

# Secunia Vulnerability Review

# 2015

Key figures and facts on vulnerabilities from a global information security perspective

Published March 25, 2015



# Index

Global Trends – All Products	3
Global Trends – Top 50 Portfolio	3
Vendor Update – Top 50 Portfolio	8
Time-to-Patch – All Products	11
Time-to-Patch – Top 50 Portfolio	11
Zero-day Vulnerabilities	12
Browser Security	13
PDF Reader Security	15
Open Source – Learnings from 2014	16

## Appendix

Secunia Software Vulnerability Tracking Process	18
Attack Vector	19
Unique and Shared Vulnerabilities	19
Secunia Vulnerability Criticality Classification	20
The 20 Core Products with Most Vulnerabilities	21
The Top 50 Software Portfolio	22
Glossary	23

# Vulnerability Update

## Numbers – All Products

### Numbers - All products

The absolute number of vulnerabilities detected was 15,435, discovered in 3,870 applications from 500 vendors. The number shows a 55% increase in the five year trend, and a 18% increase from 2013 to 2014.

Since 2013, the number of vendors behind the vulnerable products has decreased by 11% and the amount of vulnerable products has increased by 22%.

The 20 core products<sup>(1)</sup> with the most reported vulnerabilities in 2014 span different criticalities and attack vectors. and are comprised of browsers, client managers, an open source library and an operating system.

### Criticality – All Products

11% of vulnerabilities in 2014 were rated as 'Highly Critical', and 0.3% as 'Extremely Critical'.

The most notable changes in criticality levels occurred in the 'Moderately' and 'Not' critical brackets, with an increase from 23.5% in 2013 to 28.1%, and from 7.6% in 2013 to 13.5%, respectively.

'Highly Critical' decreased from 16.2% in 2013 to 11% in 2014.

### Attack Vector – All Products

With a 60.2% share, the primary attack vector available to attackers to trigger a vulnerability for all products in 2014 was again via remote network, a drop from the 73% the year before. Local network has correspondingly increased, from 20% in 2013, to 33.4% in 2014. In 2012, local network only represented 5%. Local system remained stable, from 7% in 2013, to 6.4% in 2014.

(1): Find the list of the 20 core products with the most vulnerabilities in the Appendix

## Global Trends – Top 50 Portfolio <sup>(2)</sup>

### Numbers - Top 50 Portfolio

The number of vulnerabilities in the Top 50 portfolio was 1,348, discovered in 17 products from 7 vendors plus the most used operating system, Microsoft Windows 7. The number shows a 42% increase in the 5 year trend, and a 11% increase from 2013 to 2014.

### Criticality – Top 50 Portfolio

The combined number of 'Highly Critical' and 'Extremely Critical' vulnerabilities: 74.6% represented the majority of vulnerabilities in the Top 50 rated by Secunia in 2014.

### Attack Vector – Top 50 Portfolio

With a 91.8% share, the foremost attack vector available to attackers to trigger a vulnerability in the Top 50 portfolio was Remote Network. This is an increase compared to 2013. Local Network saw a decrease, from 2.7% in 2013, to 2.2% in 2014. Local System recorded a decrease compared to last year, from 10.6%, to 6% in 2014.

(2): Find the list of the Top 50 applications in the Appendix

## What is the Top 50 Portfolio? <sup>(2)</sup>

To assess how exposed endpoints are, we analyze the types of products typically found on an endpoint. Throughout 2014, 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 76 applications installed on it.

Naturally, there are country- and region-based variations regarding which applications 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 2014. These 50 applications are comprised of 34 Microsoft applications and 16 non-Microsoft (third-party) applications.

## We divide the products into three categories

### Product composition, PSI computer

**Microsoft applications:** Represent on average 40% of the applications on a computer with the PSI installed.

**Non-Microsoft applications:** Software from all other vendors – represents 60% of the applications on a computer with the PSI installed.

**Operating Systems:** We track vulnerabilities in Windows operating systems: Windows XP<sup>(3)</sup>, Windows Vista, Windows 7 and Windows 8.

### Product composition, Top 50 portfolio

**Microsoft applications:** Represent 67% of the Top 50 applications on a computer with the PSI installed.

**Non-Microsoft applications:** Software from all other vendors – represents 31% of the Top 50 applications on a computer with the PSI installed.

**Operating Systems:** We track vulnerabilities in the most prevalent operating system Windows 7. Windows 7 represents 2% of the applications in the Top 50 portfolio.

(2): Find the list of the Top 50 applications in the Appendix

(3): Windows XP is only tracked until April 2014 when it went End of Life.

FIGURE 1: SECUNIA ADVISORIES/VULNERABILITIES IN ALL PRODUCTS

	Secunia Advisories	Vulnerability count	Vendors	Products *
Average 2009-13	3,262	9,956	633	3,202
Total 2014	4,217	15,435	500	3,870
Trend 5 yr	29%	55%	-21%	21%
Trend 2013/14	27%	18%	-11%	22%

\* : Number of applications, including different major versions of the same product. The method differs from previous years where all major versions of the same product were counted as a single application. The numbers used in this figure for Products are comparable, as they are reached using the same method. Consequently, the year-on-year comparison in this figure is reliable.

FIGURE 2: SECUNIA ADVISORIES/VULNERABILITIES IN ALL PRODUCTS

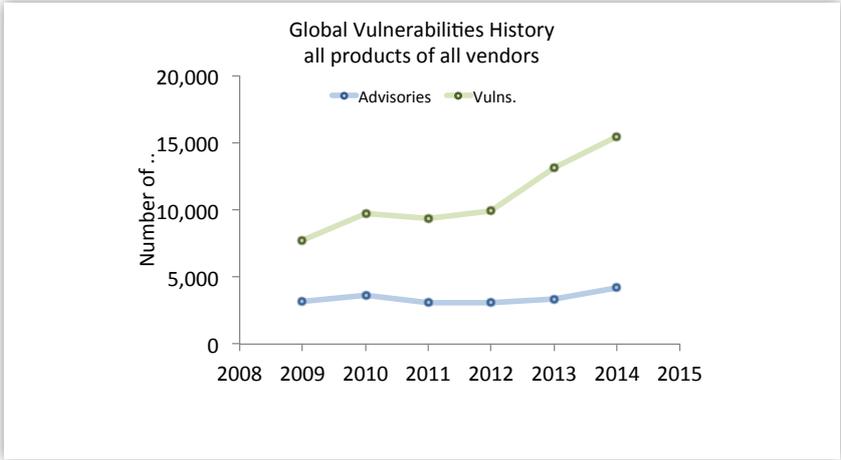
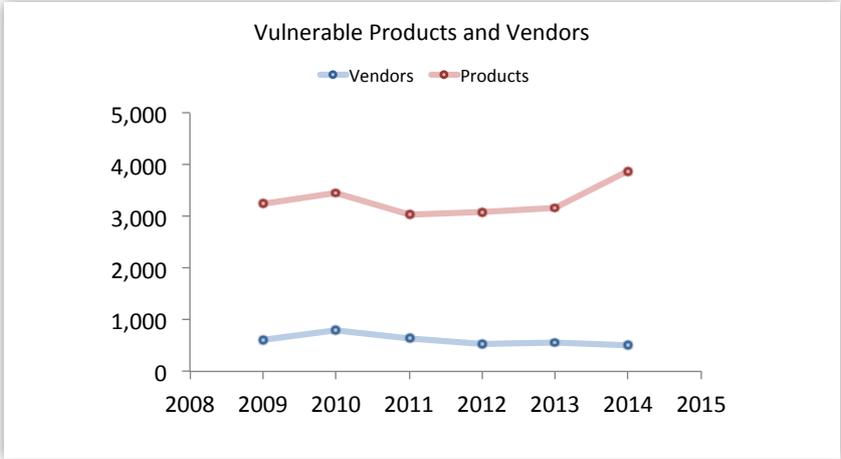


FIGURE 3: VULNERABLE PRODUCTS AND VENDORS, ALL PRODUCTS



See the Appendix for methodology, including definitions of Secunia Advisories, CVEs and Vulnerabilities; criticality ratings, attack vectors.

FIGURE 4: CRITICALITY, ALL PRODUCTS

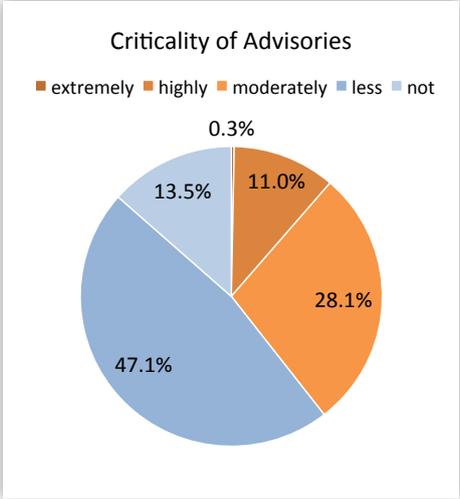


FIGURE 5: ATTACK VECTORS, ALL PRODUCTS

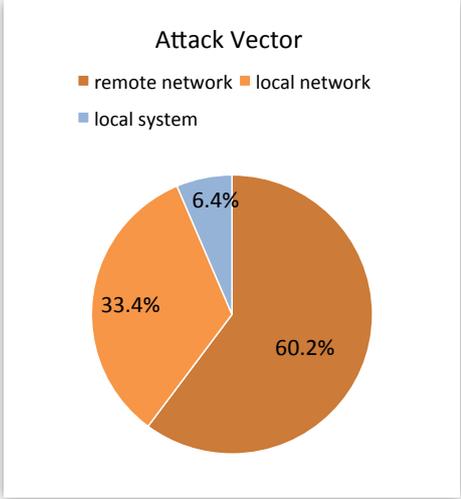
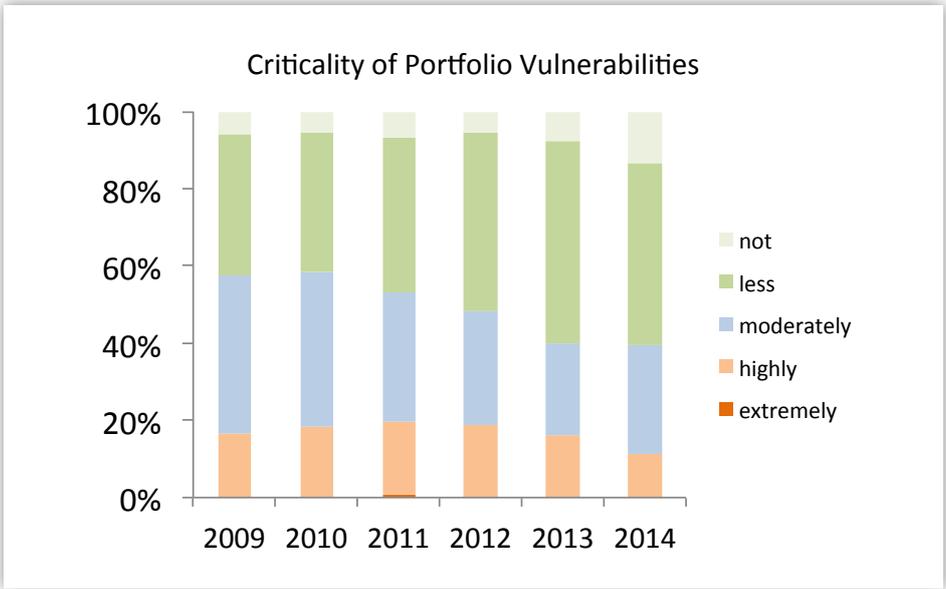


FIGURE 6: CRITICALITY OF VULNERABILITIES IN ALL PRODUCTS, HISTORICALLY



See the Appendix for methodology, including definitions of Secunia Advisories, CVEs and Vulnerabilities; criticality ratings, attack vectors.

FIGURE 7: SECUNIA ADVISORIES/VULNERABILITIES IN TOP 50 PRODUCTS

	Secunia Advisories	Vulnerability count	Vendors	Products *
Average 2009-13	128	949	6	22
Total 2014	134	1,348	7	18
Trend 5 yr	5%	42%	9%	-20%
Trend 2013/14	-11%	11%	0%	-33%

\* All major versions of the same product are counted as a single application.

The numbers used in this figure for Products are comparable, as they are reached using the same method.

Consequently, the year-on-year comparison in this figure is reliable.

FIGURE 8: VULNERABLE PRODUCTS AND VENDORS, TOP 50

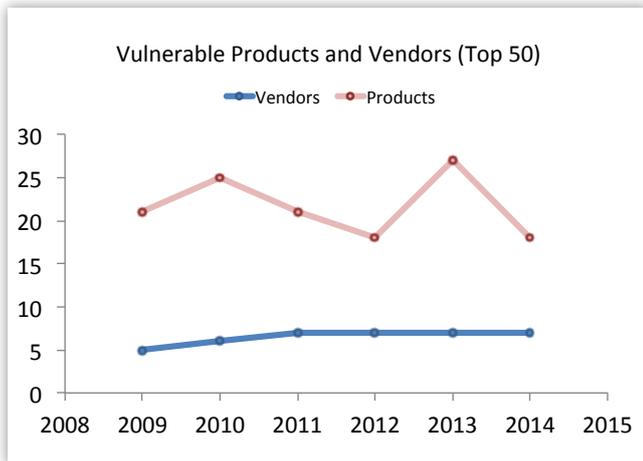


FIGURE 9: SECUNIA ADVISORIES/VULNERABILITIES IN TOP 50 PRODUCTS

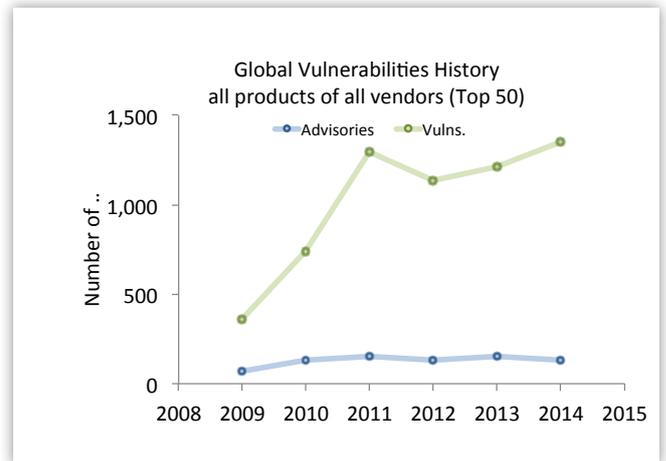


FIGURE 10: CRITICALITY, TOP 50

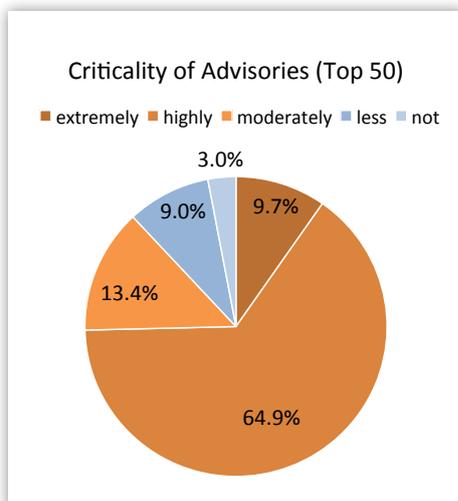
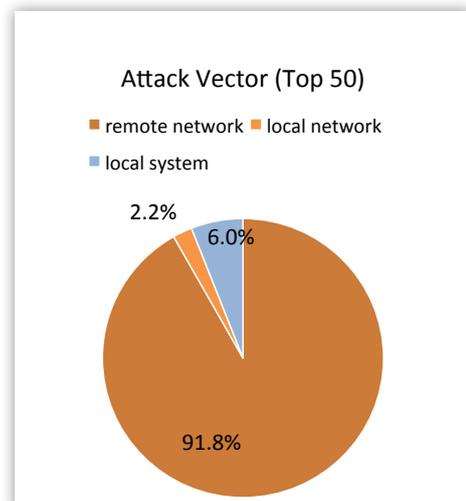


FIGURE 11: ATTACK VECTORS, TOP 50



# Vendor Update – Top 50 Portfolio<sup>(2)</sup>

Different vendors have different security update mechanisms. Microsoft applications (including Windows 7 operating system), which account for 69% of the applications in the Top 50 portfolio, are updated automatically. But Microsoft applications are only responsible for 23.1% of the vulnerabilities discovered in the Top 50 portfolio.

Vulnerabilities in non-Microsoft applications in your system have a significant impact on security efforts. In this section we break down the source of vulnerabilities in the Top 50 portfolio.

## Non-Microsoft software

In 2014, 76.9% of the vulnerabilities affecting the Top 50 applications in the representative software portfolio affected non-Microsoft applications. This means that 23.1% of the remaining vulnerabilities in the Top 50 applications installed on the computers of PSI users stem from the Windows 7 operating system and Microsoft applications.

On average, over a five year period, the share of non-Microsoft vulnerabilities has hovered around 78%, peaking at 88.5% in 2012. This high-level percentage plateau is significant and makes it evident why end users and organizations cannot manage security by focusing on patching their Microsoft applications and operating systems alone. If they do that, they are only protecting their computers and IT infrastructures from 23.1% – less than a quarter – of the total risk posed by vulnerabilities.

Non-Microsoft software is by definition issued by a variety of vendors, who each have their own security update mechanisms and varying degrees of focus on security. Consequently, it is up to the users of personal computers and administrators of IT infrastructures to make sure that they stay updated about the security status of all the different products on their computers. This is a major challenge because not all vendors offer automated update services and push security updates to their users. Therefore, users and administrators have to resort to alternative methods and sources of information to ensure that their systems are protected from vulnerable software, and that patches or other mitigating actions are deployed.

No IT administrator has the time and resources to manually keep track of the patch state of all the applications on all

computers in their IT infrastructure on a continuous basis. Similarly, it is an unrealistic assumption that an end user is going to take the time to stay updated by visiting the websites of a multitude of vendors whose applications are installed on their PC – and then search, download and apply individual security updates.

## Operating systems

The choice of operating system had a minor impact on the total number of vulnerabilities on a typical endpoint: In 2014, 2.4% of vulnerabilities were reported in Windows 7, the operating system we are tracking with the Top 50 portfolio.

## Microsoft applications

Again this year, there were significantly more vulnerabilities reported in Microsoft applications in 2014 compared to the previous year: up from 15.9% to 20.7%. The vulnerability count in Microsoft applications was 279 in 2014; 45.3% higher than in 2013.

## Decrease of vulnerabilities in Windows

Data shows a decrease in the number of vulnerabilities recorded in all Windows operating systems:

- Windows 8 went from 156 in 2013, to 105 in 2014.
- Windows 7 went from 102 in 2013, to 33 in 2014.
- Windows Vista went from 102 in 2013, to 30 in 2014.
- Windows XP went from 99 in 2013, to 5 in 2014.

Windows XP went End of Life in April 2014, and therefore new vulnerabilities in the OS are not recorded. Secunia data indicates that globally, 11.9% of end users were still using Windows XP in December 2014.

The decrease in vulnerabilities in Windows operating systems brings the numbers down to levels similar to the years preceding 2013.

(2): Find the list of the Top 50 applications in the Appendix

FIGURE 12 :VULNERABILITIES IN TOP 50 PORTFOLIO, HISTORICALLY

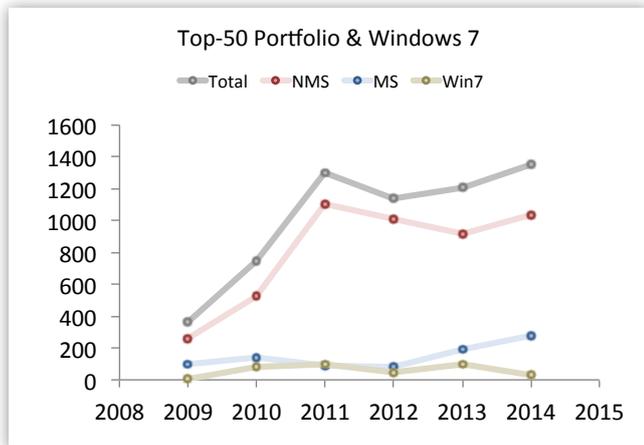


FIGURE 13: VULNERABILITIES IN WINDOWS OPERATING SYSTEMS, HISTORICALLY

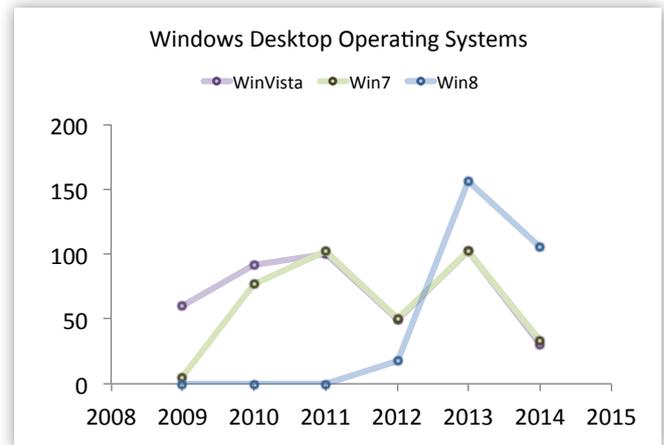


FIGURE 14:VULNERABILITIES IN TOP 50 IN 2014

<b>Breakdown of end-point vulnerabilities in 2014</b>			
	WinVista	Win7	Win8
Operating System	30	33	105
Microsoft Programs	279	279	279
Non-Microsoft Programs	1036	1036	1036
<b>Total</b>	<b>1345</b>	<b>1348</b>	<b>1420</b>

FIG 15: CRITICALITY OF VULNERABILITIES IN TOP 50, HISTORICALLY

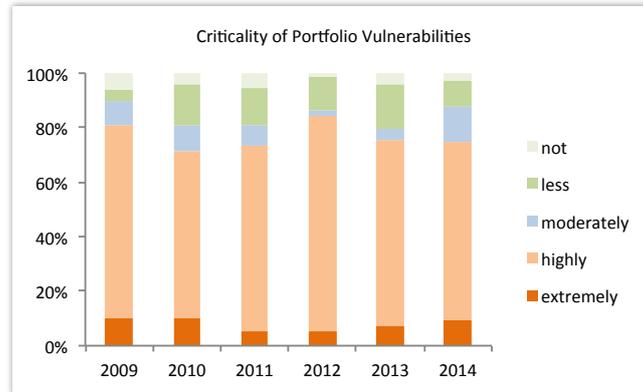


FIGURE 16: SHARE BY SOURCE, TOP 50

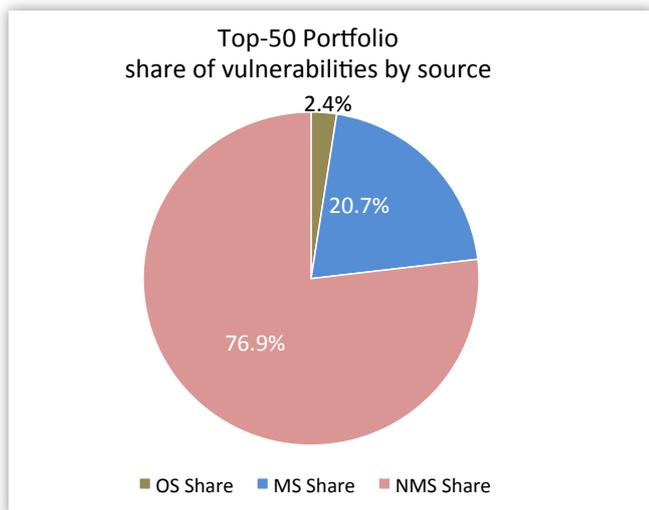


FIGURE 17: SHARE OF NON-MICROSOFT VULNERABILITIES IN TOP 50, HISTORICALLY

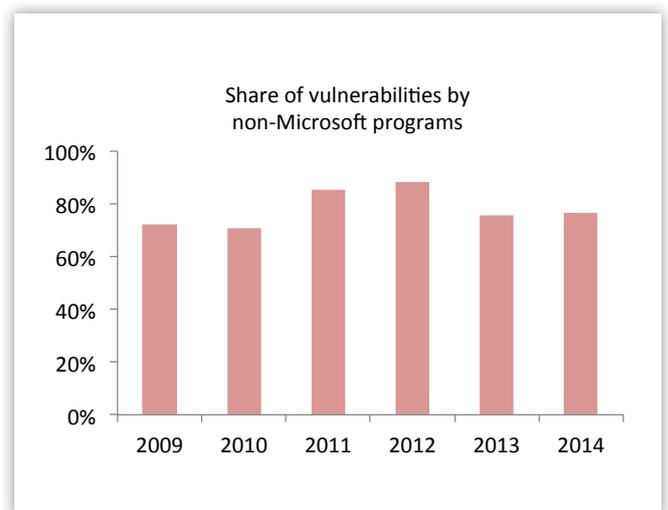
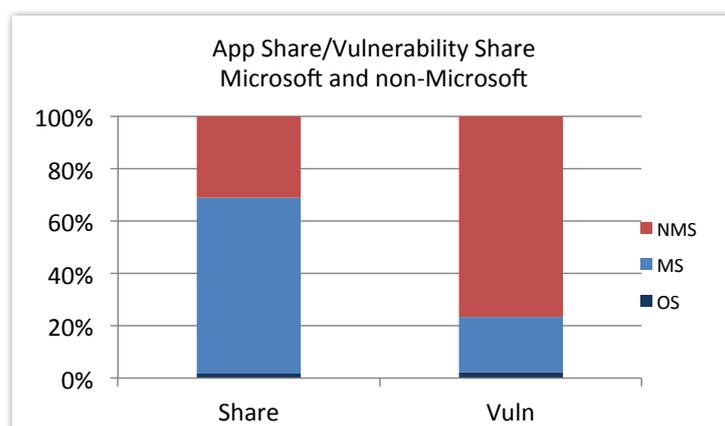


FIGURE 18: TOP 50 APP SHARE/VULNERABILITY SHARE MICROSOFT AND NON-MICROSOFT



See the Appendix for methodology, including definitions of Secunia Advisories, CVEs and Vulnerabilities; criticality ratings, attack vectors.

## Time-to-Patch<sup>(4)</sup>

In 2014, 83.1% of all vulnerabilities had a patch available on the day of disclosure - an increase compared to the 78.5% in 2013.

In the Top 50 applications, 86.6% of vulnerabilities had a patch available on the day of disclosure. This number is on a par with the 86% time-to-patch rate that was recorded in 2013.

The 2014 results remain positioned at the higher end of the scale, indicating that it is still possible to remediate the majority of vulnerabilities.

It is however worth noting that some vendors choose to issue major product releases rather than minor updates, which can be more complex for users and administrators to manage manually.

The 2014 time-to-patch results show that 16.9% / 13.4% of vulnerabilities respectively were without patches for longer than the first day of disclosure. This percentage is a representative proportion of software products that are not patched immediately – e.g. due to a lack of vendor resources, uncoordinated releases or, more rarely, 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 a variety of mitigating efforts are required to ensure sufficient protection, in support of patch management efforts.

### Cooperation between vendors and researchers

That 83.1% of vulnerabilities in All products, and 86.6% 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 49.9% recorded in 2009 in All products. The most likely explanation for the continuously improving 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.

30 days after day of disclosure, 84.3% of vulnerabilities have a patch available, indicating that if a patch is not available on the first day, the vendor does not prioritize patching the vulnerability.

FIGURE 19: PATCH AVAILABILITY FOR VULNERABILITIES IN ALL PRODUCTS, HISTORICALLY

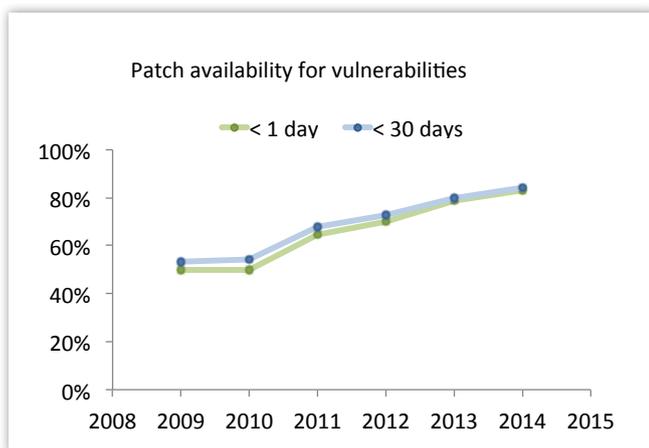
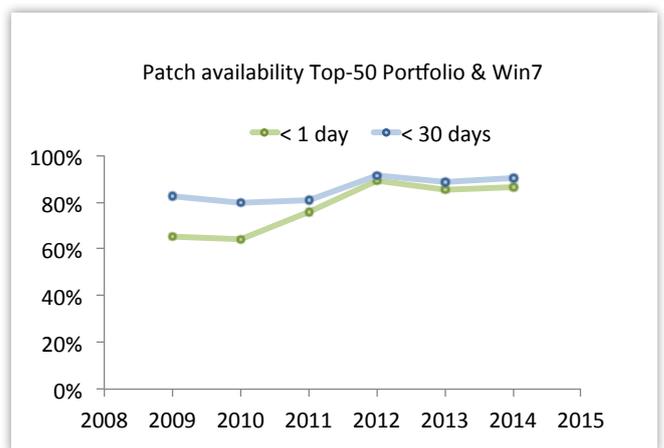


FIGURE 20: PATCH AVAILABILITY FOR VULNERABILITIES IN TOP 50 PRODUCTS, HISTORICALLY



(4): "The Time-to-Patch numbers released in 2015 and 2014 are not directly compatible with the numbers released in previous years. We have applied a different method from 2014 onwards because an increasing number of vendors, particularly browser vendors, started to 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."

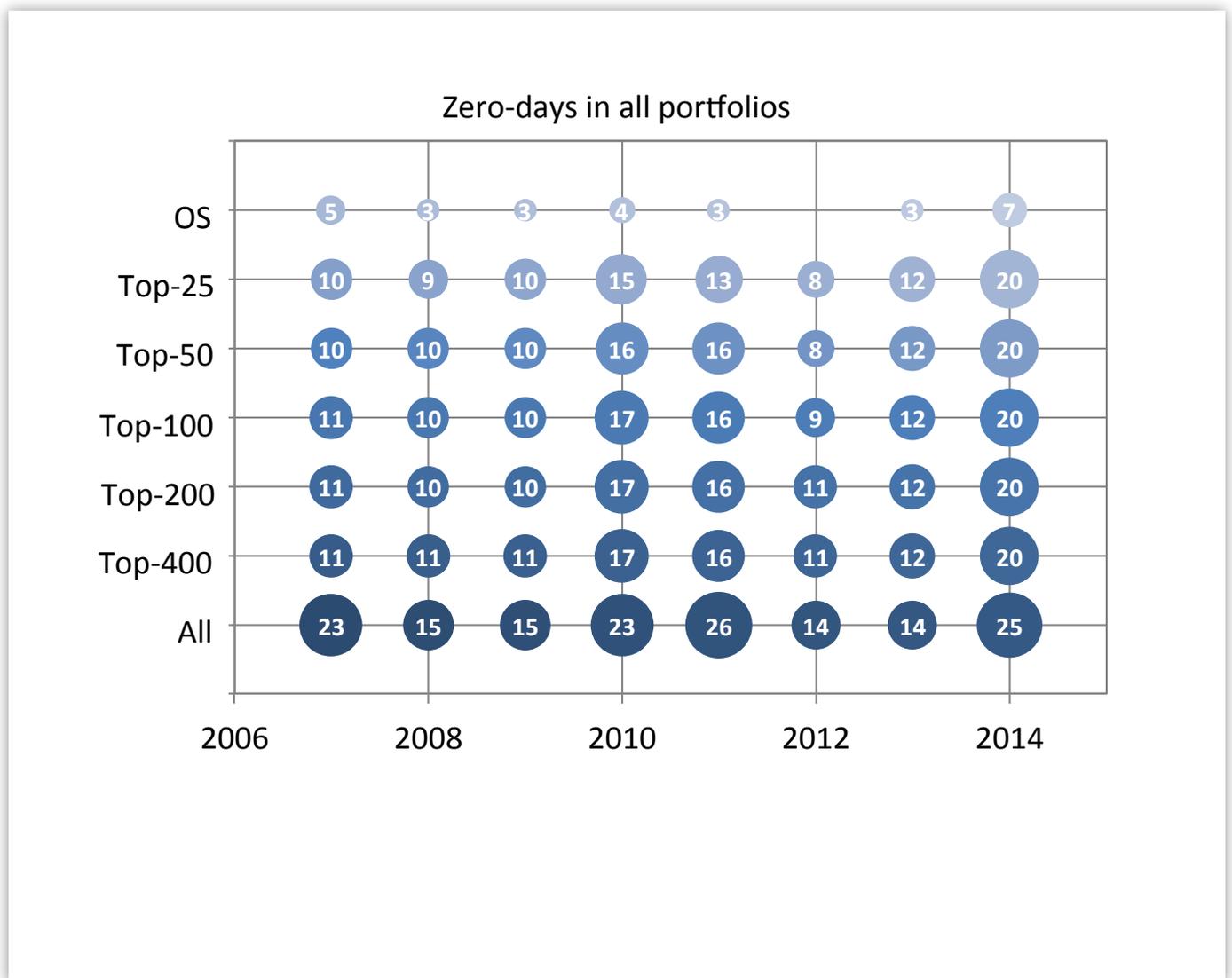
# Zero-Days

2014 saw a dramatic increase in the number of discovered zero-day vulnerabilities – 25 zero-day vulnerabilities in All products, compared to 14 the year before. 20 of the 25 zero-day vulnerabilities were discovered in the Top 25 portfolio, compared to 12 the year before.

A zero-day vulnerability is a vulnerability that is being actively exploited by hackers before it is publicly known.

The fact that so many zero-days were discovered in 2014 is interesting when considering the potential attack vector zero-day vulnerabilities represent in one of the media favorites of 2014: APT (Advanced Persistent Threat) attacks.

FIGURE 21: ZERO-DAY VULNERABILITIES REGISTERED BY SECUNIA IN 2014



See the Appendix for methodology, including definitions of Secunia Advisories, CVEs and Vulnerabilities; criticality ratings, attack vectors.

# Browser Security

This snapshot of browser security outlines the evolution of vulnerabilities relating to the five most popular browsers (Google Chrome, Mozilla Firefox, Internet Explorer, Opera and Safari). Overall, data shows that there were 1,035 vulnerabilities in these browsers in 2014 compared to 728 in 2013 – a year-on-year increase of 42%. The majority of these vulnerabilities were rated as 'Highly Critical'.

Figure 23 illustrates the distribution of vulnerabilities across the five browsers in 2014, including their market share and exposure level, and patch status.

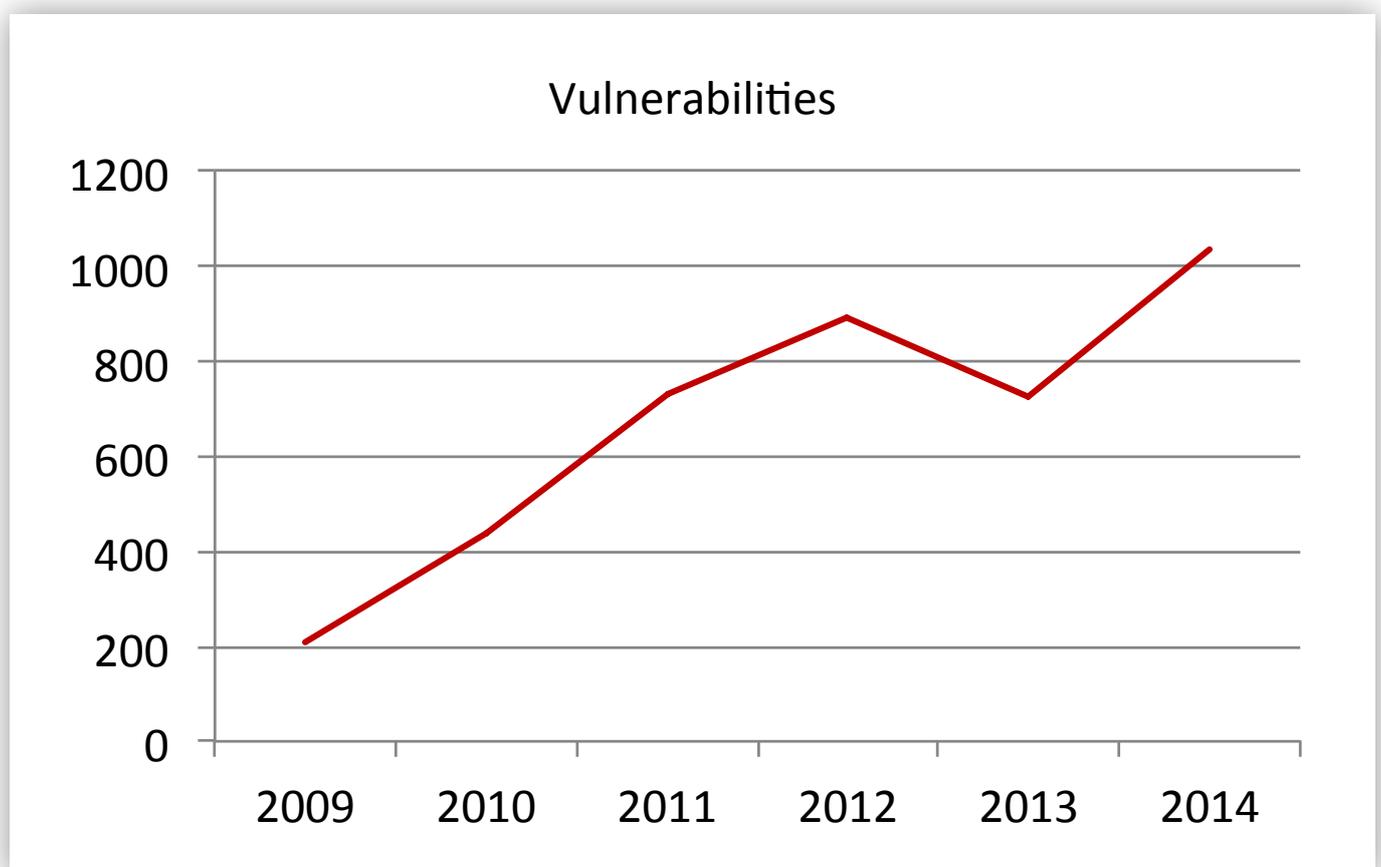
In Figure 24 we have ranked the Top 5 browsers, based on risk exposure. We rank them by exposure based on two parameters: "Market share" in %, multiplied by "Unpatched" in %. That is, how widespread the browser is, multiplied by how many of the private users who have installed the browser neglected to apply a patch, even though a patch is available. The position of the bubbles on the axes shows the market

share and unpatched level. The size of the bubbles shows the exposure, indicating how exposed a target the software is. 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%, Firefox and Chrome are actually installed on 64% and 65% 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.

FIGURE 22: VULNERABILITIES IN THE 5 MOST POPULAR BROWSERS



See the Appendix for methodology, including definitions of Secunia Advisories, CVEs and Vulnerabilities; criticality ratings, attack vectors.

FIGURE 23: BROWSER EXPOSURE BY MARKET SHARE AND UNPATCHED USERS

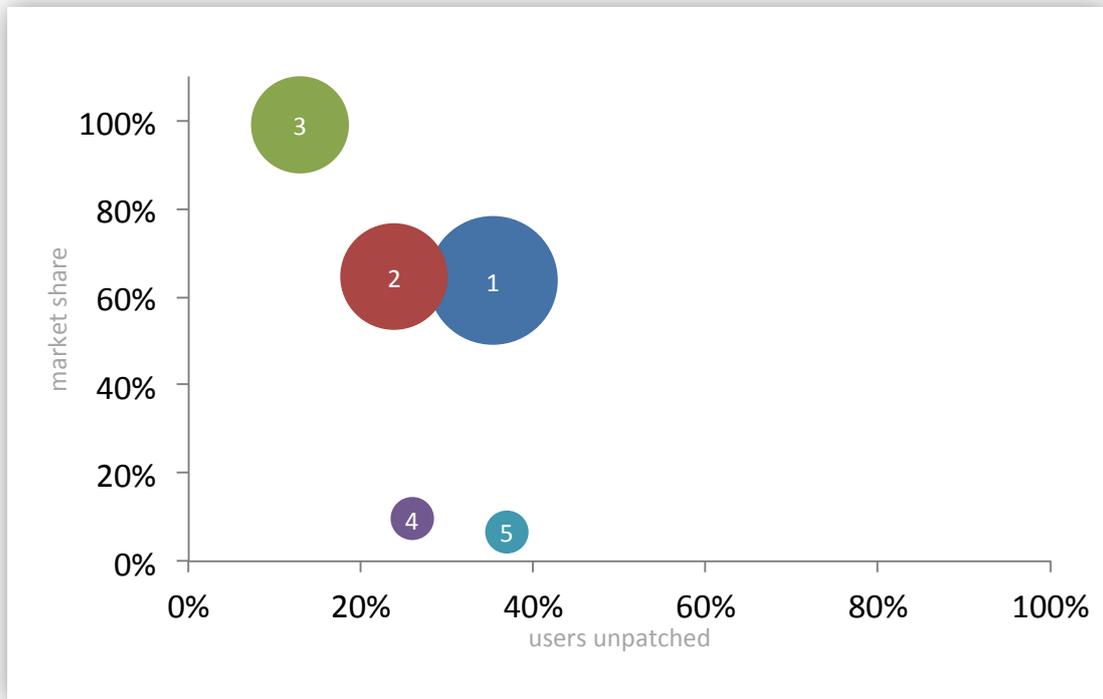
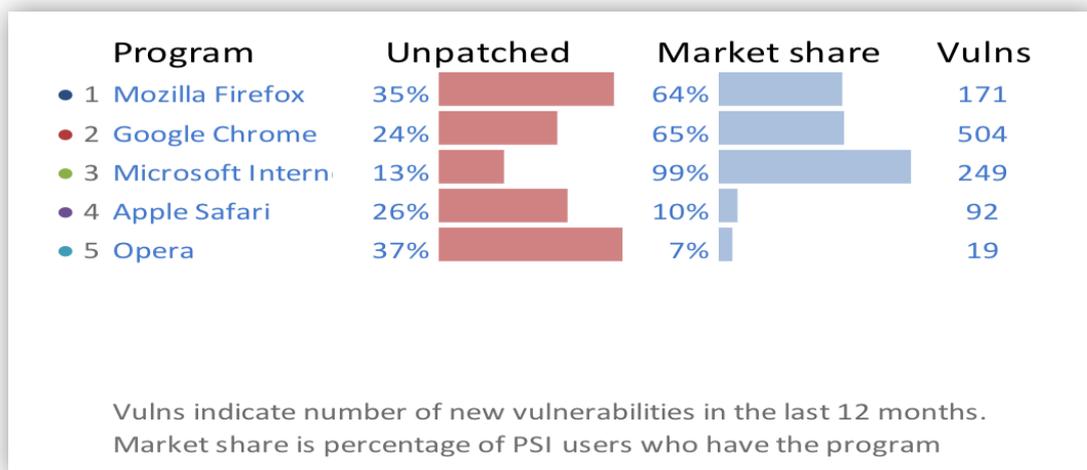


FIGURE 24: VULNERABILITIES IN THE 5 MOST POPULAR BROWSERS



# PDF Readers

This snapshot of the security status of PDF readers outlines the evolution of vulnerabilities relating to the five most popular products (Adobe Reader, Foxit Reader, PDF-XChange Viewer, Sumatra PDF and Nitro PDF Reader). There has been a decrease in the overall number of vulnerabilities in these PDF readers, with 45 vulnerabilities identified in 2014 (70 in 2013). The majority of these vulnerabilities were rated as 'Highly Critical'.

Figure 25 illustrates the distribution of vulnerabilities across the five PDF readers in 2014, including their market share and exposure level, and patch status.

In Figure 26 we have ranked the Top 5 PDF readers, based on risk exposure. We rank them by exposure 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 is available. The position of the bubbles on the axes shows the market share and unpatched level. The size of the bubbles shows the exposure, indicating how exposed a target the software is. 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: 43 in 2013 – with 32% of its users leaving it unpatched despite this fact. While the only other PDF reader with reported vulnerabilities, Foxit Reader, only had 2, more than half of the users – 55% - failed to patch it. Even though the remaining three PDF readers are listed as having 0 vulnerabilities they can be still be labelled 'unpatched' if vulnerable versions from a previous year still have not been patched.

FIGURE 25: PDF READER EXPOSURE BY MARKET SHARE AND UNPATCHED USERS

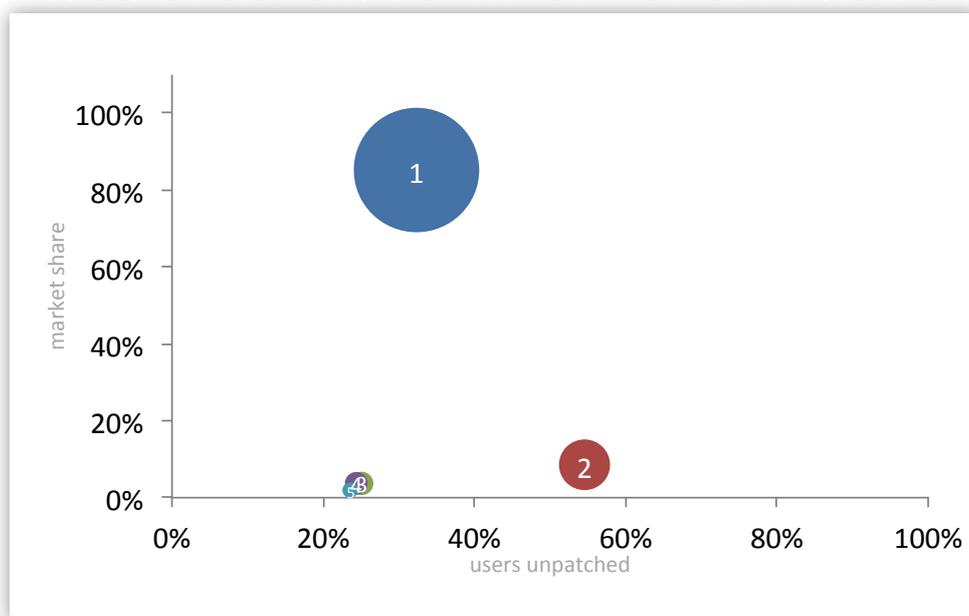


FIG 26: PDF READER MARKET SHARE/UNPATCHED SHARE/NUMBER OF VULNERABILITIES

Program	Unpatched	Market share	Vulns
1 Adobe Reader	32%	85%	43
2 Foxit Reader	55%	8%	2
3 PDF-XChange Viewer	25%	4%	0
4 SumatraPDF	24%	4%	0
5 Nitro PDF Reader	24%	2%	0

See the Appendix for methodology, including definitions of Secunia Advisories, CVEs and Vulnerabilities; criticality ratings, attack vectors.

# Open Source Vulnerabilities in 2014

In 2014, vulnerabilities discovered in a number of open source products brought attention to a previously neglected potential security issue: the use of open source applications and libraries in IT environments. An open source application or library is not in itself a security risk, of course. The risk lies in the fact that the applications and libraries can be bundled in a variety of products, and installed in a host of different contexts.

With the Heartbleed vulnerability, and the three subsequent security releases for the open source library OpenSSL, the extent to which shared code complicates security became apparent. Heartbleed highlighted just how many products use Open SSL. It caught vendors by surprise as the majority – large and small – first had to identify which of their products had been made vulnerable before they could begin to issue fixes.

In the following months, Open SSL released three new sets of security patches. As OpenSSL vulnerabilities were disclosed a second, third and fourth time, we expected vendors to be much better prepared. After Heartbleed, they should have their security pages ready and know precisely which products and versions would be affected. This in return should have improved their response times.

We expected vendors to react more quickly in both disclosing which of their products were made vulnerable

by the latest OpenSSL vulnerability, and issuing security patches to fix it.

That was not what happened. When we look at the number of days lapsed between the time when OpenSSL vulnerabilities were disclosed, until third-party vendors informed of their product being vulnerable, we find that there is no general pattern of improvement.

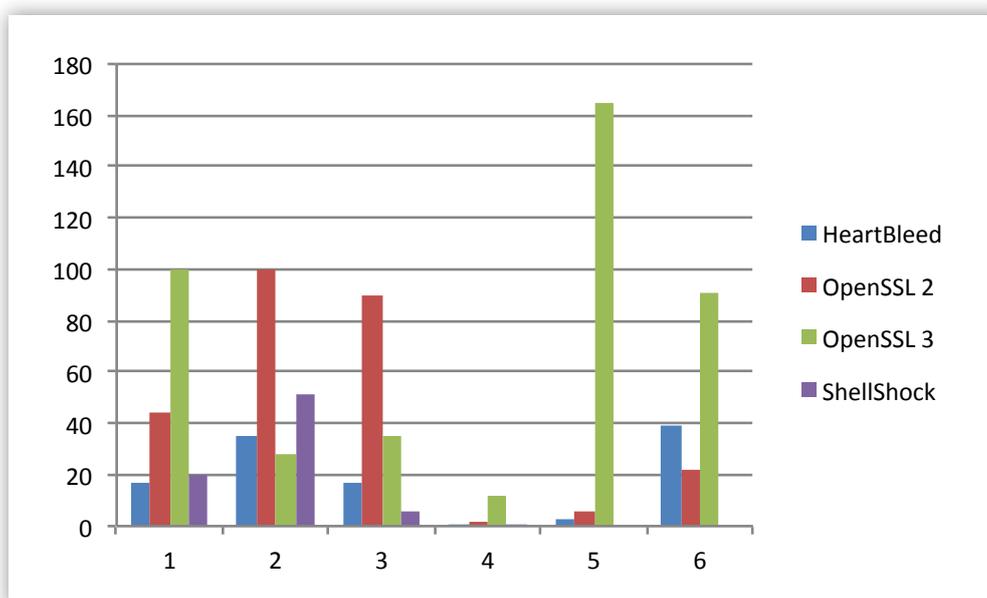
Figure 27 shows the response times for six different vendors – all of them major, global software vendors catering to businesses. We have anonymized the data, because the point is not to call out specific vendors but rather draw attention to the fact that response times are random: The six column groups illustrate that the same vendor may be quick to respond to one vulnerability but slow on the next.

If we can deduce anything from the data, it is that organizations should not presume to be able to predict which vendors are dependable and quick to react, when vulnerabilities are discovered in products bundled with open source libraries.

It is therefore important to be aware of which open source libraries are in use in an environment, and to have a solid mitigation strategy in place. Because the applications that use these libraries are not always patched – often, they are not even reported vulnerable.

FIGURE 27: DAYS LAPSED BETWEEN PATCH RELEASED FOR OPENSLL/SHELLSHOCK VULNERABILITY TO PRODUCT VULNERABILITY DISCLOSED BY SIX MAJOR THIRD-PARTY VENDORS.

NOTE: VENDORS 4, 5 AND 6 HAVE NOT REPORTED ANY PRODUCTS VULNERABLE TO SHELLSHOCK



See the Appendix for methodology, including definitions of Secunia Advisories, CVEs and Vulnerabilities; criticality ratings, attack vectors.

# Appendix & Glossary

# Appendix

## Secunia Software 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

#### **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 applications 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.

## Unique and Shared vulnerabilities

### Unique 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 categorized as shared vulnerabilities for both vendor A and vendor B.

### Total vulnerabilities

The total number of vulnerabilities found in the products of the vendor; be it unique 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 applications 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 applications 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 20 core products with the most vulnerabilities in 2014

These are the 20 core products with the most vulnerabilities in 2014 out of the more than 50,000 systems and applications tracked by Secunia Research, and recorded in the Secunia Vulnerability Database. All major versions of the same product are counted as one single application.

RANK	PRODUCT	VULNERABILITIES
1	GOOGLE CHROME	504
2	ORACLE SOLARIS	483
3	GENTOO LINUX	350
4	MICROSOFT INTERNET EXPLORER	289
5	AVANT BROWSER	259
6	IBMTIVOLI ENDPOINT MANAGER	258
7	IBMTIVOLI STORAGE PRODUCTIVITY CENTER	231
8	IBM WEBSHERE APPLICATION SERVER	210
9	IBM DOMINO	177
10	IBM NOTES	174
11	MOZILLA FIREFOX	171
12	X.ORG XSERVER	152
13	APPLE MACINTOSH OS X	147
14	IBMTIVOLI COMPOSITE APPLICATION MANAGER FOR TRANSACTIONS	136
15	VMWARE VCENTER SERVER	124
16	IBMTIVOLI APPLICATION DEPENDENCY DISCOVERY MANAGER	122
17	ORACLE JAVA	119
18	VMWARE VSPHERE UPDATE MANAGER	111
19	IBM WEBSHERE PORTAL	107
20	MICROSOFT WINDOWS 8	105

## The Top 50 Software Portfolio

The following table lists the applications in the Top 50 software portfolio together with the type of program (MS Microsoft, NMS non-Microsoft), market share as of December 2014 and the number of vulnerabilities affecting the program in 2013 and 2014. The ranking and market share is derived from anonymous scans of the Secunia PSI throughout 2014. 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 (#7) and Adobe AIR (#29) share code components and thereby also share numerous vulnerabilities.

RANK	TYPE	PRODUCT	SHARE	ADVS	VULNS
1	MS	MICROSOFT WINDOWS SCRIPT CONTROL	99,9%	0	0
2	MS	MICROSOFT XML CORE SERVICES (MSXML)	99,9%	3	3
3	MS	MICROSOFT .NET FRAMEWORK	99,5%	5	8
4	MS	MICROSOFT WINDOWS MEDIA PLAYER	99,3%	0	0
5	MS	MICROSOFT INTERNET EXPLORER	99,1%	13	289
6	MS	MICROSOFT VISUAL C++ REDISTRIBUTABLE	96,1%	0	0
7	NMS	ADOBE FLASH PLAYER	96,1%	20	99
8	MS	MICROSOFT SILVERLIGHT	85,6%	0	0
9	NMS	ADOBE READER	85,3%	5	43
10	MS	MICROSOFT WINDOWS DEFENDER	81,0%	1	1
11	NMS	ORACLE JAVA JRE	79,1%	4	119
12	MS	WINDOWS POWERSHELL	76,1%	0	0
13	MS	WINDOWS DVD MAKER	75,5%	0	0
14	MS	MICROSOFT WORD	75,1%	6	13
15	MS	MICROSOFT EXCEL	74,3%	1	2
16	MS	MICROSOFT POWERPOINT	72,4%	0	0
17	MS	MICROSOFT XPS-VIEWER	69,8%	0	0
18	NMS	GOOGLE CHROME	65,6%	23	504
19	MS	WINDOWS MEDIA CENTER	65,2%	0	0
20	NMS	MOZILLA FIREFOX	64,5%	18	171
21	MS	MICROSOFT VISIO VIEWER	59,4%	0	0
22	MS	DRIVER PACKAGE INSTALLER (DPINST)	58,5%	0	0
23	MS	MICROSOFT SQL SERVER	57,3%	1	2
24	MS	MICROSOFT OUTLOOK	56,5%	0	0
25	NMS	REALTEK AC 97 UPDATE AND REMOVE DRIVER TOOL	54,6%	0	0
26	MS	COMDLG32 ACTIVEX CONTROL	54,0%	0	0
27	MS	MICROSOFT PUBLISHER	52,6%	1	1
28	MS	MICROSOFT ACCESS	52,2%	0	0
29	NMS	ADOBE AIR	50,8%	10	59
30	MS	MSCOMCT2 ACTIVEX CONTROL	50,3%	0	0
31	NMS	APPLE QUICKTIME	49,6%	2	14
32	NMS	MOZILLA MAINTENANCE SERVICE	49,2%	0	0

33	NMS	CCLEANER	48,9%	0	0
34	MS	WINDOWS LIVE MAIL	48,9%	0	0
35	MS	WINDOWS LIVE MOVIE MAKER	46,8%	0	0
36	NMS	APPLE BONJOUR FOR WINDOWS	46,6%	0	0
37	MS	WINDOWS LIVE WRITER	46,5%	0	0
38	NMS	REALTEK VOICE MANAGER	45,8%	0	0
39	MS	WINDOWS LIVE MESSENGER	43,8%	0	0
40	MS	MICROSOFT POWERPOINT VIEWER	43,5%	0	0
41	NMS	APPLE ITUNES	43,5%	2	84
42	MS	SKYPE	42,8%	0	0
43	MS	WINDOWS LIVE PHOTO GALLERY	41,5%	0	0
44	NMS	VLC MEDIA PLAYER	40,6%	2	2
45	MS	WINDOWS LIVE ESSENTIALS	39,0%	0	0
46	NMS	GOOGLE EARTH	38,0%	0	0
47	NMS	INSTALLSHIELD UPDATE SERVICE	34,8%	0	0
48	MS	MICROSOFT OFFICE PICTURE MANAGER	33,3%	0	0
49	MS	MICROSOFT POWERSHELL	32,9%	0	0
50	MS	MICROSOFT OFFICE TEMPLATE AND MEDIA CONTROL ACTIVEX CONTROL	32,2%	0	0
OS	MS	MICROSOFT WINDOWS 7	N/A	27	33

## Glossary

### Vulnerability

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

### Zero-day vulnerability

A zero-day vulnerability is a vulnerability that is actively exploited by hackers before it is publicly known.

### Exploit

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

For further information,  
please visit

Secunia  
Mikado House  
Rued Langgaards Vej 8  
DK-2300 Copenhagen S  
Denmark

[secunia.com](http://secunia.com)

Email: [info@secunia.com](mailto:info@secunia.com)  
Phone: +45 7020 5144  
Fax: +45 7020 5145

**Copyright 2015 Secunia. All rights reserved.**

This report may only be redistributed unedited and unaltered.

This report may be cited and referenced only if clearly crediting Secunia and this report as the source. Any other reproduction and redistribution in print or electronically is strictly prohibited without explicit permission