Secunia
Stay Secure

Secunia Vulnerability Review

2013

Key figures and facts from a global IT-Security perspective

Published March 14th, 2013

Vulnerability Update

Global Trends - All products

Numbers - All products
The absolute number of vulnerabilities detected was 9,776, discovered in 2,503 products from 421 vendors. The number shows a 15% increase in the five year trend, and a 5% increase from 2011 to 2012.

The number of vendors and products in which vulnerabilities are discovered continues to decrease. Vendors are buying each other up, and products are being merged and incorporated into fewer offerings. The amount of code developed to deliver the functionalities of the offerings, however, is the same – and that is where the vulnerabilities reside.

Criticality – all products
One fifth of the criticalities discovered in all products were rated as either 'Highly critical' (18.3%) or 'Extremely critical' (0.5%).

Attack Vector – all products
With a 80% share, the primary attack vector for all products, was Remote Network.

Global Trends - Top 50 portfolio

Numbers - Top 50 portfolio
The number of endpoint vulnerabilities in Top 50 portfolio was 1.137 discovered in 18 products from 8 vendors.
The number shows a 98% increase in the 5 year trend, and a 10% decrease from 2011 to 2012.

Criticality – Top 50 portfolio
Most of these were rated by Secunia as either 'Highly critical' (78.8%) or 'Extremely critical' (5.3%).

Attack Vector – Top 50 portfolio
With a 91% share, the primary attack vector in the Top 50 portfolio, was Remote Network.

What is the Top 50 portfolio?
To asses how exposed endpoints are, we analyze the types of products typically found on an endpoint. For this analysis we use anonymous data gathered from scans throughout 2012 of the millions of private computers which have the Secunia Personal Software Inspector (PSI) installed.

PSI users' computers have an average of 72 programs installed on it – from country to country and region to region there are variations as to which programs are installed. For the sake of clarity, we have chosen to focus on the state of representative portfolio of the 50 most common products found on the computers. These 50 programs are comprised of 29 Microsoft programs and 21 third-party programs.

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

FIGURE 1: ALL PRODUCTS

	Secunia Advisories	CVEs	Vulnerability count	Vendors	Products
Average 2007-11	3,371	4,340	8,531	550	2,806
Total 2012	3,051	4,293	9,776	421	2,503
Trend 5 yr	-9%	-1%	15%	-23%	-11%
Trend 2011/12	-2%	12%	5%	-12%	-1%

FIGURE 3: ALL PRODUCTS

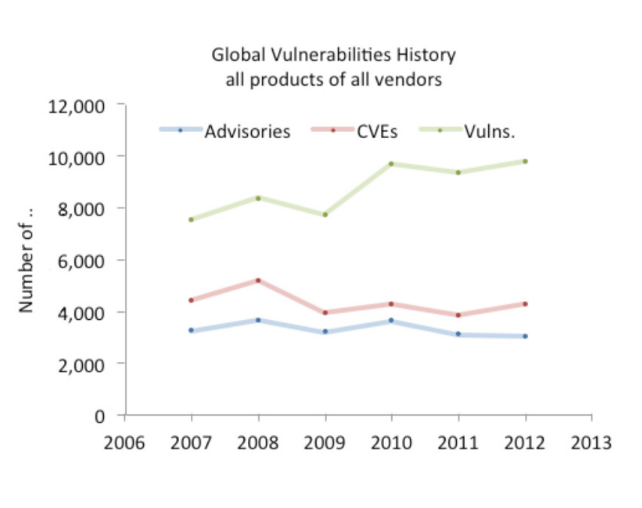


FIGURE 4: ALL PRODUCTS

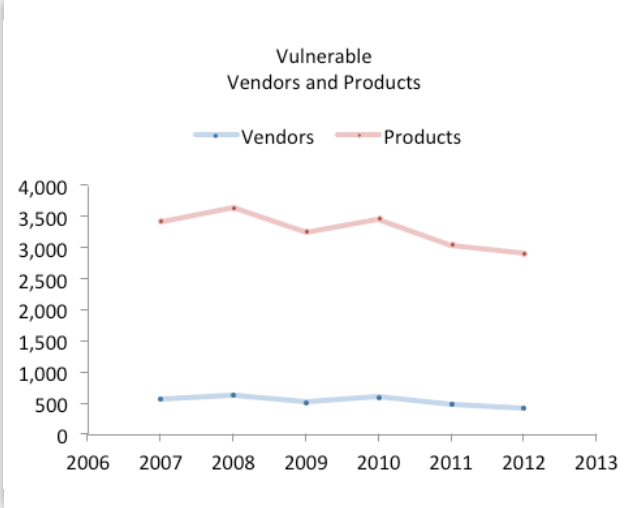


FIGURE 5: ALL PRODUCTS

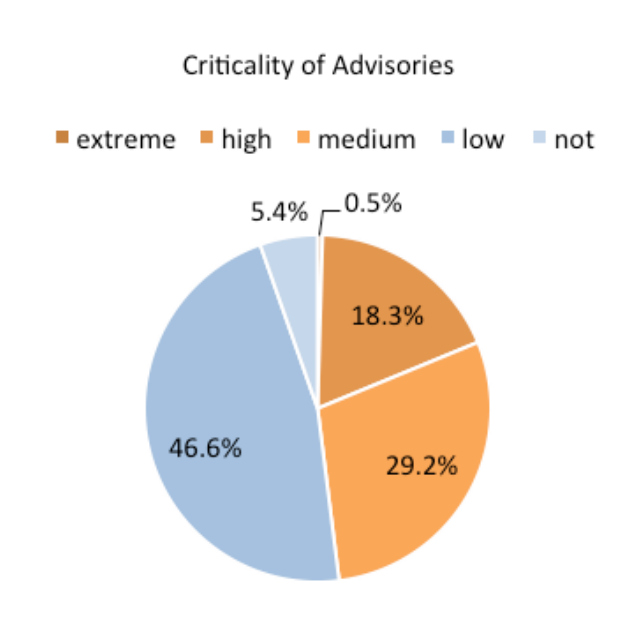


FIGURE 6: ALL PRODUCTS

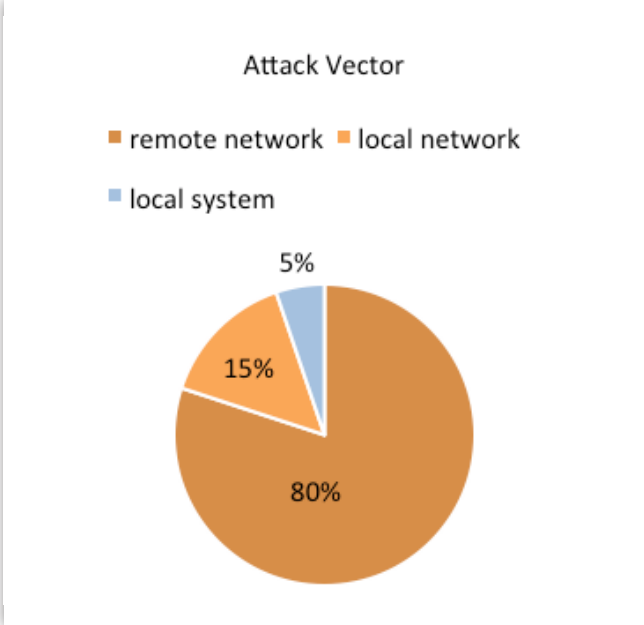


FIGURE 2:TOP 50

	Secunia Advisories	CVEs	Vulnerability count	Vendors	Products
Average 2007-11	107	452	573	7	22
Total 2012	132	916	1,137	8	18
Trend 5 yr	24%	103%	98%	18%	-17%
Trend 2011/12	-13%	10%	-9%	0%	-10%

FIGURE 7:TOP 50

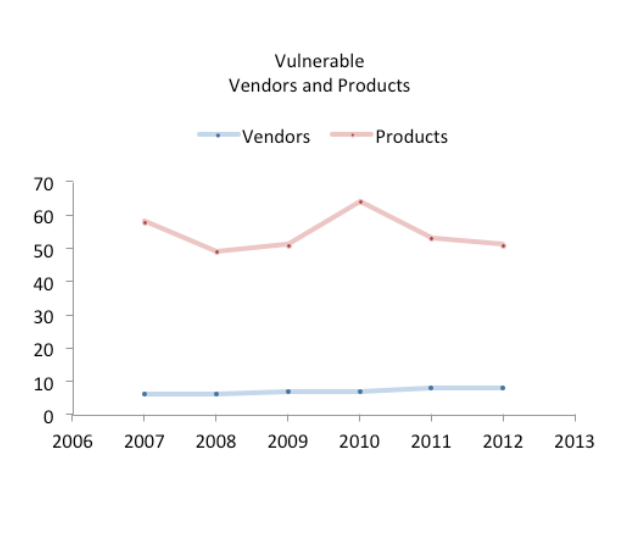


FIGURE 8:TOP 50

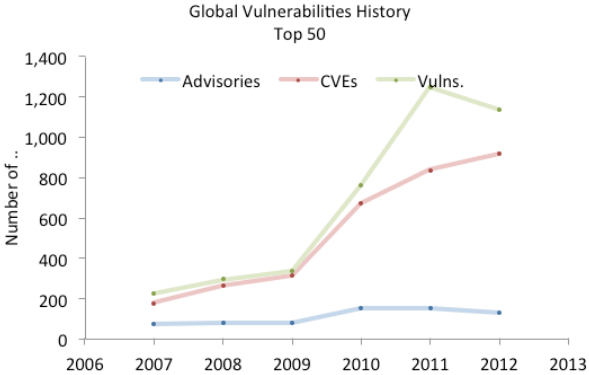


FIGURE 9:TOP 50

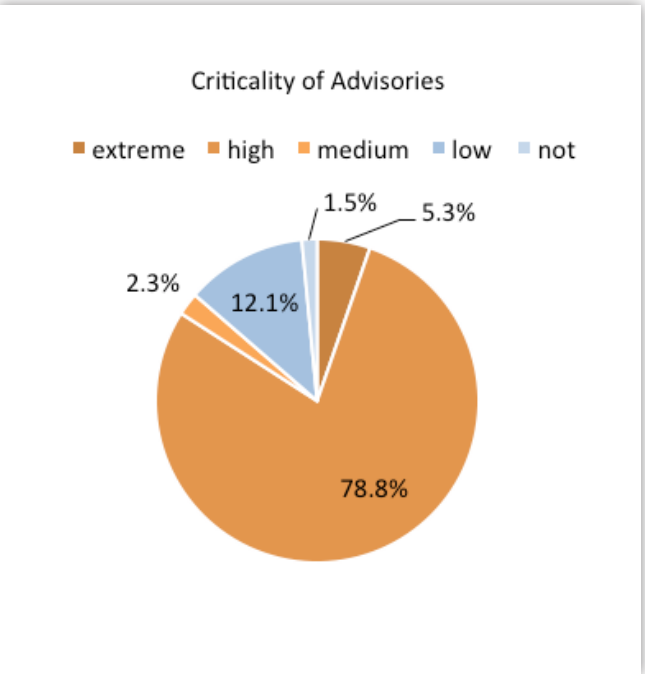
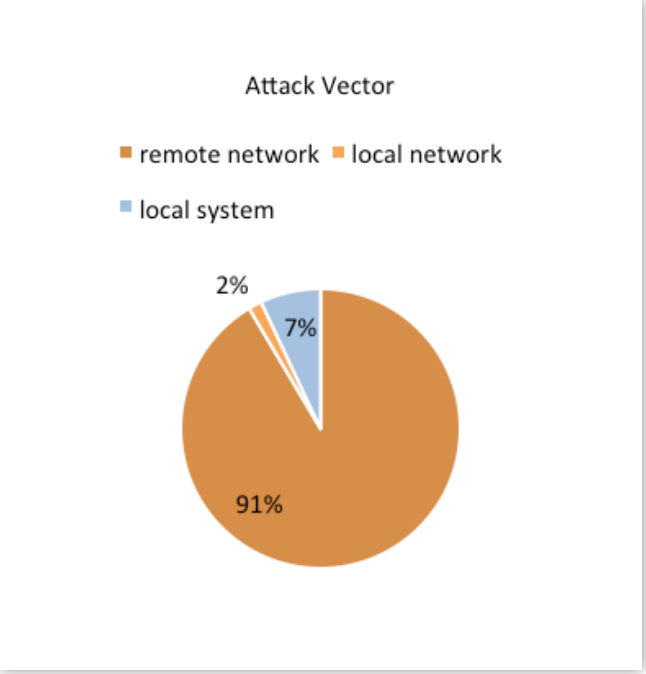


FIGURE 10:TOP 50



Vendor Update - Top 50

Endpoints need to be updated with available patches issued by the vendor to stay secure. If updates are not performed, the computer and the systems it is connected to are at risk of being hacked. Analyzing the patch status on endpoints is relevant information, when we want to assess the state of security on individual endpoints – both for the sake of the private users whose personal security is being compromised and for the sake of organisations, who need to address any blind spots in their IT security efforts.

To asses how exposed endpoints are, we analyze the types of products typically found on an endpoint. For this analysis we use anonymous data gathered from scans throughout 2012 of the millions of private computers which have the Secunia Personal Software Inspector (PSI) installed.

PSI users' computers have an average of 72 programs installed on them – from country to country and region to region there are variations as to which programs are installed. For the sake of clarity, we have chosen to focus on the state of a representative portfolio of the 50 most common products found on the computers. These 50 programs are comprised of 29 Microsoft programs and 21 third-party programs.

We divide the products into three categories:

- Microsoft programs. Represent on average 35% of the programs on a computer with PSI installed.
- Third-party programs. Software from all other vendors – represents 65% of the programs on a computer with PSI installed.
- Operating Systems. We track vulnerabilities in the most prevalent operating systems: Windows XP, Windows Vista, and Windows 7.

Third-party software

In 2012, 86% of the vulnerabilities affecting the Top-50 programs in the representative portfolio, affected third-party programs. This means that only 14% of vulnerabilities present in the Top-50 programs on the computers of the PSI users stem from Operating Systems and Microsoft programs. The 86% is a substantial increase from the previous year – 2011 - when vulnerabilities in third-party software represented 78%.

Over a five year period, the share of third-party vulnerabilities has increased from 57% in 2007 to 86% in 2012. The significance of this number is that it has become more difficult for end users and administrators to keep their systems secure: If end users and organizations focus on patching their Microsoft programs and operating systems they only protect their computer and IT infrastructure from 14% of the threats posed by vulnerabilities.

The fact that third-party software is issued by a multitude of vendors, with each their own security update mechanisms and varying degrees of focus on security, means that the users of personal computers and administrators of IT infrastructures have to stay updated about the security status of the different products on their computers.

Not all vendors offer automated update services and push security updates to their users, who have to find alternative methods to ensure that their computers are properly patched to protect them from vulnerable software.

Effectively, it is unrealistic to assume that an end user is going to take the time to stay updated on the websites of all vendors whose programs are installed on their PC.

Similarly, no IT administrator is going to be able to manually keep constant track of the patch state of all the programs on all computers in their system.

Operating systems

The choice of operating systems has only minor impact on the total number of vulnerabilities on a typical endpoint: Only 5.5% of vulnerabilities on a typical endpoint are reported in Windows operating systems.

Microsoft programs

Fewer vulnerabilities were reported in Microsoft programs in 2012. The CVE count in Microsoft programs was 8.3% lower in 2012 than in 2011, indicating less vulnerabilities in Microsoft programs.

The rise and fall of vulnerabilities in Windows

When you look at figure 12 it appears that Windows 7 saw a dramatic increase in vulnerabilities in 2010 – 2011, reaching 102 vulnerabilities. In 2012, it is back down to 51, the same number as in 2009.

The reason behind this increase in the number of vulnerabilities reported in Windows is a result of the work of one security researcher, who decided to dig into one specific component, win32k.sys. By doing so, he discovered 22 vulnerabilities in 2010 and 59 vulnerabilities in 2011 in the program, where in the year before – 2009 – only 4 had been discovered.

This shift in focus is a common condition in the security industry – sometimes individual programs come under scrutiny, sometimes entire product types.

FIGURE 11: CVEs IN TOP 50

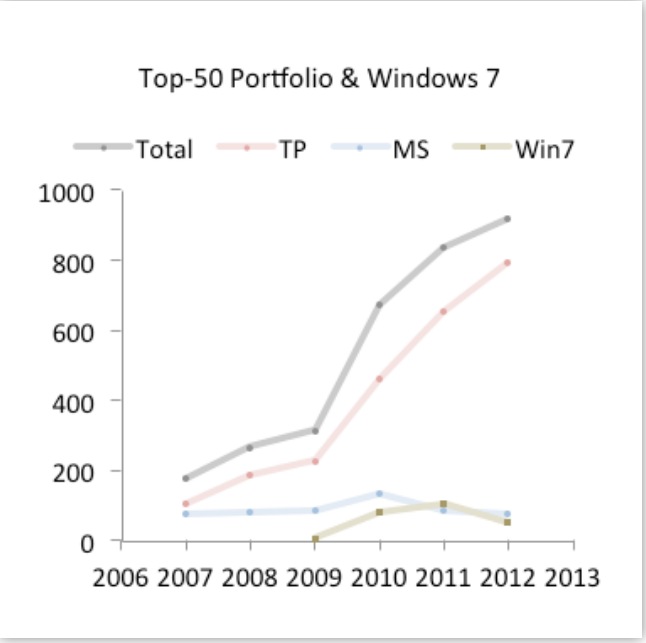


FIGURE 12: CVEs IN TOP 50

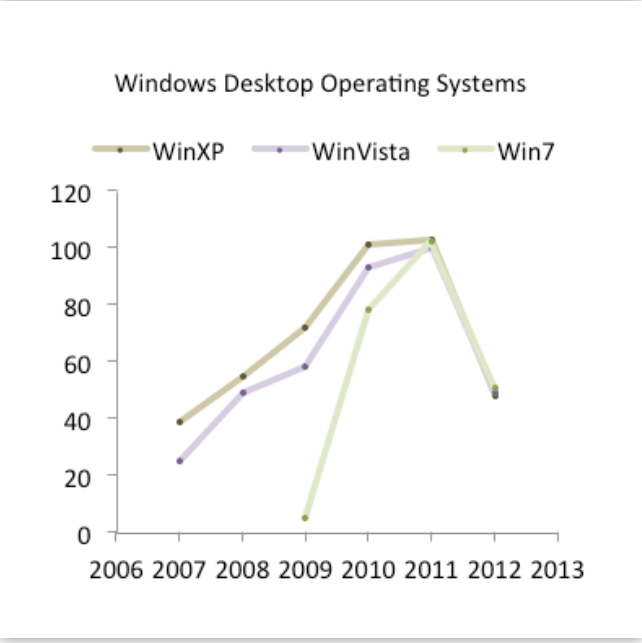


FIGURE 13: CVEs IN TOP 50

Breakdown of end-point vulnerabilities in 2012

	WinXP	WinVista	Win7
Operating System	48	49	51
Microsoft Programs	77	77	77
Third-Party Programs	792	792	792
Total	**917**	**918**	**920**

FIGURE 14:TOP 50

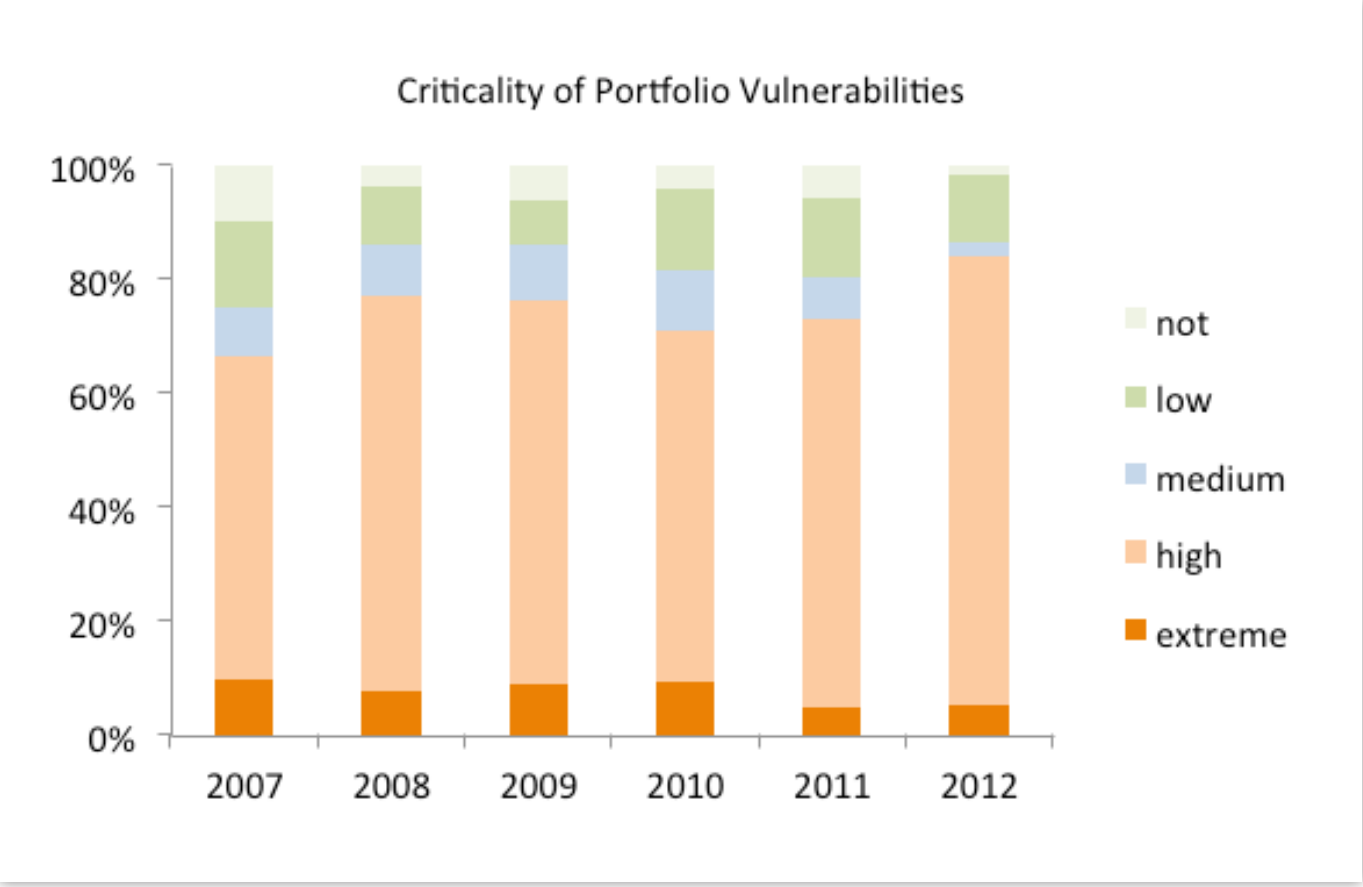


FIGURE 15:TOP 50

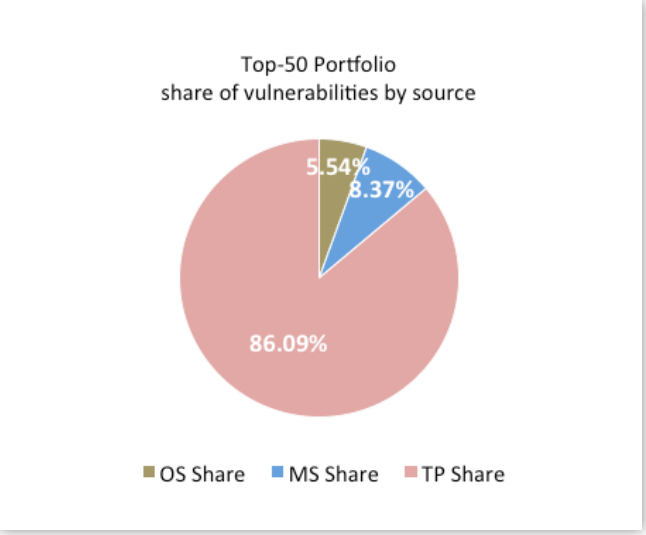
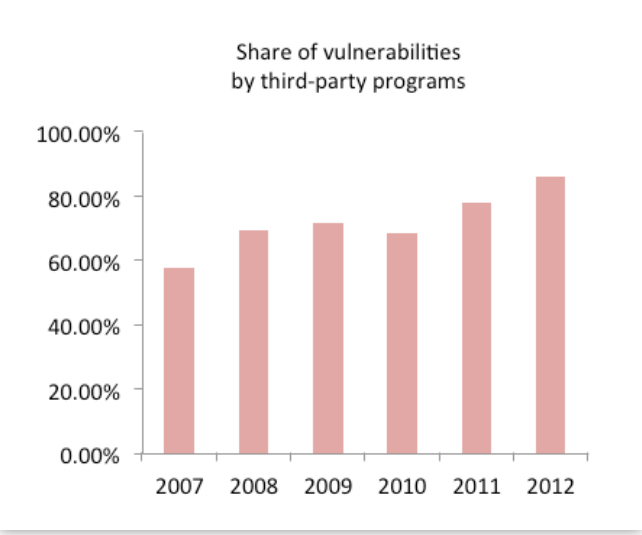


FIGURE 16:TOP 50



Time-to-Patch

Time-to-patch has decreased

The good news is that Time-to-Patch has decreased. In 2012, 80% of vulnerabilities had a patch available on the day they were disclosed. This means that it is possible to remediate the majority of vulnerabilities, and that organizations and private users alike have a solution available for the root cause of security issues: vulnerabilities in software.

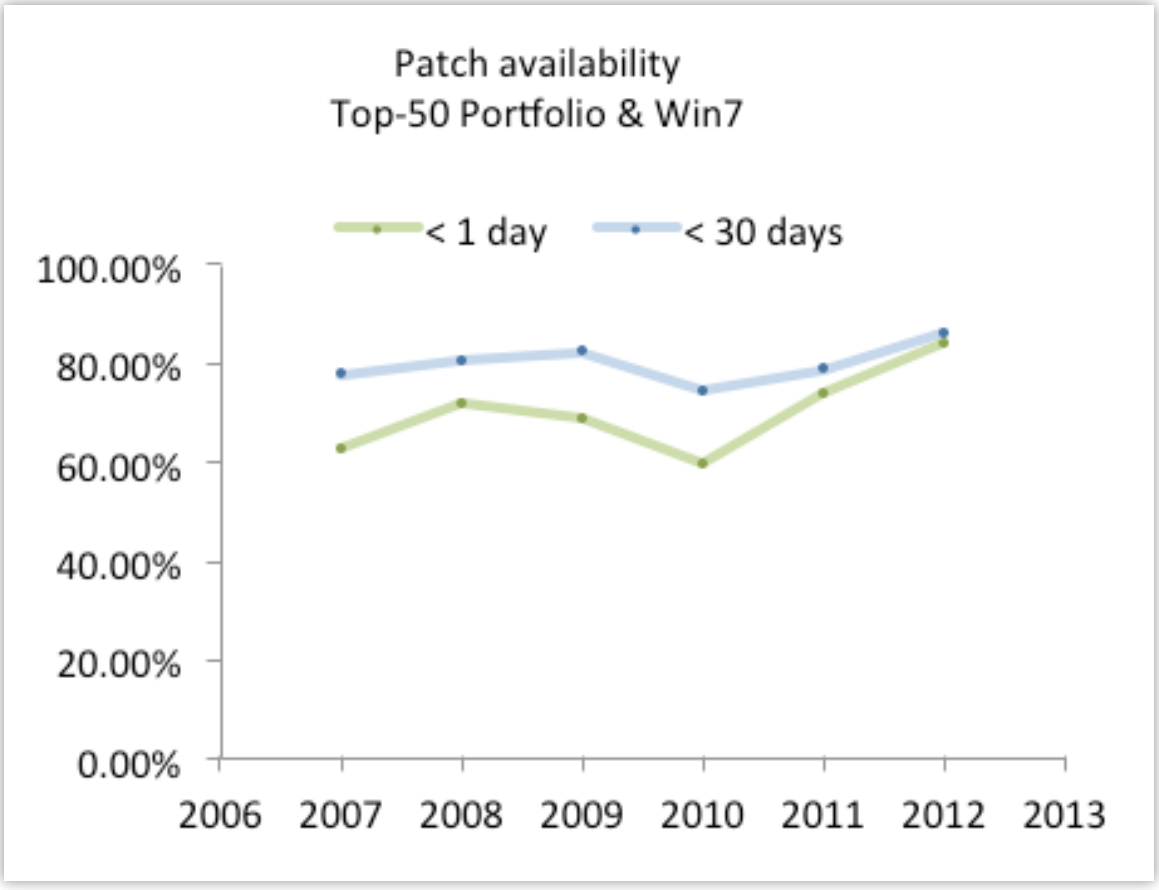
The fact that 20% of vulnerabilities are without patches for longer than the first day of disclosure, however, means that patch management is not sufficient protection – vulnerability intelligence and alternative remediation measures are required, if organizations wish to keep their IT infrastructure watertight.

It is unlikely that many more than 80% of vulnerabilities will have a patch available in the future, and it is realistic to assume that 20% is a representative proportion of software products that are not patched quickly – for example as a result of the lack of vendor resources, uncoordinated releases, zero-days or vulnerabilities in End-of-Life products.

Increased cooperation between vendors and researchers

That 80% of vulnerabilities have a patch available on the day of disclosure is an improvement to the previous year, 2011, in which 72% had a patch available on the day of disclosure. The most likely explanation for this improvement in Time-to-Patch is that more researchers coordinate their vulnerability reports with vendors, which mean that patches are available immediately.

FIGURE 17: TOP 50



Browser Security

This snapshot of browser security in the most popular browsers (Google Chrome, Mozilla Firefox, Internet Explorer, Opera, Safari) shows an increase in the number of vulnerabilities discovered.

But it is a very positive trend that patches are made available very quickly for vulnerabilities in browsers because it indicates that browser vendors are serious about security.

FIGURE 19: ALL BROWSERS

Summary		
Advisories YoY	75 (63)	19%
Vulnerabilities YoY	739 (629)	17%
Report date	2012-12-31	
Reporting period	2012/	
Overview		
	Advisories	Vulnerabilities
YTD	75	739
Preceding 12 mo.	63	629
Last 12 mo.	75	739
YoY Trend	19%	17%

FIGURE 20: ALL BROWSERS

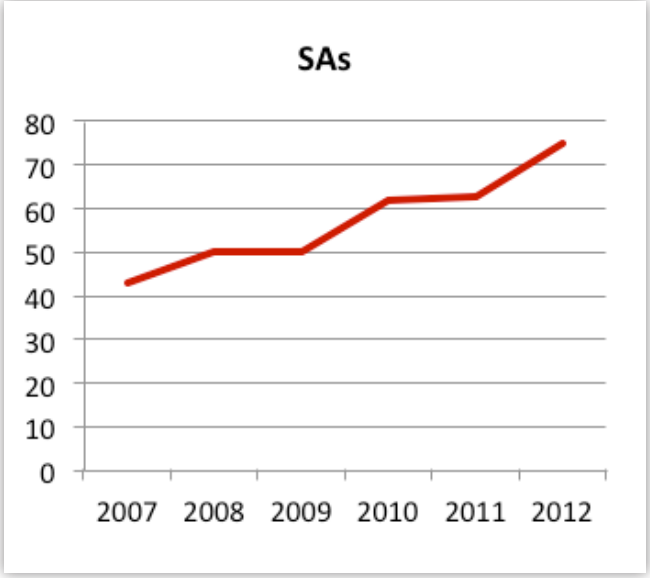


FIGURE 21: ALL BROWSERS

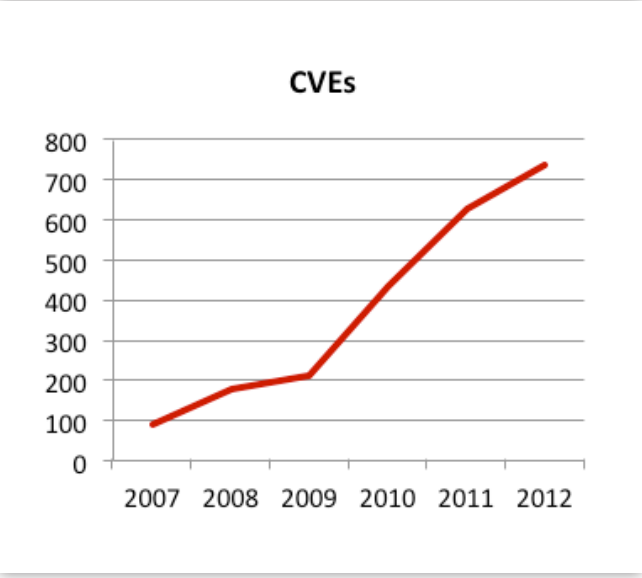


FIGURE 22: ALL BROWSERS

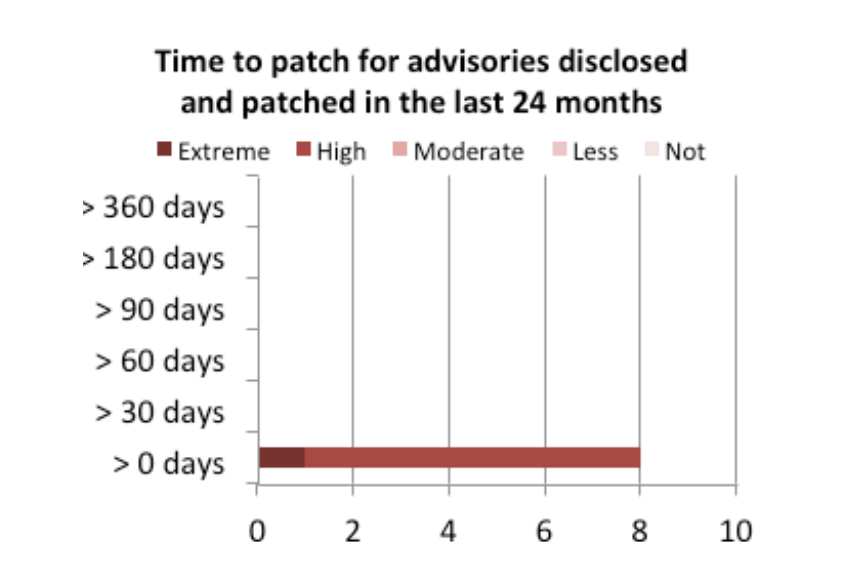


FIGURE 23: ALL BROWSERS

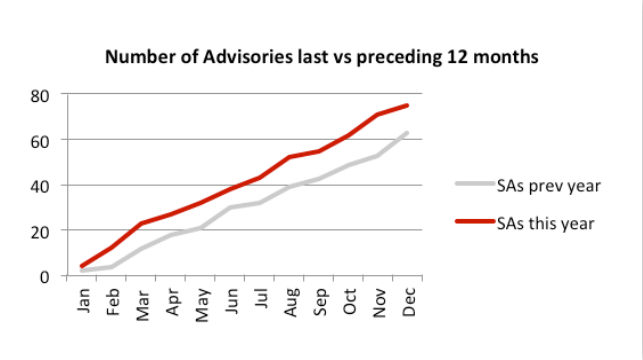


FIGURE 24: ALL BROWSERS

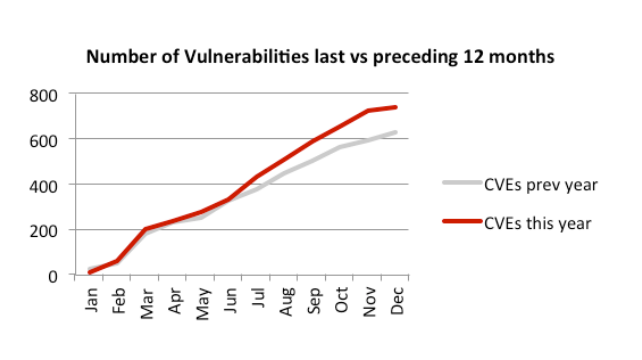


FIGURE 25: ALL BROWSERS

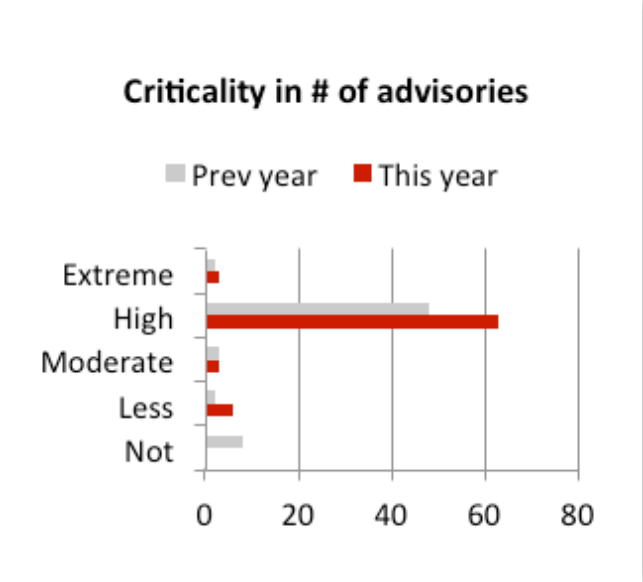
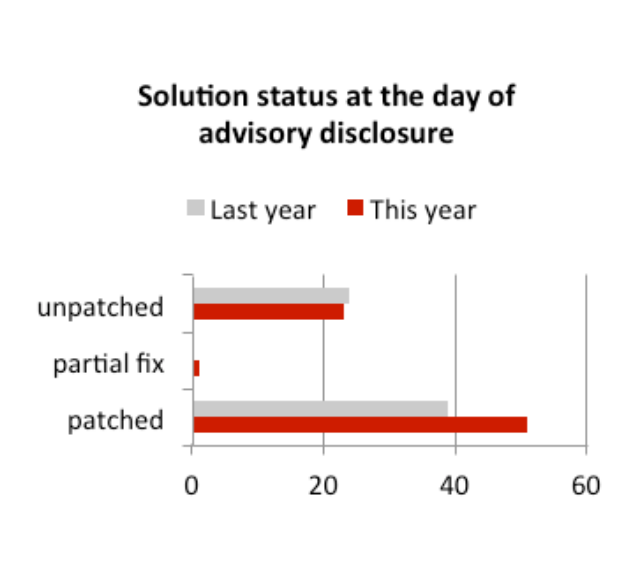


FIGURE 26: ALL BROWSERS



SCADA Security

Over the past 5 years, we have seen a rise in the number of vulnerabilities in SCADA software.

SCADA software today is at the stage mainstream software was 10 years ago: security updates are erratic (there is great variation in how they are handled), compared to what we are accustomed to in mainstream programs.

Many vulnerabilities remain unpatched for longer than one month in SCADA software.

FIGURE 27: REPRESENTATIVE SELECTION

Summary		
Advisories YoY	59 (73)	-19%
Vulnerabilities YoY	104 (130)	-20%
Report date	2012-12-31	
Reporting period	2012/	
Overview		
	Advisories	Vulnerabilities
YTD	59	104
Preceding 12 mo.	73	130
Last 12 mo.	59	104
YoY Trend	-19%	-20%

FIGURE 28: REPRESENTATIVE SELECTION

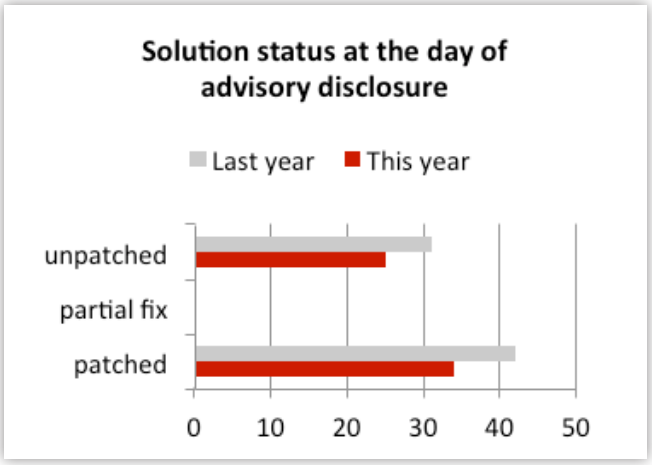


FIGURE 29: REPRESENTATIVE SELECTION

FIGURE 30: REPRESENTATIVE SELECTION

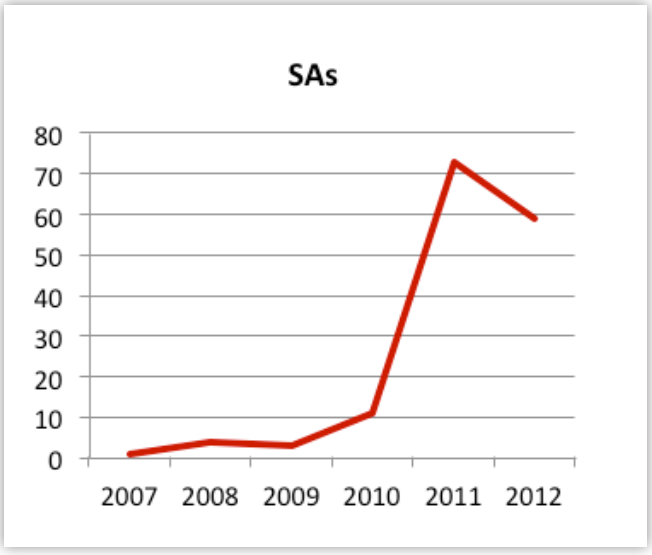


FIGURE 31: REPRESENTATIVE SELECTION

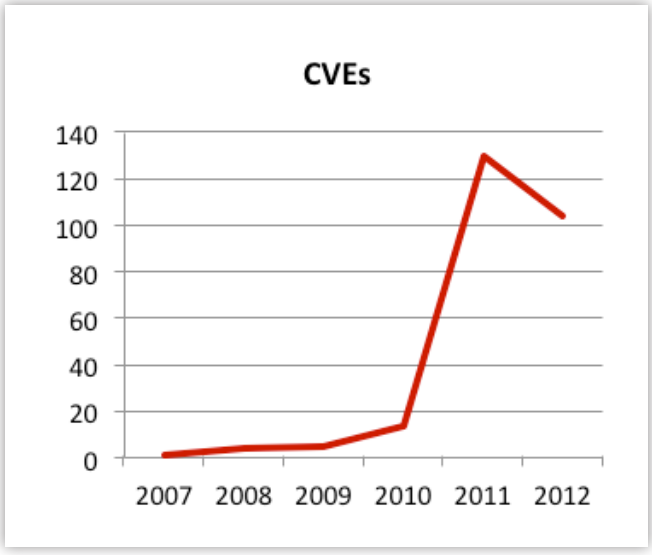


FIGURE 32: REPRESENTATIVE SELECTION

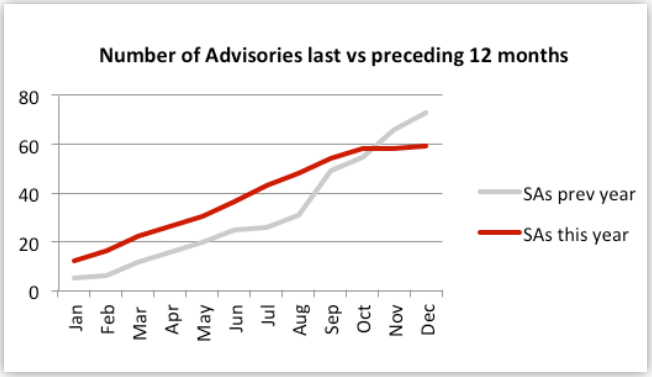


FIGURE 33: REPRESENTATIVE SELECTION

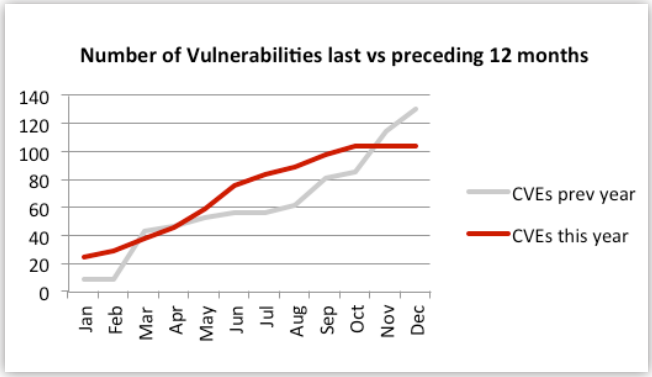


FIGURE 34: REPRESENTATIVE SELECTION

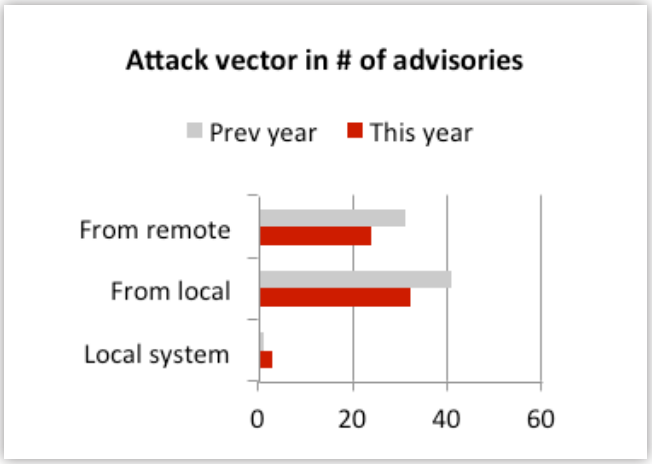
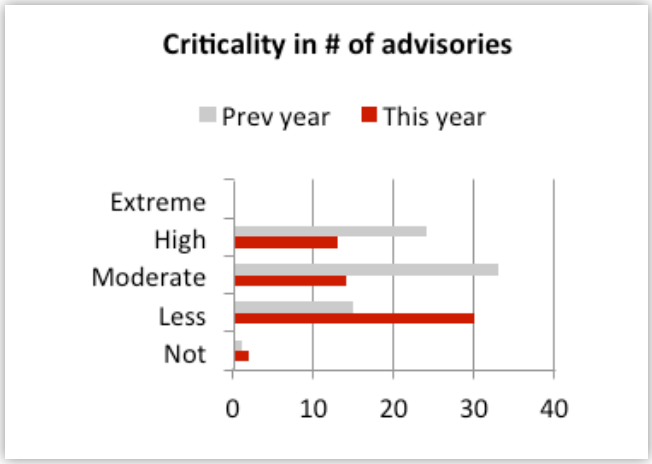


FIGURE 35: REPRESENTATIVE SELECTION



Zero-Days

Not many zero-day vulnerabilities were identified in 2012 – only 8 in total in the top 50 software portfolio.

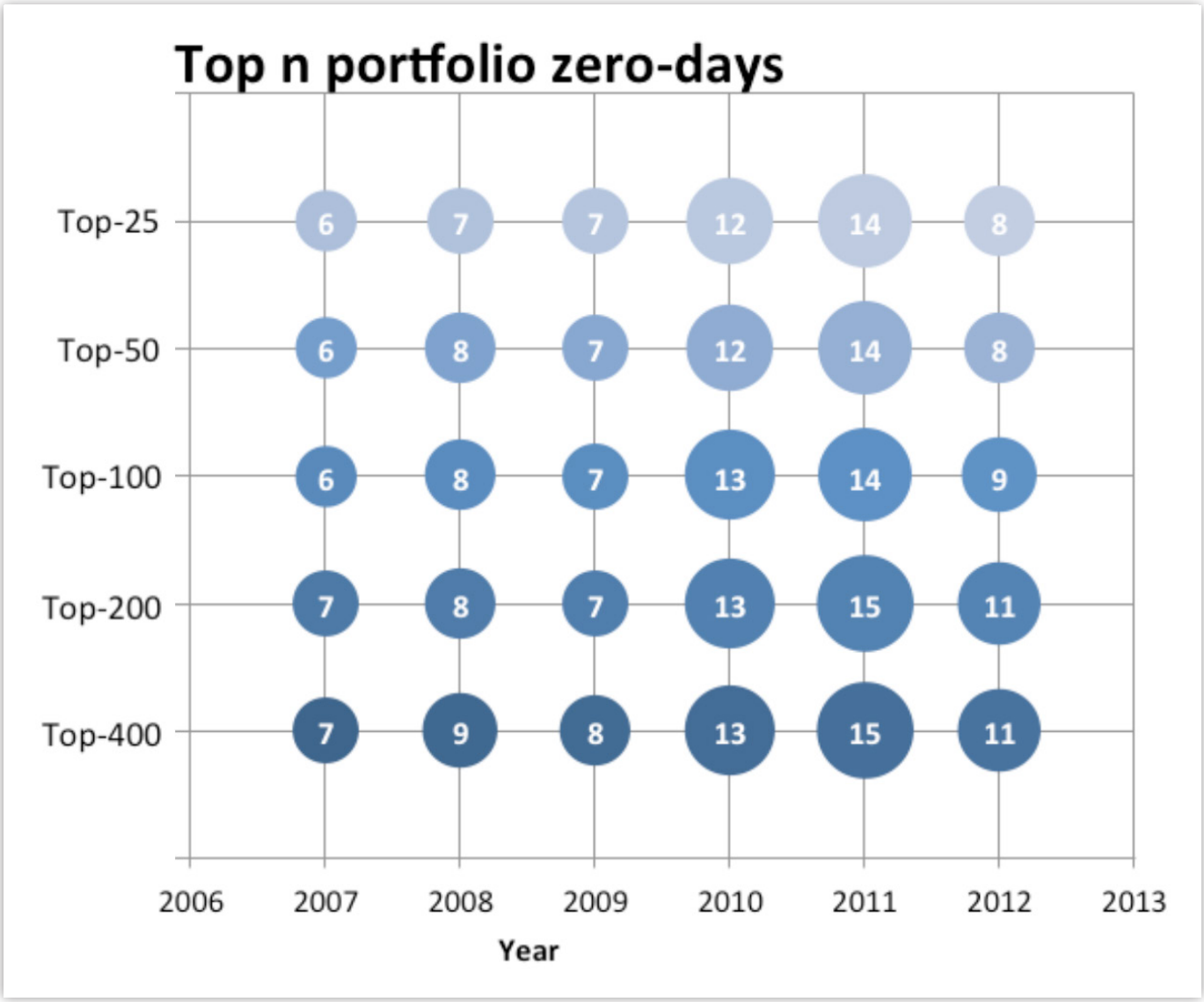
This makes 2010 and 2011 stand out as exceptions (with 12 and 14 zero-day vulnerabilities respectively).

These numbers are good news. They indicate that researchers and software vendors are good at coordinating their efforts, discovering vulnerabilities and issuing patches and workarounds for them, before they are discovered by hackers.

FIGURE 36: ZERO-DAYS IDENTIFIED BY SECUNIA IN 2012

Year	Top-25	Top-50	Top-100	Top-200	Top-400
2007	6	6	6	7	7
2008	7	8	8	8	9
2009	7	7	7	7	8
2010	12	12	13	13	13
2011	14	14	14	15	15
2012	8	8	9	11	11

FIGURE 37: ZERO-DAYS IDENTIFIED BY SECUNIA IN 2012



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.

Genuine and Shared Vulnerabilities

Genuine Vulnerabilities
Vulnerabilities found in the software of this and only this vendor. These are vulnerabilities in the code developed by this vendor that are not shared in the products of other vendors.

Shared Vulnerabilities
Vulnerabilities found in the software of this and other vendors due to the sharing of either code, software libraries, or product binaries. If vendor A develops code or products that are also used by vendor B, the vulnerabilities found in these components are genuine for vendor A and counted as shared vulnerabilities for vendor B.

Total Vulnerabilities
The total number of vulnerabilities found in the products of the vendor, be it genuine or shared vulnerabilities. These are the vulnerabilities that affect the users of the vendor's products.

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 as of December 2012 and the number of vulnerabilities (CVEs) affecting the program in 2011 and 2012.

The ranking and market share is derived from anonymous scans of the Secunia PSI in December 2012. 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), Adobe Reader (#8), and Adobe AIR (#20) share code components and thereby also share numerous vulnerabilities. For each program the unique number of CVEs of this given program in the given year is listed.

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

RANK	TYPE	PROD	ADVS	CVES	VULNS
OS	MS	MICROSOFT WINDOWS 7	29	51	50
1	MS	MICROSOFT XML CORE SERVICES (MSXML)	1	1	1
2	MS	MICROSOFT INTERNET EXPLORER	10	40	41
3	MS	MICROSOFT WINDOWS MEDIA PLAYER	0	0	0
4	MS	MICROSOFT .NET FRAMEWORK	6	14	14
5	TP	ADOBE FLASH PLAYER	10	69	67
6	MS	MICROSOFT VISUAL C++ REDISTRIBUTABLE	0	0	0
7	TP	ORACLE JAVA JRE SE	4	62	66
8	TP	ADOBE READER	4	42	43
9	MS	MICROSOFT SILVERLIGHT	2	5	5
10	MS	MICROSOFT WINDOWS DEFENDER	0	0	0
11	MS	MICROSOFT WORD	2	3	3
12	MS	MICROSOFT EXCEL	2	10	10
13	MS	MICROSOFT POWERPOINT	0	0	0
14	MS	WINDOWS DVD MAKER	0	0	0
15	TP	MOZILLA FIREFOX	21	164	257
16	TP	APPLE SOFTWARE UPDATE	0	0	0
17	MS	MICROSOFT OUTLOOK	0	0	0
18	TP	COMDLG32 ACTIVEX CONTROL	0	0	0
19	MS	MICROSOFT POWERSHELL	0	0	0
20	TP	ADOBE AIR	6	58	56
21	TP	GOOGLE CHROME	28	293	291
22	MS	DRIVER PACKAGE INSTALLER (DPINST)	0	0	0
23	TP	APPLE QUICKTIME	2	26	29
24	TP	CCLEANER	0	0	0
25	MS	MICROSOFT OFFICE (EXTENSION FOR FIREFOX)	0	0	0
26	MS	WINDOWS LIVE MESSENGER	0	0	0
27	MS	MICROSOFT ACCESS	0	0	0
28	MS	MICROSOFT POWERPOINT VIEWER	0	0	0
29	MS	WINDOWS LIVE	0	0	0
30	MS	MICROSOFT PUBLISHER	0	0	0
31	TP	REALTEK VOICE MANAGER	0	0	0

32	TP	SKYPE	1	0	1
33	TP	VLC MEDIA PLAYER	5	23	11
34	TP	APPLE ITUNES	3	237	243
35	TP	ITDETECTOR ACTIVEX CONTROL	0	0	0
36	TP	APPLE BONJOUR FOR WINDOWS	0	0	0
37	MS	CAPICOM	0	0	0
38	MS	WINDOWS LIVE ESSENTIALS	0	0	0
39	TP	GOOGLE EARTH	0	0	0
40	TP	REALTEK AC 97 UPDATE AND REMOVE DRIVER TOOL	0	0	0
41	MS	MICROSOFT OFFICE PICTURE MANAGER	0	0	0
42	TP	INSTALLSHIELD UPDATE SERVICE	0	0	0
43	MS	WINDOWS LIVE PHOTO GALLERY 2011	0	0	0
44	MS	WINDOWS MEDIA CENTER	0	0	0
45	MS	WINDOWS LIVE MOVIE MAKER 2011	0	0	0
46	MS	MICROSOFT OFFICE TEMPLATE AND MEDIA CONTROL ACTIVEX CONTROL	0	0	0
47	TP	ADOBE UPDATER	0	0	0
48	MS	MICROSOFT VISIO VIEWER	3	7	7
49	MS	MICROSOFT WINDOWS GENUINE ADVANTAGE ACTIVEX CONTROL	0	0	0
50	TP	NVIDIA CONTROL PANEL	0	0	0

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 developed 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