critical

Typically used for very limited privilege escalation vulnerabilities and locally exploitable Denial of Service vulnerabilities. This rating is also used for non-sensitive system information disclosure vulnerabilities (e.g. remote disclosure of installation path of applications).

*Illustration 8: Breakdown by criticality of all advisories published from 2003-2006
(innermost ring is 2003; outermost ring is 2006)*



Moderately critical vulnerabilities led the pack with 2,152 advisories with year, followed by less critical vulnerabilities, with 1,511, highly critical with 1,191, not critical, with 250, and extremely critical with 24; mostly zero-day attacks that had actively used exploits. The same trend can be seen, on average, for the previous years.

In terms of percent increase per criticality, the graph below shows the behaviour of each criticality over the years. Between 2004 and 2005, a positive surge for each criticality can be seen, which may be an indication of the increase interest in security-focused research. Secunia Research also made use of additional resources to boost vulnerability analysis.

	2003/2004	2004/2005	2005/2006
Extremely critical	-72.73%	33.33%	20.00%
Highly critical	38.36%	40.43%	39.95%
Moderately critical	37.63%	47.84%	18.44%
Less critical	1.37%	45.04%	-5.97%
Not critical	-16.46%	36.36%	-7.41%

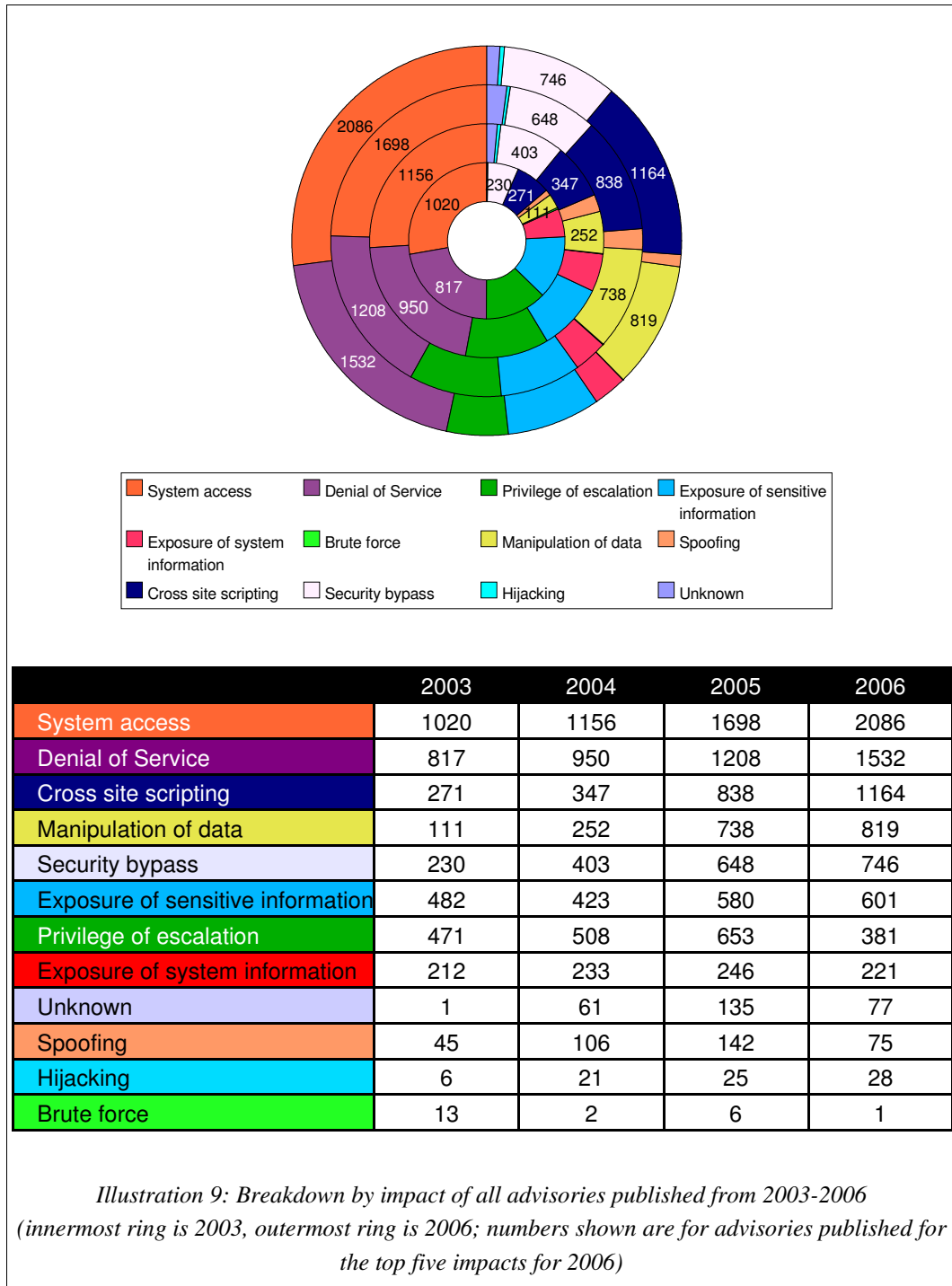
Table 4: Breakdown by percent increase of the criticality of all published advisories from 2003 to 2006

Throughout the last four years, highly critical and moderately critical advisories have always enjoyed an increase in number, which supports the idea that system access is a consistently profitable and successful attack vector.

** The information contained within this year-end report covers the period from 1 January 2006 to 19 December 2006.*

Impact

The number of advisories listing “system access” as a possible impact is at 2,086 this year, more than 500 advisories more than the next impact with the most number of advisories.



** The information contained within this year-end report covers the period from 1 January 2006 to 19 December 2006.*

The graph above shows a breakdown over the past four years of the different impacts that vulnerabilities can have on a system, and which are indicated in Secunia advisories:

Brute force

This impact is used in cases where an application or algorithm allows an attacker to guess passwords in an easy manner.

Cross-Site Scripting

Cross-Site Scripting vulnerabilities allow a third party to manipulate the content or behaviour of a web application in a user's browser, without compromising the underlying system. Different Cross-Site Scripting related vulnerabilities are also classified under this category, including "script insertion" and "cross-site request forgery".

Cross-Site Scripting vulnerabilities are often used against specific users of a website to steal their credentials or to conduct spoofing attacks.

DoS (Denial of Service)

This includes vulnerabilities ranging from excessive resource consumption (e.g. causing a system to use a lot of memory) to crashing an application or an entire system.

Exposure of sensitive information

This impact is used for vulnerabilities where documents or credentials are leaked or can be revealed either locally or from remote.

Exposure of system information

This impact is used for vulnerabilities where excessive information about the system (e.g. version numbers, running services, installation paths, and similar) are exposed and can be revealed from remote and in some cases locally.

Hijacking

This covers vulnerabilities where a user session or a communication channel can be taken over by other users or remote attackers.

Manipulation of data

This includes vulnerabilities where a user or a remote attacker can manipulate local data on a system, but not necessarily be able to gain escalated privileges or system access. The most frequent type of vulnerabilities with this impact are SQL-injection vulnerabilities, where a malicious user or person can manipulate SQL queries.

Privilege escalation

This covers vulnerabilities where a user is able to conduct certain tasks with the privileges of other users or administrative users. This typically includes cases where a local user on a client or server system can gain access to the administrator or root account thus taking full control of the system.

** The information contained within this year-end report covers the period*

from 1 January 2006 to 19 December 2006. 19

Security Bypass

This covers vulnerabilities or security issues where malicious users or people can bypass certain security mechanisms of the application. The actual impact varies significantly depending on the design and purpose of the affected application.

Spoofing

This covers various vulnerabilities where it is possible for malicious users or people to impersonate other users or systems.

System access

This covers vulnerabilities where malicious people are able to gain system access and execute arbitrary code with the privileges of a local user.

Unknown

This impact is used when covering various weaknesses, security issues, and vulnerabilities not covered by the other impact types, or where the impact isn't known due to insufficient information from vendors and researchers.

	2003/2004	2004/2005	2005/2006
System access	13.33%	46.89%	22.85%
Denial of Service	16.28%	27.16%	26.82%
Cross site scripting	28.04%	141.50%	38.90%
Manipulation of data	127.03%	192.86%	10.98%
Security bypass	75.22%	60.79%	15.12%

Table 5: Breakdown by percent increase of the top 5 impacts of all advisories published from 2003 to 2006

The graph above shows the percent in increase of the top five impacts for 2006. Each impact has displayed a positive increase, with the top increase this year coming from “cross site scripting”. However, it is important to note that the top number of impact for all advisories this year is “system access”, as it has been the last few years. This trend is, again, an indication of the profitability of Internet crime.