Secunia

Stay Secure

2008 Report

Table of Contents

Letter From the CEO
2008 proved to be another busy year

Dear customers and partners,

Welcome to Secunia's 2008 Annual Report.

What is probably more interesting for our customers than the sheer number of vulnerabilities reported in 2008 is the uptake in exploitation with a criminal purpose; especially the apparent change of focus from vulnerabilities in Microsoft products to a broader focus on popular software from other vendors.

With Microsoft's focus on regular patching and automatic installation of security-related updates via Windows Update, it is of no surprise that the criminals see their window of opportunity shrinking and, thus, seek new paths with non-Microsoft software.

Statistics from the Secunia PSI clearly show that a very large proportion of new PSI users have very old non-Microsoft software with several known vulnerabilities, thus handing criminals the opportunity to exploit these well-documented vulnerabilities for which "reliable" exploits are readily available.

As we proved with our test of various Internet Security Suites in October 2008, there is little help to get from these products. While the AV industry may do a good job catching the malicious payload (e.g. trojans), which the criminals install when exploiting vulnerabilities, they fail to detect the actual exploitation. This makes it only a question of changing the payload to avoid detection by the AV software.

Therefore, it is more important than ever to educate users and businesses to patch all their software in a timely manner. The criminals adapt to the changes and so must businesses and consumers if they do not want to fall victim.

At Secunia, we strive to ensure that both businesses and consumers have access to highly effective tools and verified Vulnerability Intelligence, which helps identifying all known vulnerabilities as well as to offer information about solutions and workarounds to prevent exploitation.

Not only did our services and research do great last year. So did Secunia as a business and, in line with previous years, we came out profitable and expanded significantly through 2008.

This means that Secunia still has an excellent and unmatched track record and is growing organically without any external funding.

In January 2009, we moved into our newly built headquarters where we have room for further expansion, and we expect to increase the headcount in 2009, both within research, development, and sales.

Stay Secure,
Niels Henrik Rasmussen

Secunia
Stay Secure

Vulnerability Research

Secunia is dedicated to vulnerability research and was the leading contributor during 2008

Essential vulnerability research

Vulnerability research is essential to root out the security-related flaws in software. Over the years, research in vulnerabilities has forced vendors like Microsoft to launch initiatives to improve the quality of their code, simply because old coding habits failed to take into account that errors, which may seem like bugs in the eyes of the user, could be exploited by criminals to gain control of the system.

Today, the legitimate research conducted by hundreds of security enthusiasts and security professionals comprises the majority of all disclosed vulnerabilities and a smaller number is discovered by criminals. This constant effort by the community to discover new vulnerabilities raises the bar for the criminals and forces the software vendors to realise the need for improving their overall code quality.

At Secunia, we also conduct a significant amount of research not only to contribute to the community and the overall security of software, but also for internal education and motivation. Secunia staff, who continue to prove a good track record of discovering new vulnerabilities are given dedicated work time to conduct research.

How much does the vulnerability industry contribute?

This year, we decided to check out how some of the "old" players in the vulnerability field fare when it comes to in-house vulnerability research. We decided to only consider companies with a certain historical track record and to only count "System Access" vulnerabilities with a "remote" vector in fairly popular software of relevance to enterprises. To ensure a fair comparison, we decided to only count CVE entries despite CVE not being the most accurate measurement, as a single CVE identifier may cover more than one actual vulnerability.

Generally speaking, "System Access" vulnerabilities with a "remote" vector are the most hard-to-find, since everybody wants to find them. They are also the most critical vulnerabilities when taking into account both the security of individual systems and entire networks.

Company	Vulnerabilities
Secunia	44
iDefense Labs	24
IBM/ISS	15
Google Security	13
NGS Software	12
CoreSecurity	12
Fortinet	9
DVLabs	8
CERT/CC	6
McAfee Avert Labs	5

Table 1: *"System Access" vulnerabilities discovered in popular software.*

When counting vulnerabilities, we chose to count CVE references with a "remote" vector, which allows remote code execution, "System Access", in popular products.

Note: When counting vulnerabilities, we did not consider individual researchers (many with impressive track records) simply because we only wanted to compare companies.

Software Inspection Results

Results from Secunia's Software Inspector solutions, based on inspections conducted during 2008

Secunia Software Inspector solutions

Secunia is proud to be the inventor of a technology which can truly help people track all the missing security updates for their software, a task which is literally impossible without an automated tool. Very few users are willing to put in the effort it takes to track every single software installation on a system and correlate it with vulnerability information from sources like Secunia.

The Secunia Software Inspector solutions simply list all the unpatched applications and provide direct download links to the relevant patches and upgrades.

Secunia PSI

The features and functionality of the Secunia Personal Software Inspector (PSI) are praised by many, see the next page.

Below is a table with information about the number and percentage of unpatched installations of various popular applications for Secunia PSI users based on the last scan of each Secunia PSI installation.

Software	Number of Installations, percent	
Sun Java JRE 1.6.x/6.x	1,771,802	48%
Adobe Flash Player 9.x	1,462,284	48%
Sun Java JRE 1.5.x/5.x	502,859	96%
Adobe Reader 8.x	410,786	24%
Apple Quicktime 7.x	381,088	38%
Macromedia Flash Player 6.x	368,775	83%
WinRAR 3.x	348,108	38%
Mozilla Firefox 2.0.x	346,614	34%
7-Zip 4.x	295,312	26%
Java Web Start 5.x	250,453	66%

Table 2: *Top ten most commonly detected applications based on the Secunia PSI results in 2008.*

The numbers for the Secunia PSI show a very positive development, but they also clearly show that too many users give up patching software when it is not straightforward.

Many choose to handle the applications that are easy-to-patch, whereas the applications that take longer or are difficult to patch are simply ignored.

Figures such as 83% insecure for Flash Player 6.x and 96% for Sun Java JRE installations clearly indicate this. Users have generally been quite willing to patch Adobe Reader 8.x; only 24% of these installations are insecure.

Comparing this with the figures for Internet Explorer 7, Microsoft .NET Framework 2.x, and other core Windows patches grouped under Windows XP Professional clearly shows that the easier it is to patch, the more people actually end up doing it, and this even goes for the relatively security-conscious people using the Secunia PSI. The statistics are bound to be even worse for all those not yet using the Secunia PSI.

But even Microsoft has problems getting users to patch. Some 44% of all Word 2003 installations are vulnerable and the reason is obvious: Windows Update only covers certain Microsoft products. For a better coverage users need to install Microsoft Update.

Secunia
Stay Secure

Secunia OSI

The data collected from the Secunia Online Software Inspector (OSI) is a bit different.

Rather than taking the last scan of every registered installation, like we did with the Secunia PSI, we count all the actual scans conducted with the Secunia OSI. Thus, these figures tell something about the time it takes users to patch an application. Generally speaking, the larger the percentage, the longer it takes before users actually patch.

Again, it is clear that Microsoft products are patched very frequently: 7% of all scans found unpatched Internet Explorer 7 installations and only 1% unpatched Windows Media Player. The significant difference can be explained by the fact that more Microsoft Patch Tuesdays included patches for Internet Explorer than for Windows Media Player.

Software	Number of Installations,	percent insecure
Sun Java JRE 1.6.x/6.x	2,831,001	38%
Adobe Flash Player 9.x	2,389,661	34%
Adobe Reader 8.x	1,836,982	8%
Apple QuickTime 7.x	1,205,226	27%
Mozilla Firefox 2.0.x	544,384	14%
Sun Java JRE 1.5.x/5.x	473,783	97%
Mozilla Firefox 3.0.x	400,721	10%
Macromedia Flash Player 6.x	383,884	81%
iTunes 7.x	357,439	5%
Adobe Reader 7.x	297,827	15%

***Table 3**: Top ten most commonly detected applications based on the Secunia OSI in 2008.*

While we can tell that most Secunia PSI and Secunia OSI users do patch a lot of their software, we still have work to do, or rather, the software vendors still have a lot of work to do: Apparently their software is too hard to patch, resulting in too many of their users giving up.

Software Inspection Results
Endorsements for the Secunia Personal Software Inspector

Awards for the Secunia PSI

The Secunia PSI has received a large number of awards and endorsements from leading sources worldwide.

Download.com, the world's largest download site, has chosen Secunia Personal Software Inspector as one of "The best new Windows programs of 2008". A total of six programs received this fine predicate.

Download.com also awarded Secunia PSI an editorial rating of five stars, which is their highest honours and a remarkable recognition.

Quote from 5-star award from CNET

Secunia keeps your apps up-to-date

Not only does Secunia Personal Software Inspector provide extensive details on the software installed on your computer, it also gives you direct links to update programs that are older and potentially not secure.

Secunia's plain language for instructions and explanations enhances the already robust update package, making this a highly recommended freeware.

Quote from ZDNet

Ten free security utilities you should already be using

Number one is the Secunia Personal Software Inspector, quite possibly the most useful and important free application you can have running on your Windows machine.

Quote from 101 Fantastic Freebies from PC World

Editor's review of the Secunia PSI

Here's one of the best ways to optimize your PC: Make sure that all of your applications are patched and up-to-date. That way, they'll run faster and be more secure, and so will your PC. Unfortunately, visiting the Web site of every one of your applications can be so time-consuming that you'll never get around to doing it. So instead, get this freebie. It scans your system, lists all of your applications, and regularly checks if any don't have security patches. When it finds a patch, it applies it.

The best protection against online bank heist is to keep all your software updated. Not just your operating system, but all your 3rd-party software.
The Danish Bankers Association

The top-10 exploited vulnerabilities under Microsoft Windows Vista all came from 3rd-party software.
The Security Intelligence Report vol. 5 from Microsoft

Secunia
Stay Secure

Secunia Research Highlights
Another impressive year for Secunia Research

Secunia Research
Secunia Research has prepared 64 research papers to cover the vulnerabilities discovered by Secunia Research during 2008. These papers cover vulnerabilities in a variety of products, many of which are from high profile vendors. At the time of writing, 13 papers have not yet been published as they await coordination with the vendor.

Vendor	2008 Research papers	2007 Research papers
Trend Micro	8	0
Microsoft	4 (2)	7 (1)
IBM	4 (2)	4
Novell	3	1
Evolution	3	1
HP	3 (1)	2
Sun	2	0
Adobe	1	2
Samba	1	2
Apple	1	1

Table 4: Note: Total number of research papers for each vendor, with numbers in parenthesis indicating research papers awaiting disclosure.

A shift in focus
In 2007, we published 7 papers covering vulnerabilities in Symantec products and 3 in CA products. In 2008, we shifted focus from these security vendors and decided to take a quick look at Trend Micro products instead. In fact, we had a month where our researchers competed to find the most interesting Trend Micro vulnerability. The prize was the much desired SAID 31337 (hacker language for "elite").

The Trend Micro vulnerabilities described in SA31337 and SA31583 required an in-depth analysis of the inner workings of the HouseCall ActiveX control and are a brilliant example of the effort and skill behind some of the findings by the Secunia Research team.

Critical Internet Explorer vulnerability
Secunia also succeeded in finding the first IE vulnerability that was deemed "Critical" by Microsoft in all supported versions of IE from 5.01 to 7, for all operating systems from Windows 2000 to Windows 2008 Server. The vulnerability is in a core functionality of IE which is shared by all versions on all platforms.

Initially, we did not create a working exploit for this vulnerability as we found that the PoC and our analysis plenty documented that code execution was possible. However, Microsoft responded to Secunia that though it would be fixed, they considered code execution to be only theoretically possible. Naturally, this was not satisfactory for Secunia as we had spent significant time finding and analysing the vulnerability and were thus convinced that it could be exploited.

After just a few hours of work, we could provide Microsoft with a nicely working exploit.

Secunia Advisory Statistics

Secunia advisories during 2008 in terms of 0-days, browser vulnerabilities, impact, and criticality

Method

The statistics shown in this section cover 1st January 2008 to 31st December 2008.

When comparing these statistics to other sources, it is important to keep in mind that the quality and interpretation of data is different depending on who presents it.

Secunia validates and verifies the vulnerability information we gather. In this process, we often arrive at conclusions different from those originally reported because, e.g. other versions or related products are affected, the alleged vulnerability is merely a bug, the software in question is in beta, the report is erroneous and irrelevant, the reported issue already has been described, etc. This naturally makes it difficult to compare our data with the many other sources, who do not conduct equally extensive verification and validation of the vulnerabilities reported.

Number of advisories

In 2008, Secunia published 5,114 advisories making it the second busiest year ever. 5,114 advisories is an increase of 9% compared to 2007 and it is 3% less than in 2006 where we published 5,280 advisories.

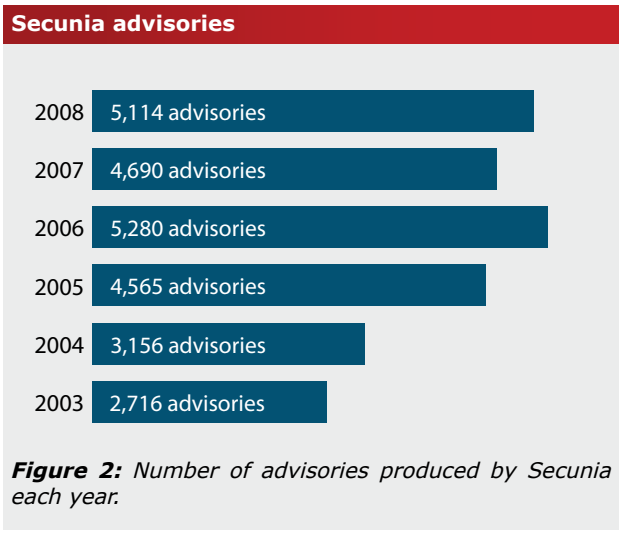


Figure 2: *Number of advisories produced by Secunia each year.*

Secunia
Stay Secure

0-day vulnerabilities

A 0-day vulnerability is a vulnerability that has been exploited in the wild prior to public disclosure of technical details or patches.

0-day vulnerabilities are naturally of particular concern to all of us, because no one has any effective ways to protect against exploitation and everybody running the affected software is a potential victim.

The good news is that the number of 0-days reported has decreased from 20 in 2007 to 12 in 2008.

As in previous years, the primary "target" for the criminals was Microsoft software: A total of 9 0-days in 2008 affected Microsoft software and the remaining three affected 3rd-party ActiveX controls (thus, the vector was still the Microsoft software).

This relatively low number of 0-days indicates that an efficient patch management procedure is capable of keeping most of the bad guys out of your network, since relatively few attacks are actually conducted utilising 0-days.

0-day attacks from 2006-2008

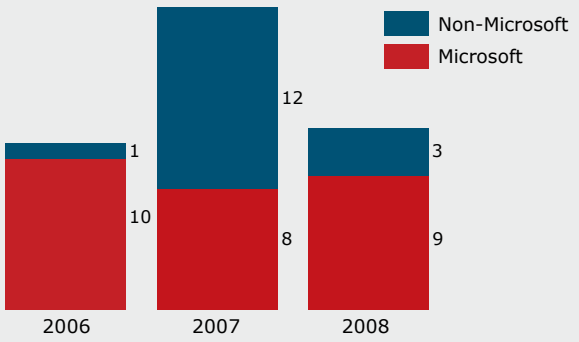


***Figure 1**: In 2006, all but one 0-day case concerned Microsoft vulnerabilities. In 2007, the number of Microsoft-related cases declined to just 8 out of 20 and in 2008, 9 cases out of 12 were Microsoft-related.*

Number of vulnerabilities by browser, 2008

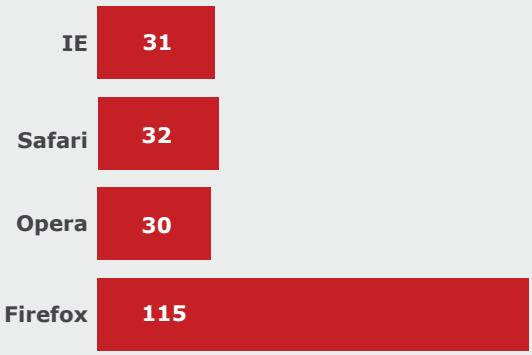


Figure 3: *Number of vulnerabilities for four of the most popular browsers.*

Number of vulnerabilities by browser plug-in, 2008

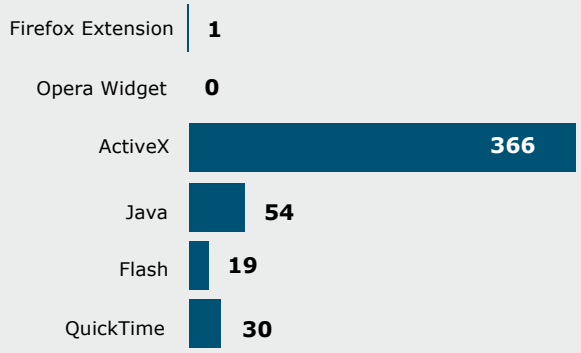


Figure 4: *Number of vulnerabilities in various browser plug-ins and add-ons.*

Web browser vulnerabilities

This year, Secunia published advisories for the four most widely used web browsers: Internet Explorer (IE), Safari, Opera, and Mozilla Firefox.

31 vulnerabilities were reported for Internet Explorer (IE 5.x, 6.x, and 7), including those publicly disclosed prior to vendor patch as well as those included in Microsoft Security Bulletins.

Safari and Opera each had 32 and 30 vulnerabilities, whereas 115 vulnerabilities were registered for Firefox in 2008.

Figure 3 presents an overview of vulnerabilities pertaining to the four most popular browsers.

Browser plug-ins

For browser plug-ins, the number of vulnerabilities in ActiveX controls in 2008 remains by far the most significant, at 366.

ActiveX controls have always been popular in terms of use and abuse. However, the figure took a jump from 2006 (45) to 2007 (339), the latter apparently increased by events such as the Month of ActiveX Controls (MoAXB)[1] and the discovery by Secunia Research of a vulnerable ActiveX component that was used in over 40 different products[2]. The news for 2008 is that the number of vulnerabilities has been even higher, possibly indicating that ActiveX controls are increasingly being targeted by cybercriminals. However, this could also be an indication that more ActiveX vulnerabilities are being found using scanning tools.

Figure 4 contains a summary of the numbers for the different kinds of browser components/ plug-ins that had vulnerabilities this year. While ActiveX controls, widgets, and Firefox extensions can be developed for just about any add-on functionality for a browser, the plug-ins for Java, Flash, and Quicktime plug-ins are developed and maintained by their respective vendors.

1 http://moaxb.blogspot.com

2 http://secunia.com/advisories/23475

Secunia
Stay Secure

Window of exposure

The windows of exposure for threats concerning IE and Firefox are compared in Table 5. This table only displays those vulnerabilities publicly disclosed by a reporter prior to vendor notification. The numbers do not include vulnerabilities responsibly disclosed or discovered internally by the vendor.

Mozilla has released patches for 3 out of 3 Firefox-related advisories, which are all concerning low-risk vulnerabilities.

Microsoft has released patches for 3 out of 6 IE-related advisories, albeit with several serious threats going unpatched for up to as much as 110 days after disclosure.

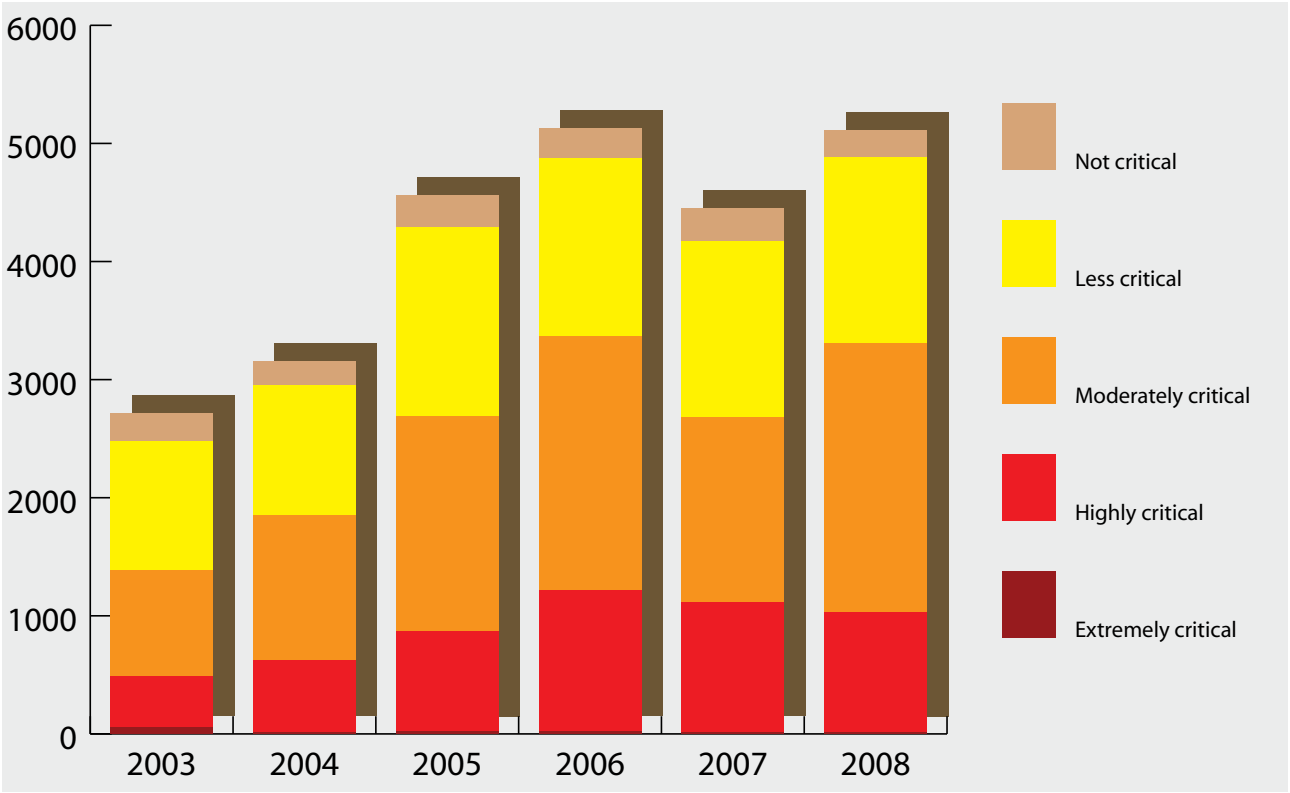
Three low-risk IE-related threats have been left unpatched during all of 2008.

Secunia Advisory ID for disclosed vulnerabilities	Criticality	Disclosure date	Patching date	Number of days before patch release
Internet Explorer				
SA30857	Moderate	2008-06-26	2008-10-14	110
SA30851	High	2008-06-26	2008-10-14	110
SA30145	Not critical	2008-05-12	Unpatched	233
SA30141	Less critical	2008-05-14	Unpatched	231
SA29453	Less critical	2008-03-24	2008-06-10	78
SA29346	Less critical	2008-03-12	Unpatched	294
Mozilla Firefox				
SA32192	Not critical	2008-10-14	2008-13-11	30
SA32040	Not critical	2008-10-01	2008-12-26	86
SA28622	Less critical	2008-01-24	2008-02-08	15

This table considers only those vulnerabilities publicly disclosed without or prior to vendor notification.

The number of days unpatched are in red for those vulnerabilities that are still unpatched as of 31 December 2008.

***Table 5:** Window of exploitation for vulnerabilities publicly disclosed in IE and Firefox, 2008.*



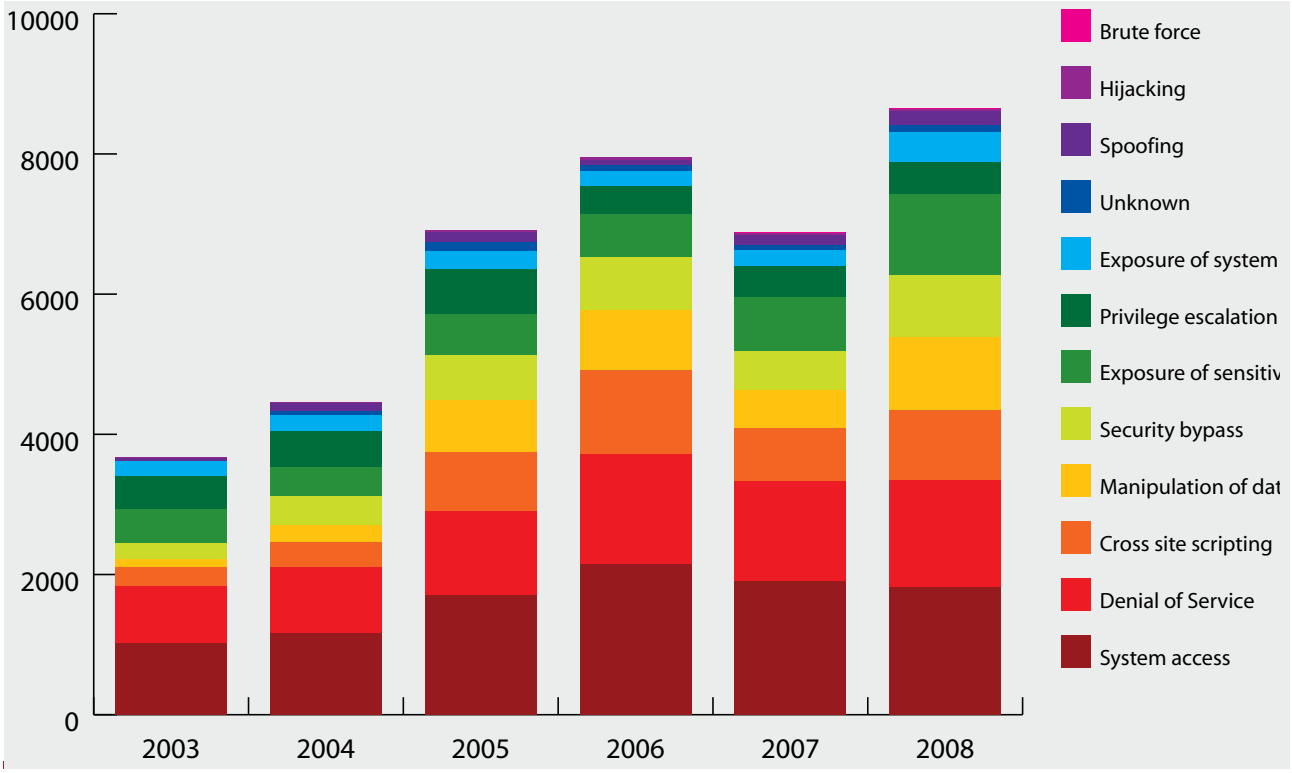
Criticality	2003	2004	2005	2006	2007	2008
Extremely critical	55	15	20	24	2	11
Highly critical	438	606	851	1,191	1,149	1,019
Moderately critical	893	1,229	1,817	2,152	1,675	2,275
Less critical	1,093	1,108	1,607	1,511	1,562	1,576
Not critical	237	198	270	250	290	233

Table 7: *Number of advisories published by Secunia from 2003 to 2008 broken down by criticality. For a description of criticality levels, see Appendix A*

Criticality

The average rating of the advisories has also shifted a bit. There has been a decrease in the number of "Highly Critical" and a significant increase in the number of "Moderately Critical".

In 2008, we set the rating to "Extremely Critical" for a total of 11 advisories, which is a sharp increase from a mere 2 in 2007. This indicates that the 0-days exploited in 2008 could potentially be more effective than the ones we saw in 2007.



Impact	2003	2004	2005	2006	2007	2008
System Access	1,020	1,156	1,698	2,148	1,981	1,814
Denial of Service	817	950	1,208	1,572	1,523	1,538
Cross site scripting	271	347	838	1,196	783	456
Manipulation of Data	111	252	738	845	580	1,162
Security Bypass	230	403	648	763	608	418
Exposure of sensitive information	482	423	580	620	805	13
Privilege escalation	471	508	653	390	452	1,040
Exposure of system information	212	233	246	225	248	192
Unknown	1	61	135	81	119	993
Spoofing	45	106	142	75	152	883
Hijacking	6	21	25	30	32	28
Brute force	13	2	6	1	22	112

Table 6: *Number of advisories published by Secunia from 2003 to 2008 broken down by impact. For a description of impact levels, see Appendix B*

Impact

Compared to 2007, we saw a small decrease in the number of advisories with "System Access" impact. The more radical changes are seen for advisories with "Manipulation of Data", "Cross Site Scripting", and "Exposure of Sensitive Information" impacts. This suggests that a large proportion of the increase in the total number of advisories is related to web applications as compared to 2007.

Appendix A
Criticality rating system

Criticality
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).

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.

Moderately Critical
Typically used for remotely exploitable Denial of Service vulnerabilities and for vulnerabilities which allow system compromises but require user interaction. 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 level is also used for non-sensitive system information disclosure vulnerabilities.

Appendix B
Impact rating system

Impact
Secunia defines the different security impacts as follows:

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 3rd-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".

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.

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 is unknown due to insufficient information from vendors and researchers.

Secunia • Weidekampsgade 14 A • DK-2300 Copenhagen S • Denmark • Tel: +45 7020 5144 • Fax: +45 7020 5145 • secunia.com