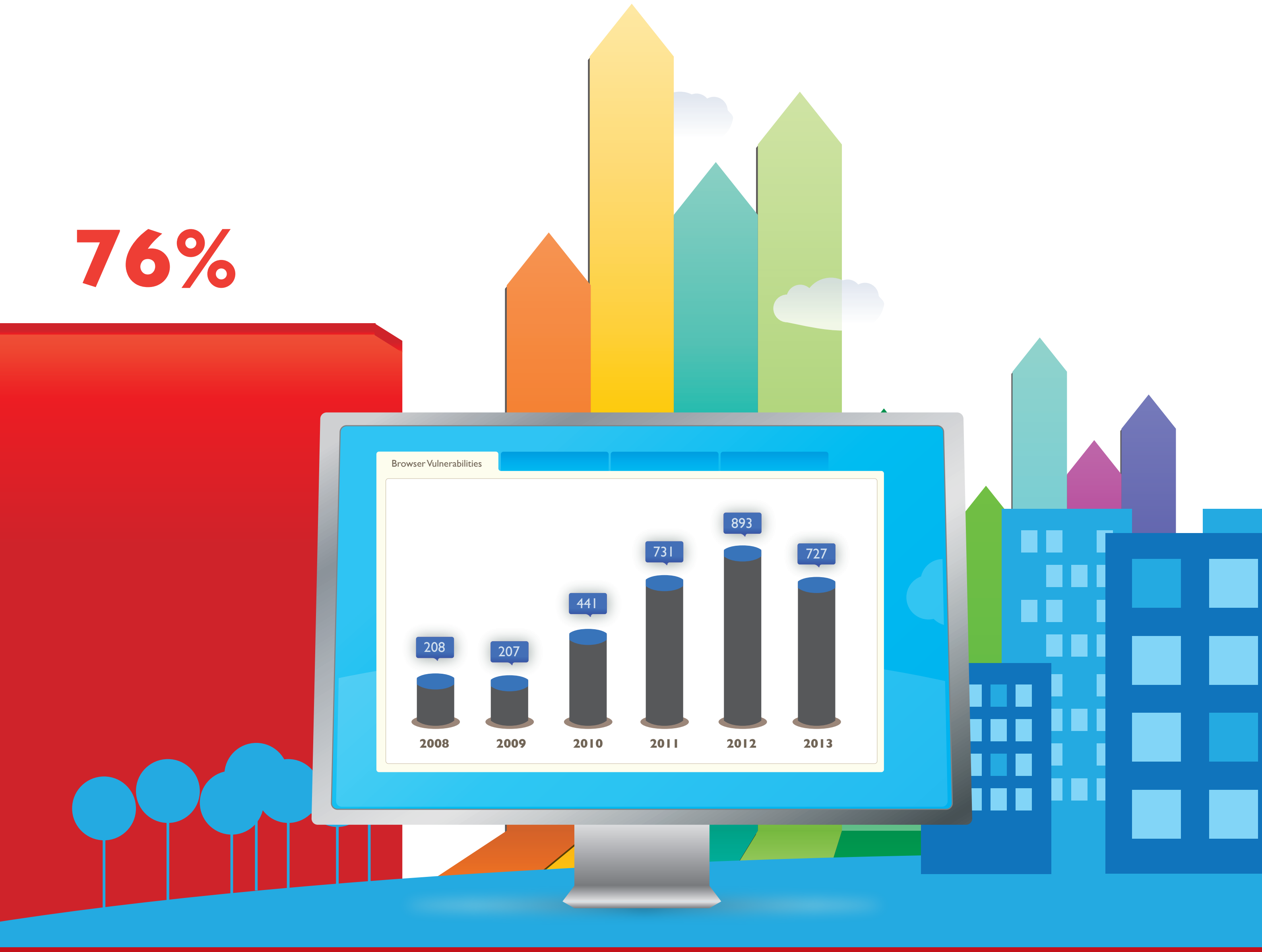
Secunia
Stay Secure

Secunia Vulnerability Review 2014

Key figures and facts from a global IT-Security perspective

Published February 26, 2014



secunia.com

Vulnerability Update

Global Trends
All products

Numbers - All products

The absolute number of vulnerabilities detected was 13,073, discovered in 2,289 products from 539 vendors. The number shows a 45% increase in vulnerabilities in the five year trend, and a 32% increase from 2012 to 2013.

Since 2012, the amount of vulnerable vendors has increased by 13% and the amount of vulnerable products has decreased by 6%. However, in comparison to the last three years, these numbers are minor fluctuations and the overall trend appears relatively stable.

Criticality – All products

16.3% of vulnerabilities in 2013 were rated as 'Highly Critical', and 0.4% as 'Extremely Critical'.

In general, there was a shift in criticality levels across the board in 2013 compared to the previous year: vulnerabilities in the higher level brackets decreased and the lower level criticalities increased.

The most notable changes occurred in the 'Moderately' and 'Less' criticality brackets, with a decrease from 29.2% in 2012 to 23.3% in 2013, and an increase from 46.6% in 2012 to 52.5% in 2013 respectively.

Attack Vector – All products

With a 73.5% share, the primary attack vector available to attackers to trigger a vulnerability in 2013 was Remote Network. Local Network saw an increase, from 15% in 2012, to 19.9% in 2013. Local System recorded an increase compared to last year, from 5%, to 6.6% in 2013.

Global Trends
Top 50 portfolio

Numbers - Top 50 portfolio

The number of vulnerabilities in the Top 50 portfolio was 1,208, discovered in 27 products from 7 vendors plus the most used operating system, Microsoft Windows 7.

The number shows a 45% increase in the 5 year trend, and a 4% increase from 2012 to 2013.

Criticality – Top 50 portfolio

68.2% of vulnerabilities in 2013 were rated as 'Highly Critical', and 7.3% as 'Extremely Critical'.

Attack Vector – Top 50 portfolio

With an 86.7% share, the foremost attack vector available to attackers to trigger a vulnerability in the Top 50 portfolio was Remote Network. This is a decrease compared to 2012.

Local Network, on the other hand saw an increase, from 2% in 2012, to 2.7% in 2013. Local System recorded an increase compared to last year, from 7%, to 10.6% in 2013.

See the Appendix and Glossary for definitions of Secunia Advisories, CVEs and Vulnerabilities.

What is the Top 50 portfolio?

To assess how exposed endpoints are, we analyze the types of products typically found on an endpoint. Throughout 2013, anonymous data has been gathered from scans of the millions of private computers which have the Secunia Personal Software Inspector (PSI) installed.

Secunia data shows that the computer of a typical PSI user has an average of 75 programs installed on it. Naturally, there are country- and region-based variations regarding which programs are installed. Therefore, for the sake of clarity, we chose to focus on a representative portfolio of the 50 most common products found on a typical computer and the most used operating system, and analyze the state of this portfolio and operating system throughout the course of 2013. These 50 programs are comprised of 33 Microsoft programs and 17 non-Microsoft (third-party) programs.

We divide the products into three categories

Product composition, PSI computer (typical private PC with the PSI and, on average, 75 programs installed on it):

Microsoft programs: Represent on average 39% of the programs on a computer with the PSI installed.

Third-party programs: Software from all other vendors – represents 61% of the programs on a computer with the PSI installed.

Operating Systems: We track vulnerabilities in Windows operating systems: Windows XP, Windows Vista, Windows 7 and Windows 8.

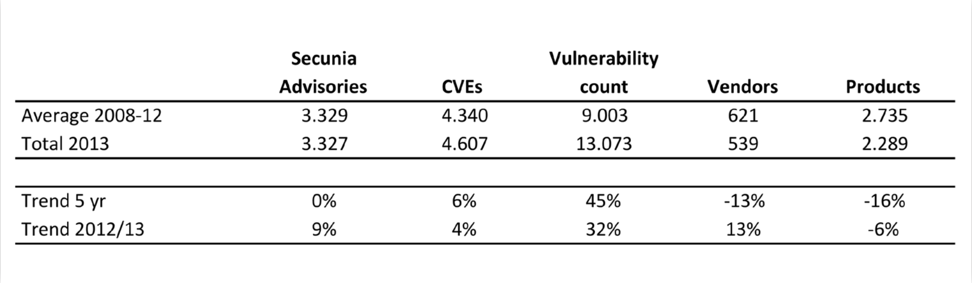
Product composition, Top 50 portfolio (the 50 most common programs found on a typical PC):

Microsoft programs: Represent on average 66% of the programs on a computer with the PSI installed.

Third-party programs: Software from all other vendors – represents 34% of the programs on a computer with the PSI installed.

Operating Systems: We track vulnerabilities in the most prevalent operating system Windows 7.

FIG 1: SECUNIA ADVISORIES/CVEs/VULNERABILITIES IN ALL PRODUCTS



	Secunia Advisories	CVEs	Vulnerability count	Vendors	Products
Average 2008-12	3.329	4.340	9.003	621	2.735
Total 2013	3.327	4.607	13.073	539	2.289
Trend 5 yr	0%	6%	45%	-13%	-16%
Trend 2012/13	9%	4%	32%	13%	-6%

Note: The 32% year-on-year increase in the total number of vulnerabilities from 2012 to 2013 is mainly due to a vulnerability increase in IBM products of 442% (from 772 vulnerabilities in 2012 to 4,181 in 2013).

FIG 3: SECUNIA ADVISORIES/CVEs/VULNERABILITIES IN ALL PRODUCTS

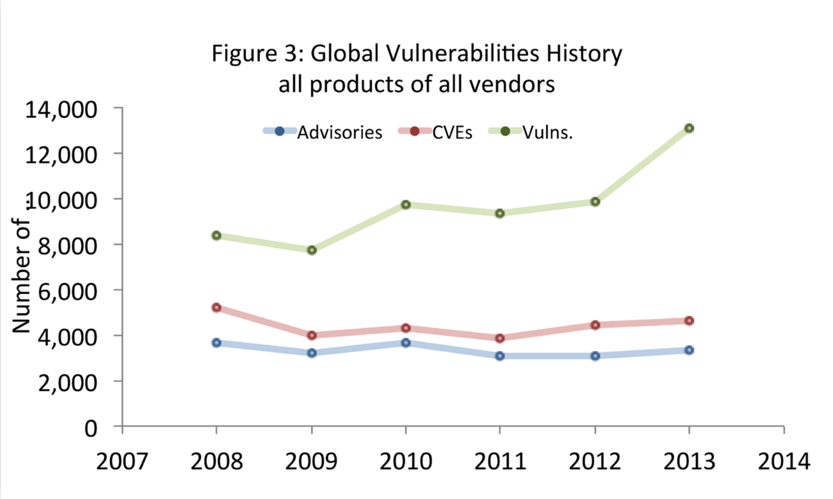


FIG 5: CRITICALITY, ALL PRODUCTS

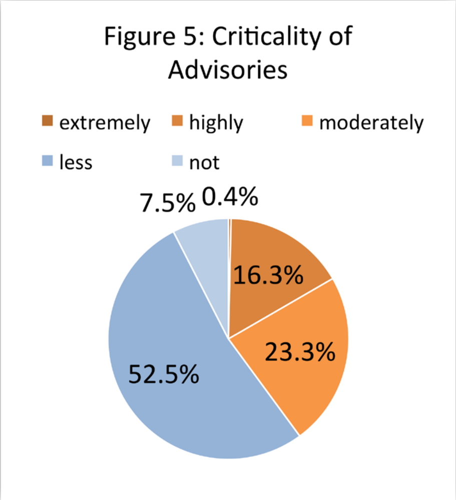


FIG 4: VULNERABLE VENDORS AND PRODUCTS, ALL PRODUCTS

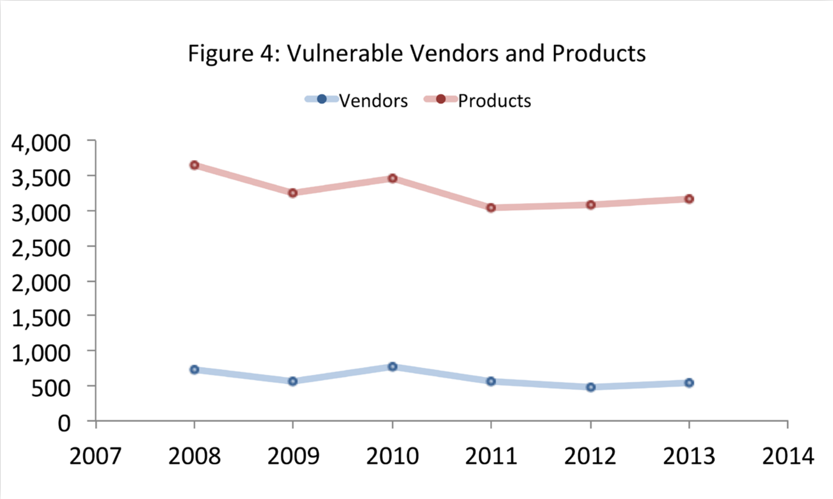


FIG 6: ATTACK VECTORS, ALL PRODUCTS

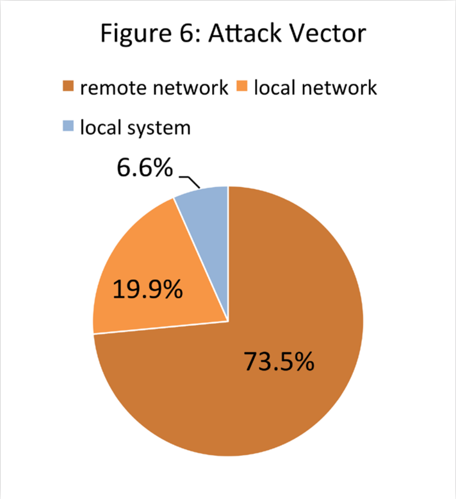
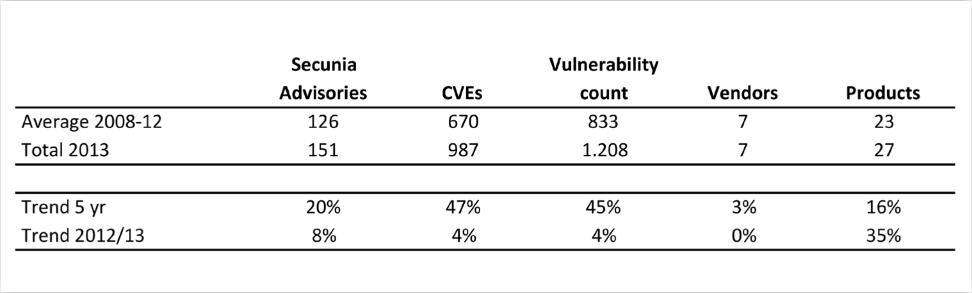


FIG 2: SECUNIA ADVISORIES/CVES/VULNERABILITIES IN TOP 50 PRODUCTS



	Secunia Advisories	CVEs	Vulnerability count	Vendors	Products
Average 2008-12	126	670	833	7	23
Total 2013	151	987	1.208	7	27
Trend 5 yr	20%	47%	45%	3%	16%
Trend 2012/13	8%	4%	4%	0%	35%

FIG 7: VULNERABLE VENDORS AND PRODUCTS, TOP 50

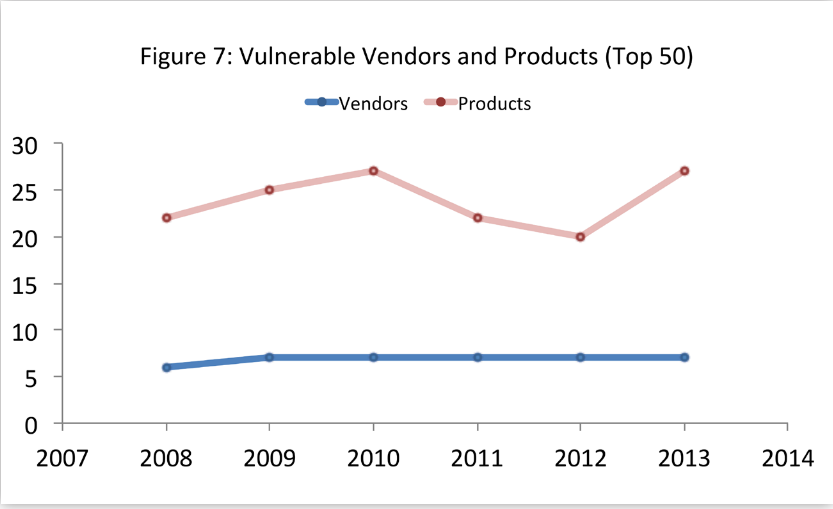


FIG 9: CRITICALITY, TOP 50

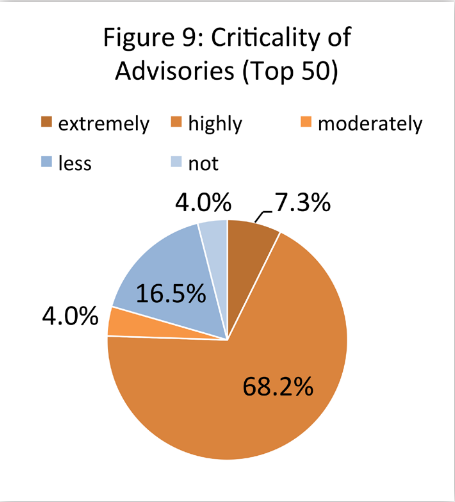


FIG 8: SECUNIA ADVISORIES/CVES/VULNERABILITIES IN TOP 50 PRODUCTS

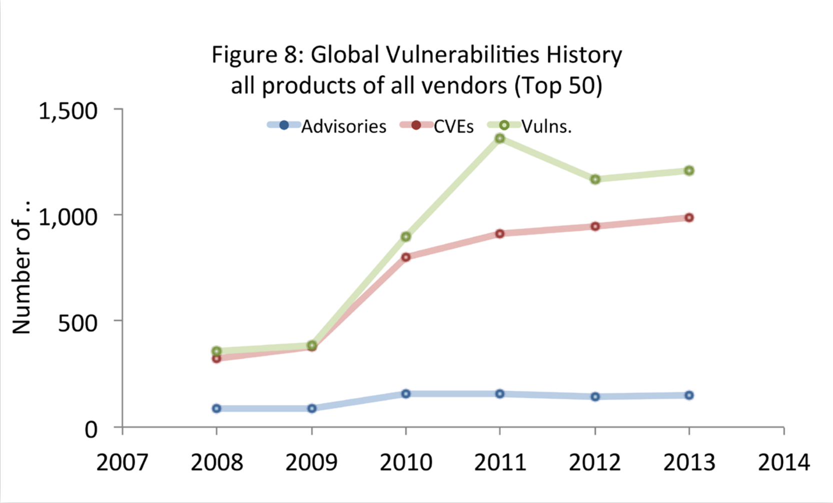
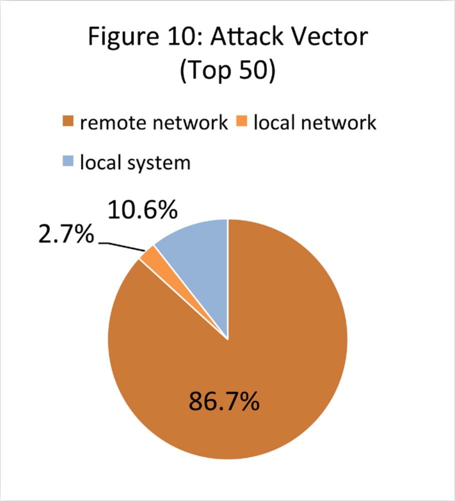


FIG 10: ATTACK VECTORS, TOP 50



Vendor Update - Top 50 Portfolio

Endpoints need to be updated with available patches issued by vendors to stay secure. A computer is at greater risk of being hacked if updates are not applied. This also serves as an increased risk to any connected system.

When assessing the state of security on individual endpoints, analyzing the patch status on those endpoints is relevant information because it helps to address any blind spots in IT security efforts.

Third-party software

In 2013, 75.7% of the vulnerabilities affecting the Top 50 programs that make up the representative software portfolio affected third-party programs. This means that 24.3% of the remaining vulnerabilities in the Top 50 programs installed on the computers of PSI users, stem from the Windows 7 operating system and Microsoft programs.

The third-party results represent a decrease compared to the previous year – 2012 – when vulnerabilities in third-party software accounted for 86%.

Nevertheless, over a five year period, the share of third-party vulnerabilities has hovered around 75%. This high-level percentage plateau is significant because it highlights the difficulties faced by end users and administrators in keeping their systems secure. For instance, if end users and organizations only focus on patching their Microsoft programs and operating systems, then they are only protecting their computers and IT infrastructures from 24.3% – a quarter – of the total risk posed by vulnerabilities.

Third-party software is issued by a vast variety of vendors. Each vendor has its own security update mechanisms and varying degrees of focus on security. This represents a major challenge to the users of personal computers and administrators of IT infrastructures, because not all vendors offer automated update services and push security updates to their users. Therefore, users and administrators have to source alternative methods – independently and per product – to ensure that their computers are properly patched, and thus protected from vulnerable software.

It is an unrealistic assumption that all end users are going to take the time to stay updated by visiting the websites of a multitude of vendors whose programs are installed on their PC – and then search, download and apply individual security updates.
Similarly, no IT administrator has the time and resources to manually keep track of the patch state of all the programs on all computers in their IT infrastructure on a continuous basis.

Operating systems

The choice of operating systems had a minor impact on the total number of vulnerabilities on a typical endpoint: In 2013, 8.4% of vulnerabilities were reported in Windows 7, the operating system we are tracking with the Top 50 portfolio.

Microsoft programs

There were significantly more vulnerabilities reported in Microsoft programs in 2013 compared to the previous year: the share went up from 8.4% to 15.9%.
The actual vulnerability count in Microsoft programs was 192 in 2013; 128.6% higher than in 2012.

The increase of vulnerabilities in Windows

Data reveals that the dip in the number of vulnerabilities recorded in Windows 7 and Windows XP in 2012 (50 and 49) has been reversed, with the number rising back up to 102 and 99 vulnerabilities respectively in 2013, almost on par with 2011 figures.

FIG 11:VULNERABILITIES IN TOP 50 PORTFOLIO, 5 YEARS

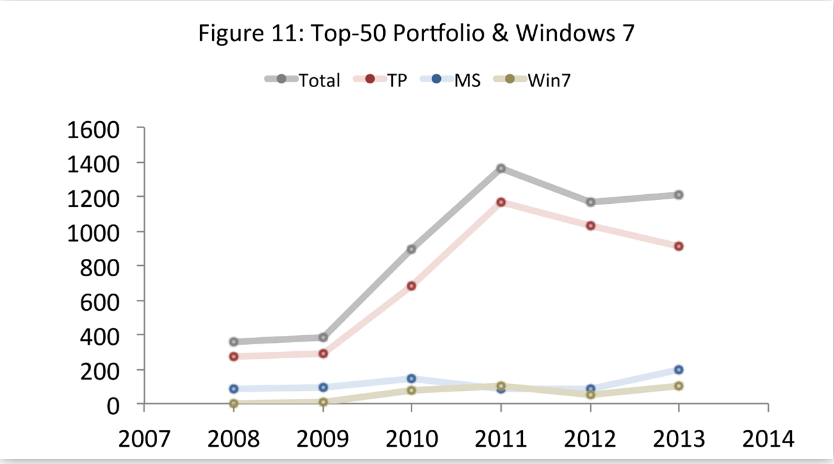
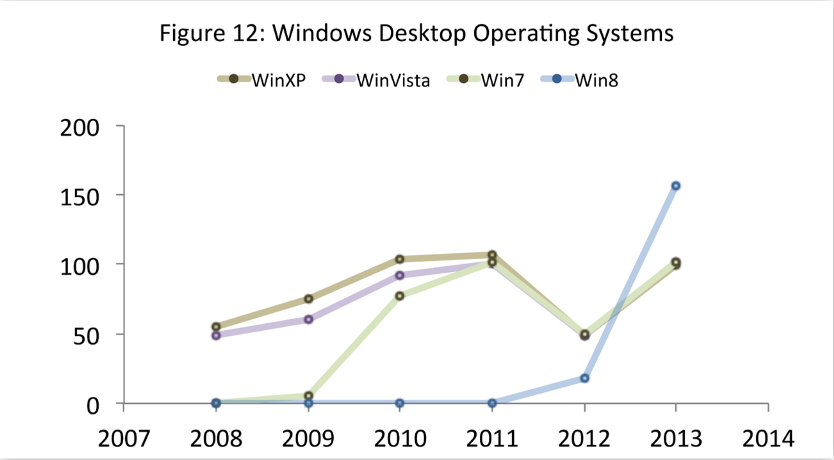
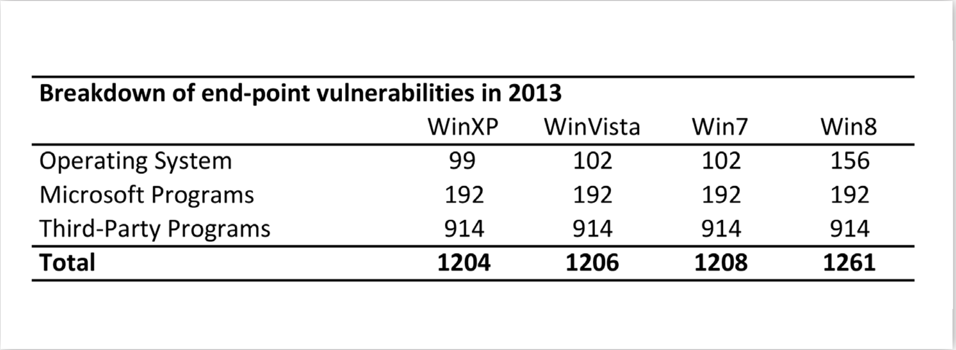


FIG 12:VULNERABILITIES IN WINDOWS OPERATING SYSTEMS, 5 YEARS



Note: The high number of vulnerabilities in Windows 8 is due to the fact that Windows 8 has Adobe Flash Player integrated into Internet Explorer. This integration is responsible for a portion of the vulnerabilities (55) detected in that operating system.

FIG 13:VULNERABILITIES IN TOP 50 IN 2013



Breakdown of end-point vulnerabilities in 2013

	WinXP	WinVista	Win7	Win8
Operating System	99	102	102	156
Microsoft Programs	192	192	192	192
Third-Party Programs	914	914	914	914
Total	**1204**	**1206**	**1208**	**1261**

FIG 14: CRITICALITY OF VULNERABILITIES IN TOP 50, 5 YEARS

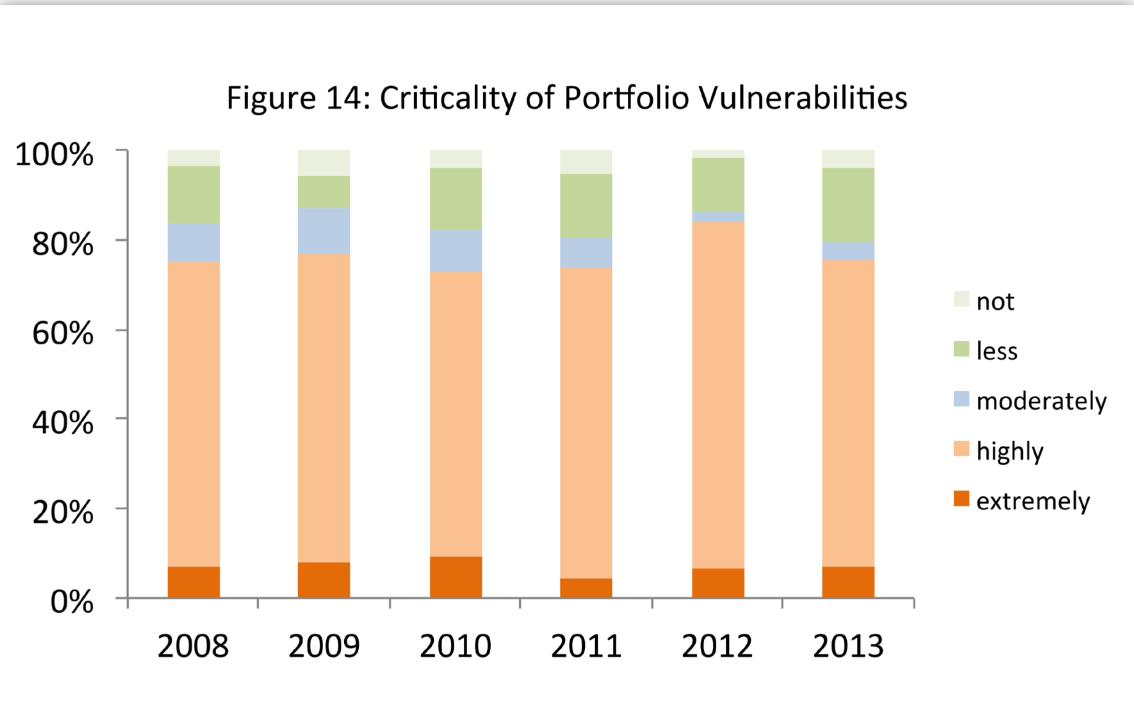


FIG 15: SHARE BY SOURCE, TOP 50

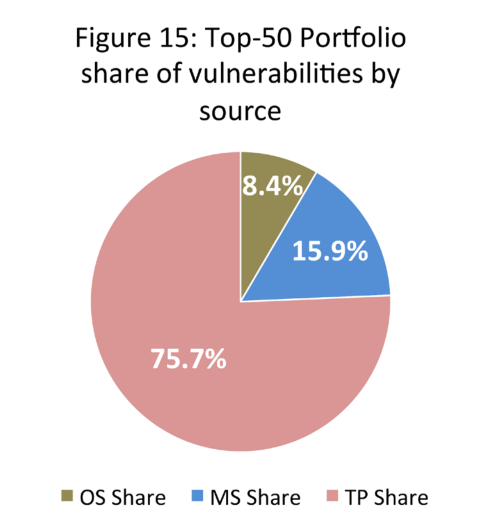
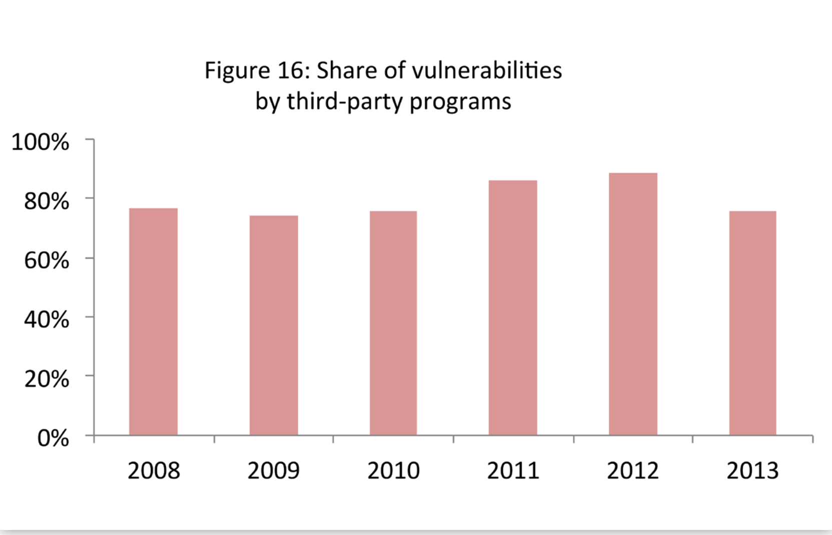


FIG 16: SHARE OF THIRD-PARTY VULNERABILITIES IN TOP 50, 5 YEARS



Time-to-Patch*

In 2013, 78.6% of all vulnerabilities had a patch available on the day of disclosure - an increase compared to the 70.1% in 2012.*

In the Top 50 programs, 86.1% of vulnerabilities had a patch available on the day of disclosure. This number represents a slight decrease compared to the 90% time-to-patch rate that was recorded in 2012. *

The number is a proportionate reflection when taking into account that some vendors choose to issue major product releases rather than minor updates, which can be more complex for users and administrators to manually manage. Overall, the 2013 result remains positioned at the higher end of the scale, indicating that it is still possible to remediate the majority of vulnerabilities.

The 2013 time-to-patch results show that 21.4% / 13.9% of vulnerabilities respectively were without patches for longer than the first day of disclosure. It is realistic to assume that this percentage is a representative proportion of software products that are not patched as quickly – e.g. due to a lack of vendor resources, uncoordinated releases or on rare occasions when there are zero-day vulnerabilities. Consequently, and particularly for organizations with a vast array of endpoints to manage (including devices not regularly connected to corporate networks), this means that patch management on its own does not ensure sufficient protection.

Increased cooperation between vendors and researchers

That 78.6% of vulnerabilities in All products, and 86.1% of vulnerabilities in products in the Top 50 portfolio have a patch available on the day of disclosure, represents a continued improvement in time-to-patch, particularly when taking a retrospective view of the last five years and the low of 61.6% recorded in 2010. The most likely explanation for the continuously good time-to-patch rate is that researchers are continuing to coordinate their vulnerability reports with vendors and vulnerability programs, resulting in immediate availability of patches for the majority of cases.

*: The Time-to-Patch numbers are not directly **compatible** with the numbers released in 2013. We have applied a different method for 2013, because an increasing number of vendors, particularly browser vendors, upgrade to new major versions, rather than patch existing versions.

The numbers used in this report for Time-to-Patch are, however, **comparable**, as they are reached using the same method. Consequently, the year-on-year comparison in this report is reliable.

FIG 17: PATCH AVAILABILITY FOR VULNERABILITIES IN ALL PRODUCTS, 5 YEARS

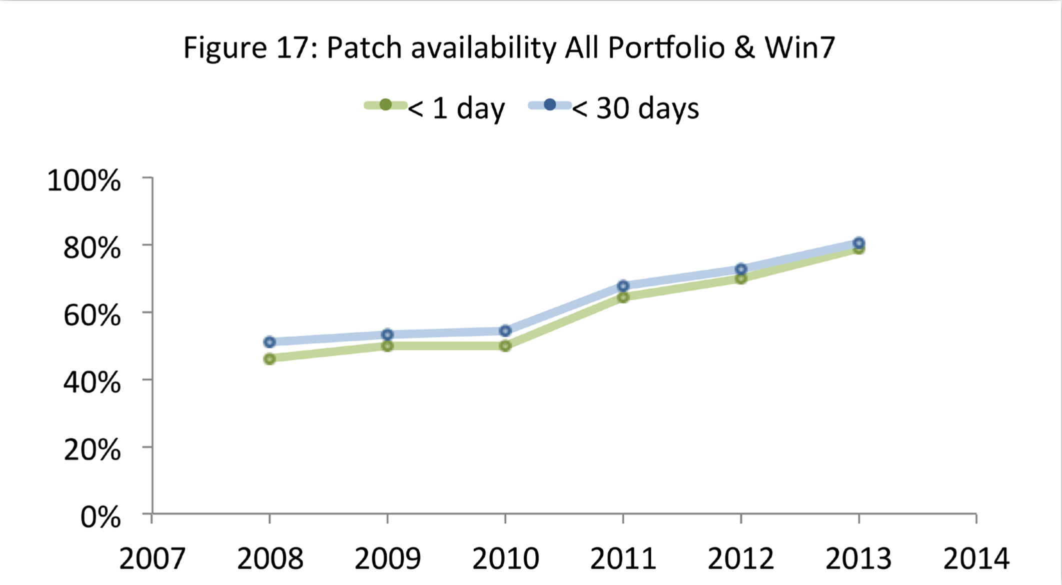
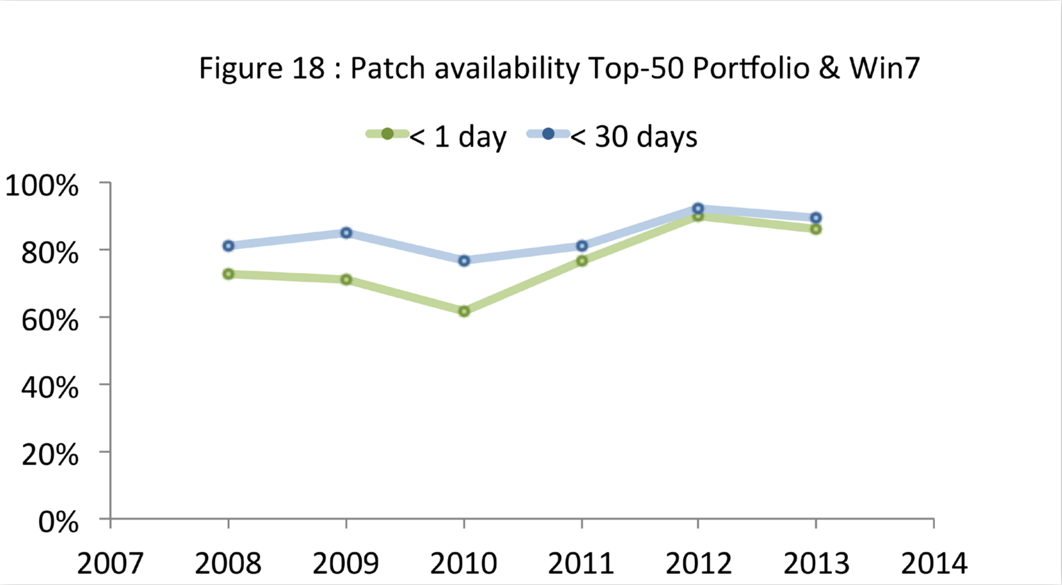


FIG 18: PATCH AVAILABILITY FOR VULNERABILITIES IN TOP 50 PRODUCTS, 5 YEARS

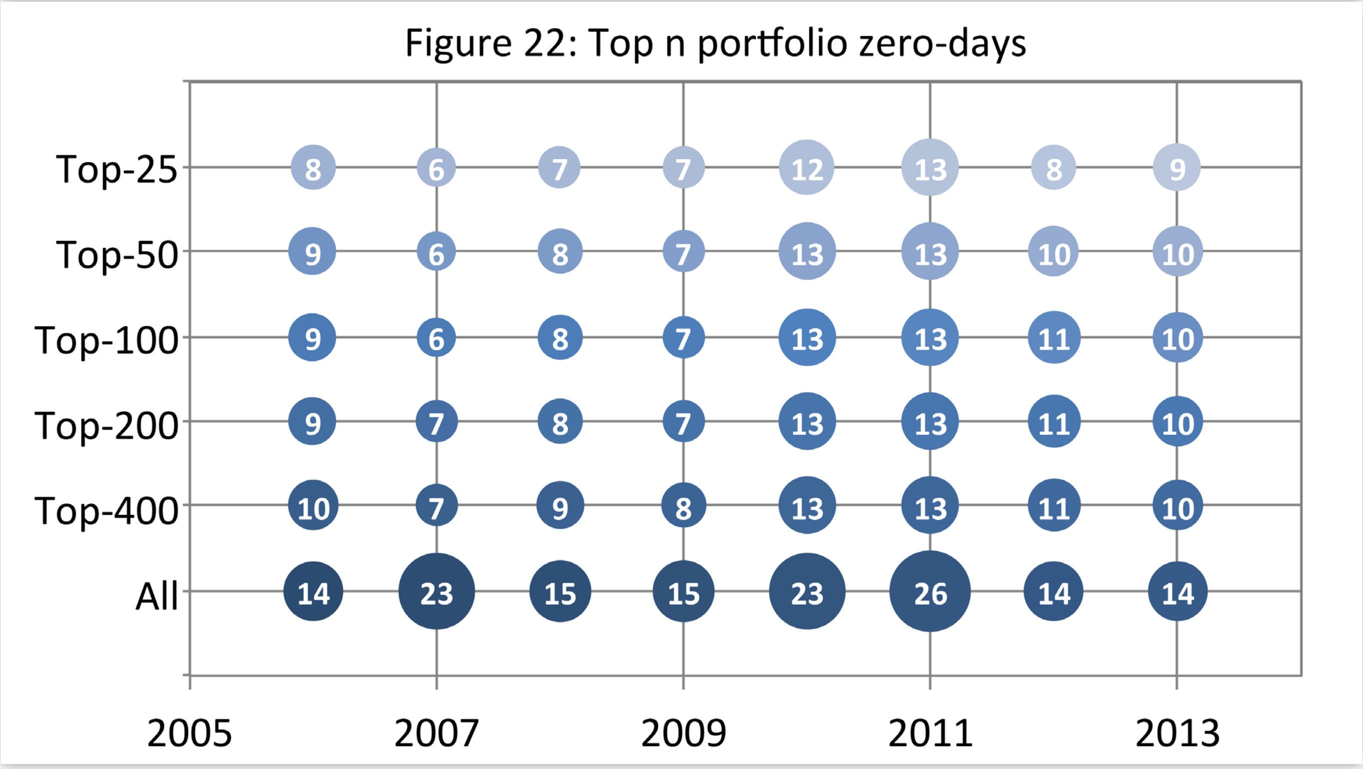


Zero-Days

As in 2012, not many zero-day vulnerabilities were identified in 2013: 10 in total in the Top 50 software portfolio, and 14 in All products.

Taking a retrospective view, 2010 and 2011 are the stand out exceptions in the five year trend with 13 and 14 (Top 50), and 23 and 26 (All products) zero-day vulnerabilities respectively.

FIG 22: ZERO-DAY VULNERABILITIES IDENTIFIED BY SECUNIA IN 2013



Browser Security

This snapshot of browser security outlines the evolvement of vulnerabilities relating to the five most popular browsers (Google Chrome, Mozilla Firefox, Internet Explorer, Opera and Safari). Overall, data shows that there were 727 vulnerabilities in these browsers in 2013 compared to 893 in 2012 – a year-on-year decrease of 18.6%. The majority of these vulnerabilities were rated as 'Highly Critical'.

The chart below illustrates the distribution of vulnerabilities across the five browsers in 2013, including their market share, patch status and exposure level.

In the chart, we have ranked the Top 5 browsers according to risk exposure. We rank them based on two parameters: "Market share" in %, multiplied by "Unpatched" in %. That is, how widespread the browser is, multiplied by how many of the private users who have installed the browser neglected to apply a patch, even though a patch was available.
The more widespread a program is, and the higher the unpatched share, the more lucrative it is for a hacker to target this program, as it will allow the hacker to compromise a lot of victims.

The calculation of the yearly average is based on Secunia PSI data.

Importantly, even though Internet Explorer has a market share of 99% percent, Firefox and Chrome are actually installed on 63% and 60% of the scanned systems with the Secunia PSI installed, respectively. Since these applications are used for the same purpose, it is fair to assume that users have multiple browsers installed but only use one of them, forgetting about the others. This practice may also directly affect the "unpatched" status of these browsers, because users are not likely to prioritize the security of a browser no longer in use.

FIG 19: VULNERABILITIES IN THE 5 MOST POPULAR BROWSERS

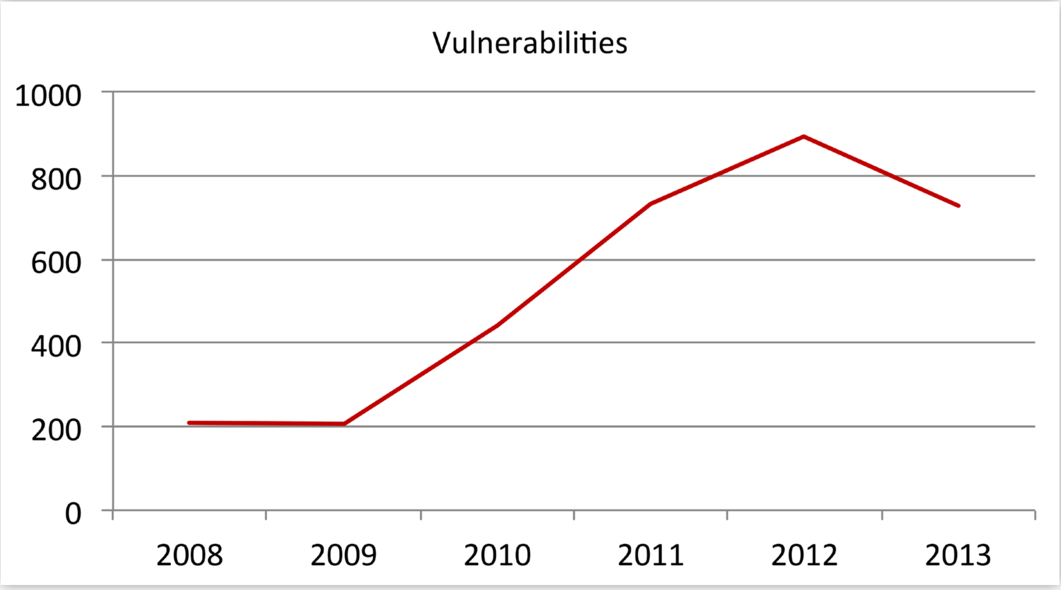


FIG 20: BROWSER EXPOSURE BY MARKET SHARE AND UNPATCHED USERS

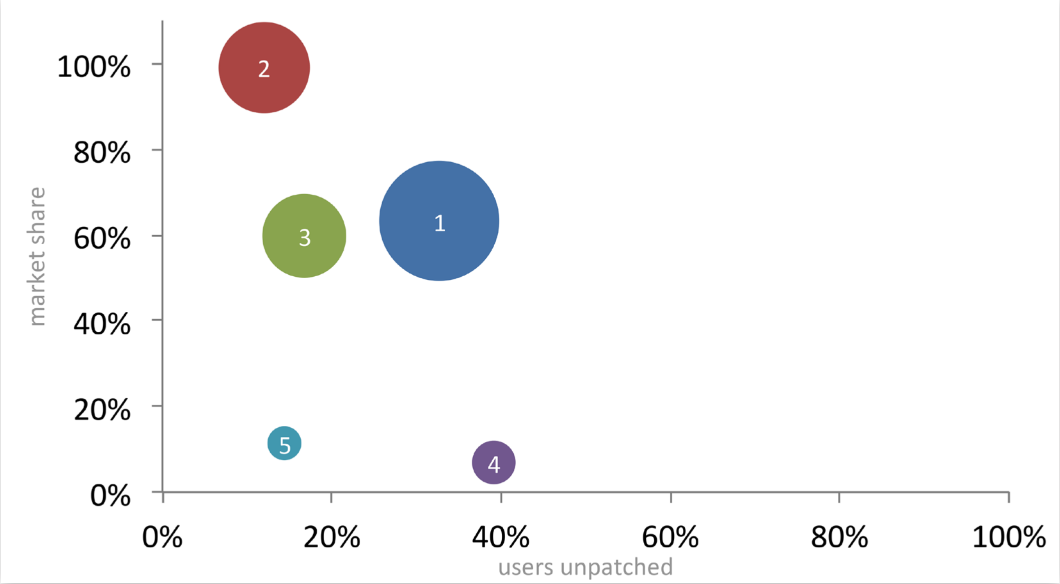
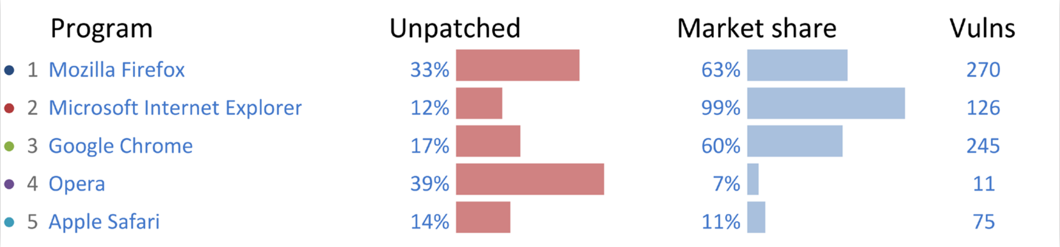


FIG 21: BROWSER MARKET SHARE/UNPATCHED SHARE/NUMBER OF VULNERABILITIES



Program	Unpatched	Market share	Vulns
● 1 Mozilla Firefox	33%	63%	270
● 2 Microsoft Internet Explorer	12%	99%	126
● 3 Google Chrome	17%	60%	245
● 4 Opera	39%	7%	11
● 5 Apple Safari	14%	11%	75

PDF Readers

This snapshot of the security status of PDF readers outlines the evolvement of vulnerabilities relating to the five most popular products (Adobe Reader, Foxit Reader, PDF-XChange Viewer, Sumatra PDF and Nitro PDF Reader). Overall, there has been a 37.3% increase in vulnerabilities in these PDF readers, with 70 vulnerabilities identified in 2013 (51 in 2012). These vulnerabilities were rated as either 'Highly Critical' or 'Extremely Critical'.

The chart below illustrates the distribution of vulnerabilities across the five PDF readers in 2013, including their market share, patch status and exposure level.

In the chart, we have ranked the Top 5 PDF readers according to risk exposure. We rank them based on two parameters: "Market share" in %, multiplied by "Unpatched" in %. That is, how widespread the PDF reader is, multiplied by how many of the private users who have installed the reader neglected to apply a patch, even though a patch was available. The more widespread a program is, and the higher the unpatched share, the more lucrative it is for a hacker to target this program, as it will allow the hacker to compromise a lot of victims.

The calculation of the yearly average is based on Secunia PSI data.

Adobe Reader has an almost monopoly-like share of the market and the largest amount of vulnerabilities: 67 in 2013 – with about a third of its users leaving it unpatched despite this fact.

FIG 23: PDF READER EXPOSURE BY MARKET SHARE AND UNPATCHED USERS

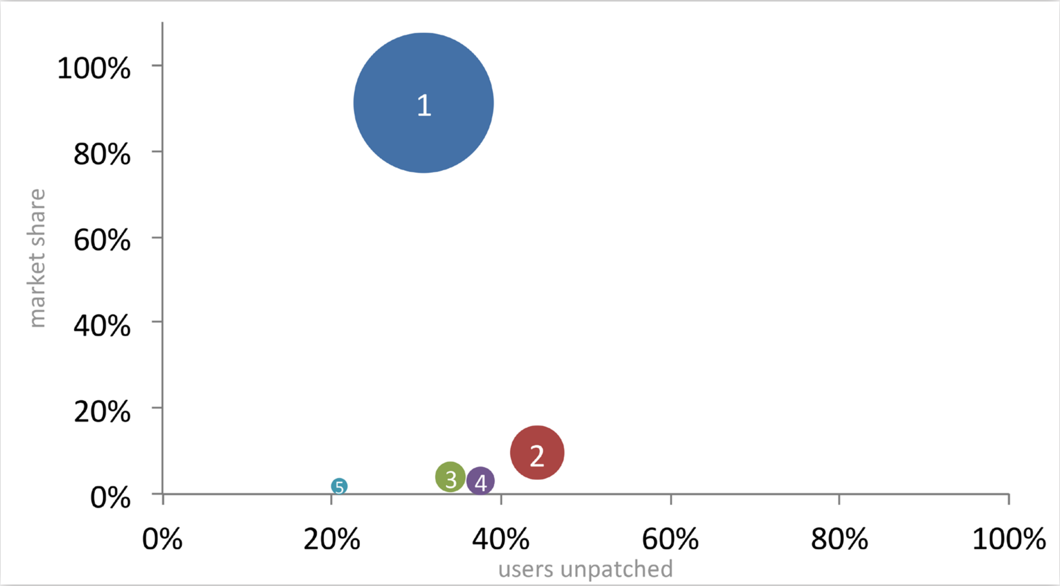
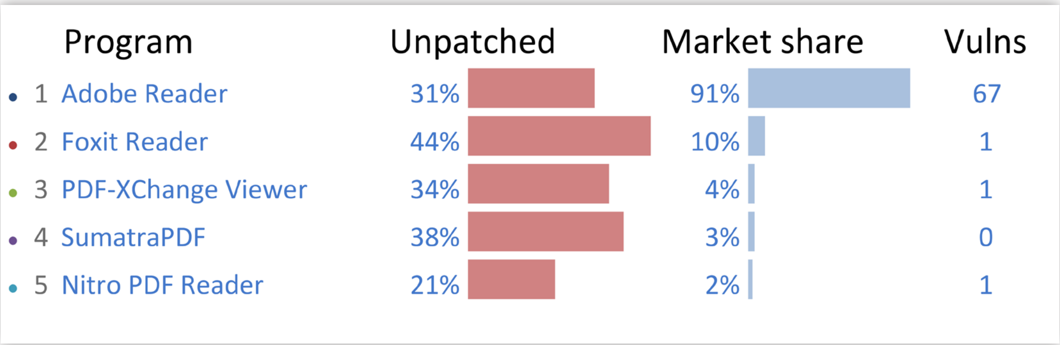


FIG 24: PDF READER MARKET SHARE/UNPATCHED SHARE/NUMBER OF VULNERABILITIES



Program	Unpatched	Market share	Vulns
● 1 Adobe Reader	31%	91%	67
● 2 Foxit Reader	44%	10%	1
● 3 PDF-XChange Viewer	34%	4%	1
● 4 SumatraPDF	38%	3%	0
● 5 Nitro PDF Reader	21%	2%	1

Appendix
& Glossary

Appendix

Secunia Vulnerability Tracking Process

A vulnerability is an error in software which can be exploited with a security impact and gain. Secunia validates, verifies, and tests vulnerability information gathered and includes it in the Secunia Vulnerability Intelligence database with consistent and standard processes, which have been constantly refined over the years.

Whenever a new vulnerability is reported, a Secunia Advisory is released after verification of the information. A Secunia Advisory provides details, including description, risk rating, impact, attack vector, recommended mitigation, credits, references, and more for the vulnerability including additional details discovered during verification and testing, thus providing the information required to make appropriate decisions about how to protect systems. After the first publication, the status of the vulnerability is tracked throughout its lifecycle and updates are made to the corresponding Secunia Advisory as new relevant information becomes available.

Metrics used to count vulnerabilities in software

Secunia Advisory
The number of Secunia Advisories published in a given period of time is a first order approximation of the number of security events in that period. Security events stand for the number of administrative actions required to keep the specific product secure throughout a given period of time.

Secunia Vulnerability Count
A vulnerability count is added to each Secunia Advisory to indicate the number of vulnerabilities covered by the Secunia Advisory. Using this count for statistical purposes is more accurate than counting CVE identifiers. Using vulnerability counts is, however, also not ideal as this is assigned per advisory. This means that one advisory may cover multiple products, but multiple advisories may also cover the same vulnerabilities in the same code-base shared across different programs and even different vendors.

Common Vulnerabilities and Exposures (CVE)
Common Vulnerabilities and Exposures (CVE) is a dictionary of publicly known information security vulnerabilities and exposures. CVE has become a de facto industry standard used to uniquely identify vulnerabilities which have achieved wide acceptance in the security industry. Using CVEs as vulnerability identifiers allows correlating information about vulnerabilities between different security products and services. CVE information is assigned in Secunia Advisories.

The intention of CVE identifiers is, however, not to provide reliable vulnerability counts, but is instead a very useful, unique identifier for identifying one or more vulnerabilities and correlating them between different sources. The problem in using CVE identifiers for counting vulnerabilities is that CVE abstraction rules may merge vulnerabilities of the same type in the same product versions into a single CVE, resulting in one CVE sometimes covering multiple vulnerabilities. This may result in lower vulnerability counts than expected when basing statistics on the CVE identifiers.

Attack Vector

The attack vector describes the way an attacker can trigger or reach the vulnerability in a product. Secunia classifies the attack vector as "Local system", "From local network", or "From remote".

Local System
Local system describes vulnerabilities where the attacker is required to be a local user on the system to trigger the vulnerability.

From Local Network
From local network describes vulnerabilities where the attacker is required to be situated on the same network as a vulnerable system (not necessarily a LAN). This category covers vulnerabilities in certain services (e.g. DHCP, RPC, administrative services) that should not be accessible from the Internet, but only from a local network or optionally from a restricted set of external systems.

From Remote
From remote describes other vulnerabilities where the attacker is not required to have access to the system or a local network in order to exploit the vulnerability. This category covers services that are acceptable to be exposed and reachable to the Internet (e.g. HTTP, HTTPS, SMTP). It also covers client applications used on the Internet and certain vulnerabilities where it is reasonable to assume that a security conscious user can be tricked into performing certain actions.

Secunia Vulnerability Criticality Classification

The criticality of a vulnerability is based on the assessment of the vulnerability's potential impact on a system, the attack vector, mitigating factors, and if an exploit exists for the vulnerability and is being actively exploited prior to the release of a patch.

Extremely Critical (5 of 5)
Typically used for remotely exploitable vulnerabilities that can lead to system compromise. Successful exploitation does not normally require any interaction and exploits are in the wild. These vulnerabilities can exist in services like FTP, HTTP, and SMTP or in certain client systems like email programs or browsers.

Highly Critical (4 of 5)
Typically used for remotely exploitable vulnerabilities that can lead to system compromise. Successful exploitation 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 (3 of 5)
This rating is also used for vulnerabilities allowing system compromise on LANs in services like SMB, RPC, NFS, LPD and similar services that are not intended for use over the Internet. Typically used for remotely exploitable Denial of Service vulnerabilities against services like FTP, HTTP, and SMTP, and for vulnerabilities that allow system compromises but require user interaction.

Less Critical (2 of 5)
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 (1 of 5)
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).

The Top-50 Software Portfolio

The following table lists the programs in the Top-50 software portfolio together with the type of program (MS Microsoft, TP third-party), market share in 2013 and the number of vulnerabilities affecting the program in 2012 and 2013.

The ranking and market share is derived from anonymous scans of the Secunia PSI in 2013. Note that the sum of the vulnerabilities in this table does not reflect the total number of vulnerabilities in the portfolio as many products share vulnerabilities.

For example Adobe Flash Player (#5) and Adobe AIR (#24) share code components and thereby also share numerous vulnerabilities. For each program the unique number of Secunia Advisories, CVEs and vulnerabilities of this given program in the given year is also listed.

See the Appendix and Glossary for definitions of Secunia Advisories, CVEs and Vulnerabilities.

RANK	TYPE	PROD	SHARE	ADVS	CVES	VULNS
1	MS	MICROSOFT XML CORE SERVICES (MSXML)	99.9%	1	2	2
2	MS	MICROSOFT WINDOWS MEDIA PLAYER	99.4%	1	1	1
3	MS	MICROSOFT INTERNET EXPLORER	99.1%	14	123	126
4	MS	MICROSOFT .NET FRAMEWORK	99.1%	6	18	18
5	TP	ADOBE FLASH PLAYER	97.5%	12	56	56
6	MS	MICROSOFT VISUAL C++ REDISTRIBUTABLE	95.4%	0	0	0
7	TP	ADOBE READER	85.6%	5	67	67
8	MS	MICROSOFT SILVERLIGHT	84.3%	3	9	9
9	MS	MICROSOFT POWERSHELL	82.1%	0	0	0
10	TP	ORACLE JAVA JRE	82.1%	7	181	181
11	MS	MICROSOFT WINDOWS DEFENDER	77.1%	1	1	1
12	MS	MICROSOFT WORD	74.9%	4	17	17
13	MS	MICROSOFT EXCEL	73.8%	3	6	6
14	MS	MICROSOFT POWERPOINT	71.7%	1	1	1
15	MS	WINDOWS DVD MAKER	70.8%	0	0	0
16	TP	MOZILLA FIREFOX	63.8%	20	140	270
17	TP	GOOGLE CHROME	61.0%	20	209	245
18	MS	WINDOWS MEDIA CENTER	59.8%	0	0	0
19	MS	MICROSOFT VISIO VIEWER	56.5%	1	1	1
20	MS	DRIVER PACKAGE INSTALLER (DPINST)	56.2%	0	0	0
21	MS	MICROSOFT OUTLOOK	55.9%	2	2	2
22	MS	COMDLG32 ACTIVEX CONTROL	54.0%	0	0	0
23	TP	REALTEK AC 97 UPDATE AND REMOVE DRIVER TOOL	51.9%	0	0	0
24	TP	ADOBE AIR	51.8%	10	51	51
25	TP	APPLE QUICKTIME	51.1%	1	12	12
26	MS	MSCOMCT2 ACTIVEX CONTROL	51.0%	0	0	0
27	MS	MICROSOFT XPS-VIEWER	50.8%	0	0	0
28	MS	MICROSOFT SQL SERVER	50.6%	0	0	0
29	TP	CCLEANER	47.9%	0	0	0
30	MS	MICROSOFT ACCESS	47.3%	1	3	3
31	MS	WINDOWS LIVE MAIL	46.9%	0	0	0
32	MS	MICROSOFT PUBLISHER	45.9%	1	11	11

33	MS	MICROSOFT POWERPOINT VIEWER	45.1%	1	1	1
34	MS	MICROSOFT WINDOWS MALICIOUS SOFTWARE REMOVAL TOOL	45.0%	1	1	1
35	MS	SKYPE	44.9%	1	0	3
36	MS	WINDOWS LIVE MESSENGER	44.7%	0	0	0
37	TP	APPLE BONJOUR FOR WINDOWS	44.6%	0	0	0
38	MS	WINDOWS LIVE WRITER	44.5%	0	0	0
39	TP	REALTEK VOICE MANAGER	44.4%	0	0	0
40	MS	WINDOWS LIVE MOVIE MAKER	43.1%	0	0	0
41	TP	APPLE ITUNES	43.1%	3	66	66
42	TP	VLC MEDIA PLAYER	39.7%	4	5	7
43	TP	GOOGLE EARTH	38.2%	0	0	0
44	MS	WINDOWS LIVE ESSENTIALS	38.1%	0	0	0
45	MS	WINDOWS LIVE PHOTO GALLERY	37.9%	0	0	0
46	TP	INSTALLSHIELD UPDATE SERVICE	35.7%	0	0	0
47	MS	MICROSOFT OFFICE PICTURE MANAGER	34.6%	0	0	0
48	MS	MICROSOFT OFFICE TEMPLATE AND MEDIA CONTROL ACTIVEX CONTROL	33.6%	0	0	0
49	TP	GOOGLE TOOLBAR	33.0%	0	0	0
50	TP	ADOBE SHOCKWAVE PLAYER	29.3%	5	11	10
OS	MS	MICROSOFT WINDOWS 7	N/A	37	100	102

Glossary

Vulnerability

A vulnerability is an error in software which can be exploited with a security impact and gain.

Exploit

Malicious code that takes advantage of software vulnerabilities to infect a computer or perform other harmful actions.

Zero-day vulnerability

A zero-day vulnerability is a vulnerability that is actively exploited by hackers before it is publicly known, and before the vendor has published a patch for it.

Secunia
Stay Secure

For further information,
please visit

Secunia
Mikado House
Rued Langgaards Vej 8
DK-2300 Copenhagen S
Denmark
secunia.com
Email: info@secunia.com
Phone: +45 7020 5144
Fax: +45 7020 5145