FLEXERA SOFTWARE

VULNERABILITY REVIEW 2016

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

Published March 16, 2016

Index

Introduction 3

Global Trends – All Products 4

Global Trends – Top 50 Portfolio 4

Vendor Update – Top 50 Portfolio 12

Time-to-Patch – All Products 17

Time-to-Patch – Top 50 Portfolio 17

Zero-day Vulnerabilities 19

Browser Security 20

PDF Reader Security 22

Appendix

Secunia Research Software Vulnerability Tracking Process 25

Attack Vector 26

Unique and Shared Vulnerabilities 26

Secunia Research Vulnerability Criticality Classification 27

The Top 50 Software Portfolio 28

Glossary 29

Introduction to the Vulnerability Review 2016

The annual Vulnerability Review analyzes the evolution of software security from a vulnerability perspective.

The review presents global data on the prevalence of vulnerabilities and the availability of patches, maps the security threats to IT infrastructures, and also explores vulnerabilities in the 50 most popular applications on private PCs.

What does the Vulnerability Review cover?

The annual Vulnerability Review is based on data from Secunia Research at Flexera Software.

Secunia Research monitors more than 50,000 applications, appliances and operating systems, and tests and verifies the vulnerabilities reported in them.

The systems and applications monitored by Secunia Research are those in use in the environments of the customers of Flexera Software's Software Vulnerability Management product line.

In the event of customers using products that are not already being monitored by Secunia Research, these products can be submitted to Secunia Research who will initiate monitoring within three business days. Secunia Research only monitors public or commercially available solutions.

The Vulnerability Database covers vulnerabilities that can be exploited in all types of products – software, hardware, firmware, etc.

The vulnerabilities verified by Secunia Research are described in Secunia Advisories and listed in the Secunia Vulnerability Database, detailing what IT Security teams need to know to mitigate the risk posed by the vulnerability in their environment. The Secunia Advisory descriptions include criticality, attack vector and solution status.

How do we count vulnerabilities?

Different approaches to counting vulnerabilities are adopted by research houses in the vulnerability management space.
Secunia Research counts vulnerabilities per product the vulnerability appears in. We apply this method to reflect the level of information our customers need, to keep their environments secure, i.e. verified intelligence on all products affected by a given vulnerability.

Vulnerability Update

Numbers - All Products

Number of Vulnerabilities - All products
The absolute number of vulnerabilities detected was 16,081, discovered in 2,484 applications from 263 vendors. The number shows a 39% increase in the five year trend, and a 2% increase from 2014 to 2015.

Since 2014, the number of vendors behind the vulnerable products has decreased by 49% and the amount of vulnerable products has decreased by 36%.

The substantial drop in numbers of Vendors and Products for 2015 is occasioned by Secunia Research's decision to focus on the products and vendors present in the environments of Flexera Software's Software Vulnerability Management customers.
As a result, a number of products and vendors not used in customer environments are no longer tracked systematically.

Criticality – All Products
13.3% of vulnerabilities in 2015 were rated as 'Highly Critical', and 0.5% as 'Extremely Critical'.

The most notable changes in criticality levels occurred in the 'Extremely' critical bracket, with an increase from 0.3% in 2014 to 0.5% in 2015.

Attack Vector – All Products
With a 57.0% 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 60.2% the year before.

Local network has increased correspondingly, from 33.4% in 2014, to 35.5% in 2015. In 2012, local network only represented 15%. Local system remained stable, from 6.4% in 2014, to 7.5% in 2015.

Global Trends – Top 50 Portfolio (2)

Number of Vulnerabilities - Top 50 Portfolio
The number of vulnerabilities in the Top 50 portfolio was 2,048, discovered in 25 products from seven vendors plus the most used operating system, Microsoft Windows 7.
The number shows a 77% increase in the five year trend, and a 47% increase from 2014 to 2015.

Criticality – Top 50 Portfolio
The combined number of 'Highly Critical' and 'Extremely Critical' vulnerabilities: 71.4% represented the majority of vulnerabilities in the Top 50 rated by Secunia Research in 2015.

Attack Vector – Top 50 Portfolio
With an 81.7% share, the foremost attack vector available to attackers to trigger a vulnerability in the Top 50 portfolio was Remote Network. This, however, is a decrease compared to 2014.

Local Network saw an increase, from 2.2% in 2014, to 3.4% in 2015. Local System recorded an increase compared to last year, from 6%, to 14.9% in 2015.

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

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

What is the Top 50 Portfolio? (2)

To assess how exposed endpoints are, we analyze the types of products typically found on an endpoint. Throughout 2015, anonymous data has been gathered from scans of the millions of private computers which have the Flexera Software Personal Software Inspector installed.

Secunia Research data shows that the computer of a typical Personal Software Inspector user has an average of 79 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 2015. These 50 applications are comprised of 33 Microsoft applications and 17 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 Personal Software Inspector installed.

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

Operating Systems: We track vulnerabilities in Windows operating systems: Windows Vista, Windows 7, Windows 8 and Windows 10.

Product composition, Top 50 portfolio

Microsoft applications: Represent 67% of the Top 50 applications on a computer with Personal Software Inspector installed.

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

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

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

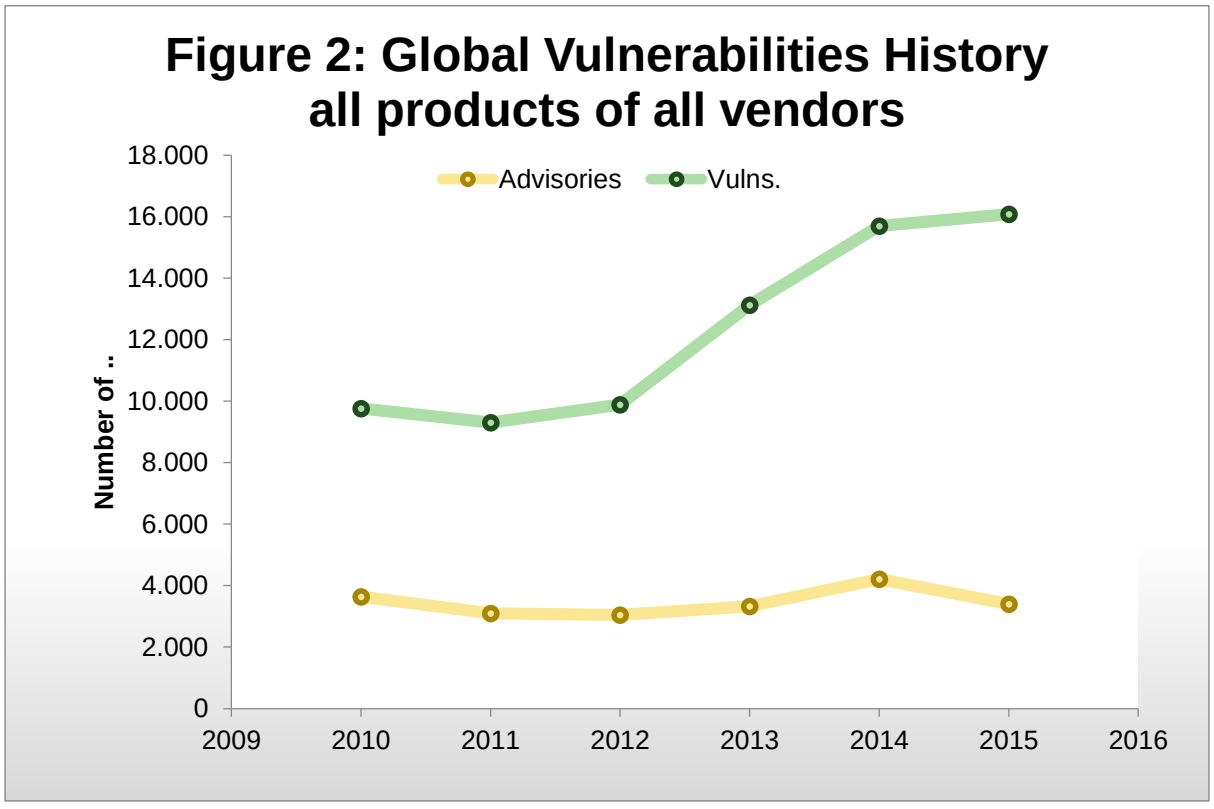
See the Appendix for methodology, including definitions of Secunia Advisories, CVEs and Vulnerabilities; criticality ratings, attack vectors.

FIGURE 1: SECUNIA ADVISORIES/VULNERABILITIES IN ALL PRODUCTS

	Secunia Advisories	Vulnerability count	Vendors	Products*
Average 2010-14	3,466	11,556	634	3,334
Total 2015	3,403	16,081	263	2,484
Trend 5 yr	-2%	39%	-59%	-25%
Trend 2014/15	-19%	2%	-49%	-36%

* : 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



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

FIGURE 3: VULNERABLE PRODUCTS AND VENDORS, ALL PRODUCTS

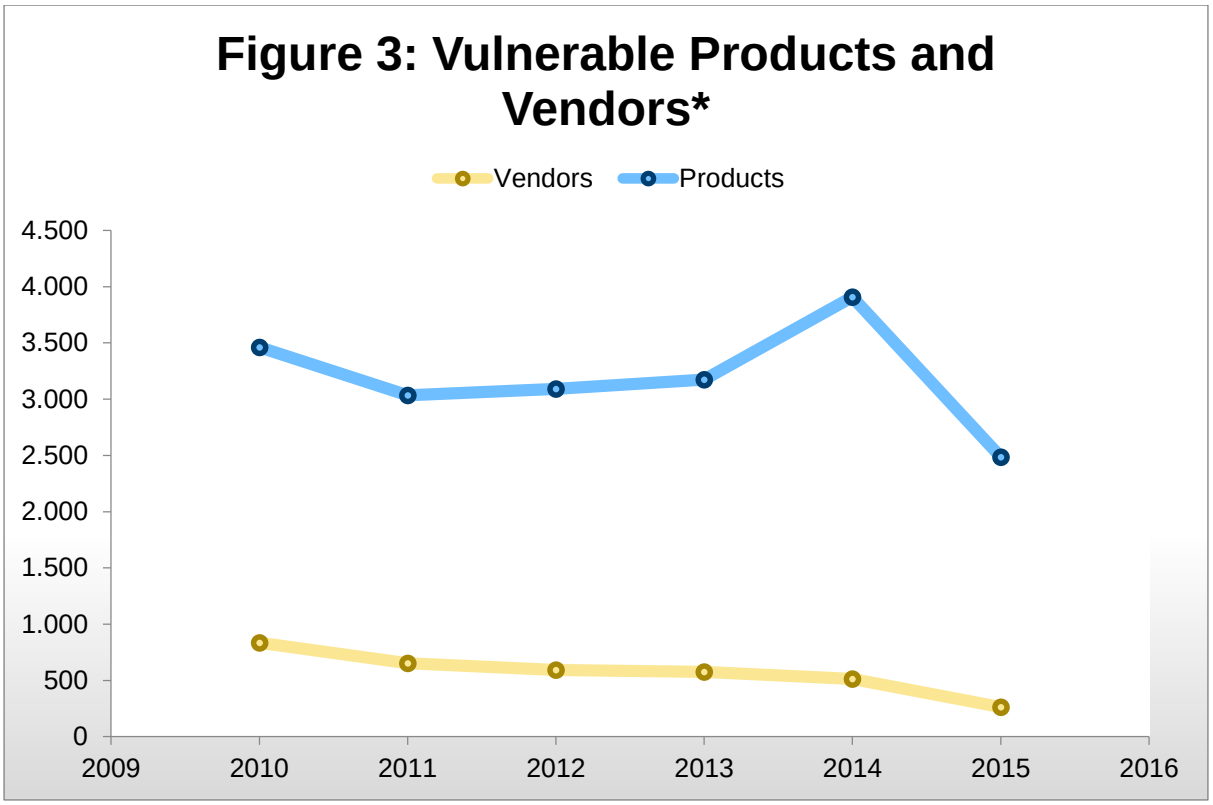
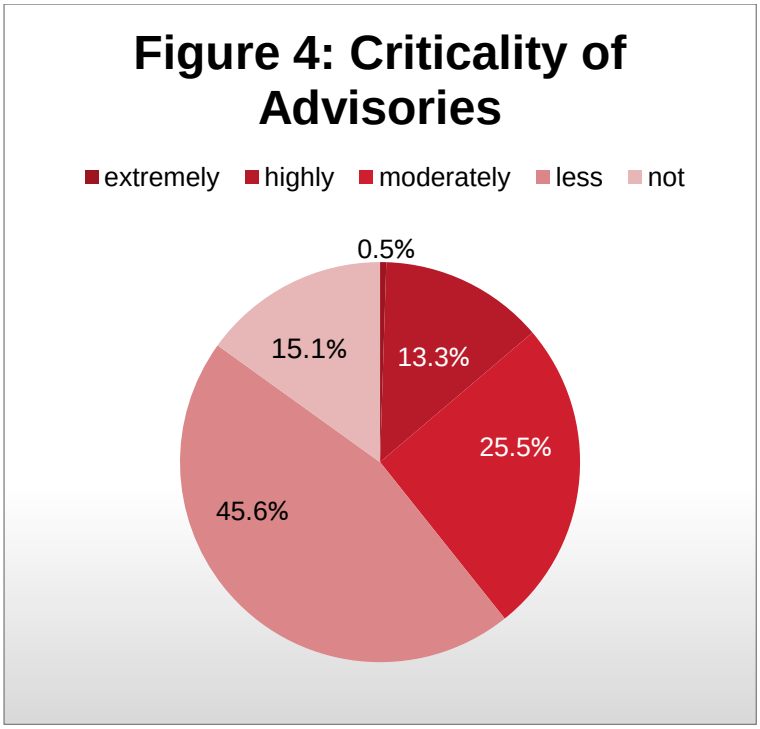


FIGURE 4: CRITICALITY, ALL PRODUCTS



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

FIGURE 5: ATTACK VECTORS, ALL PRODUCTS

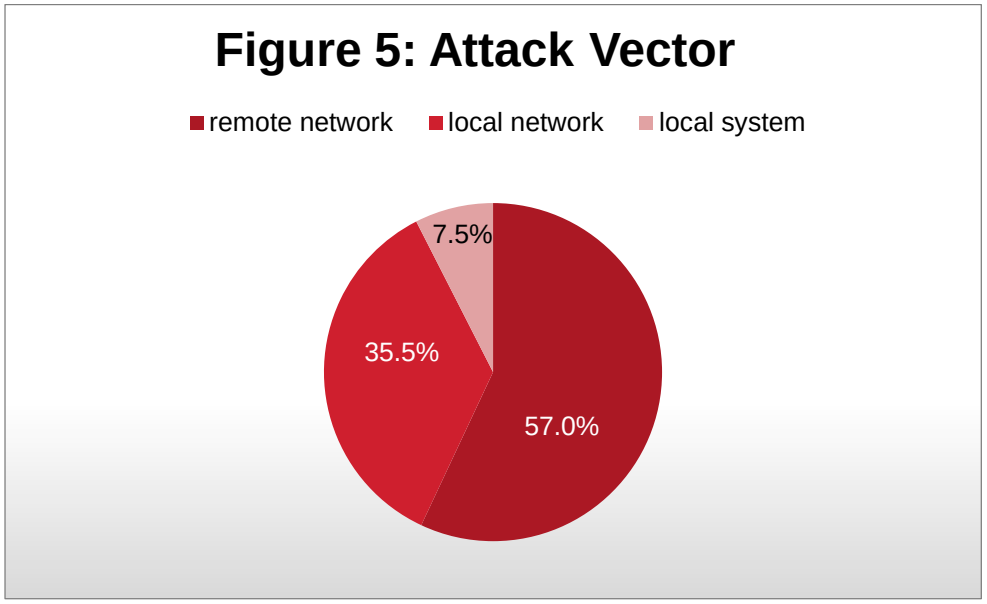
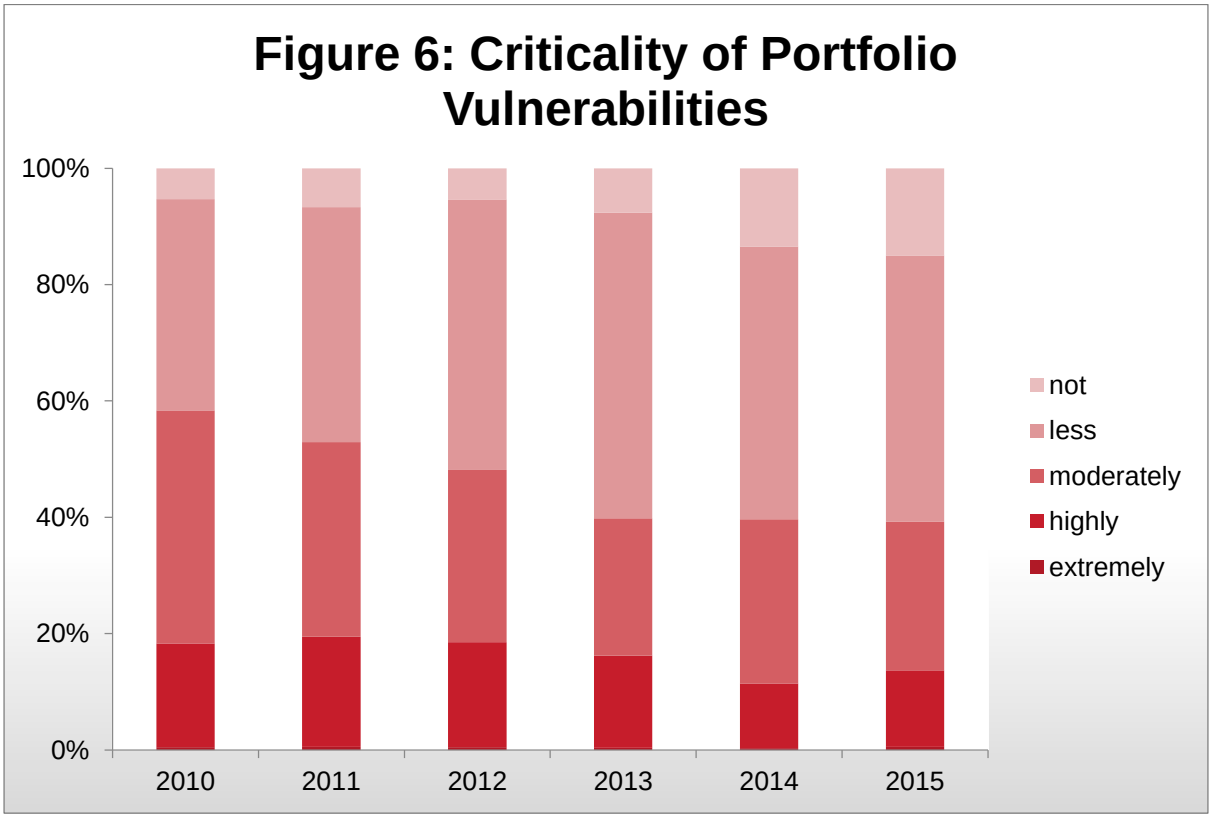


FIGURE 6: CRITICALITY OF VULNERABILITIES IN ALL PRODUCTS, HISTORICALLY



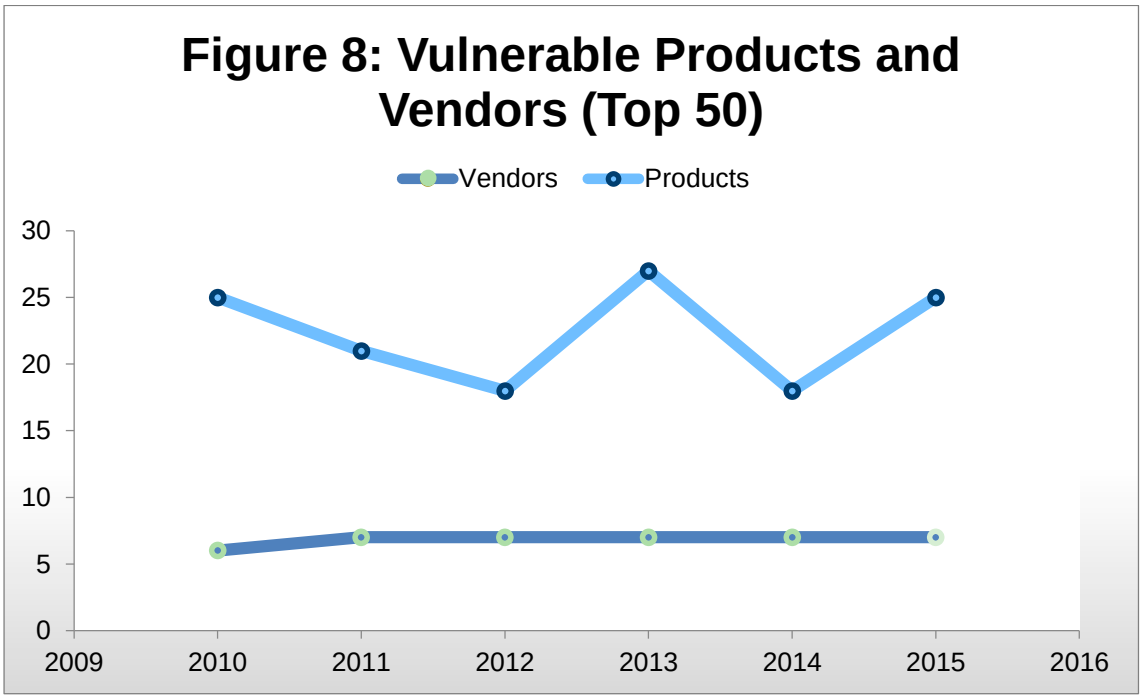
See the Appendix for methodology, including definitions of Secunia Advisories, CVEs and Vulnerabilities; criticality ratings, attack vectors.

FIGURE 7: SECUNIA ADVISORIES/VULNERABILITIES IN TOP 50

	Secunia Advisories	Vulnerability count	Vendors	Products
Average 2010-14	141	1,155	7	22
Total 2015	175	2,048	7	25
Trend 5 yr	24%	77%	3%	15%
Trend 2014/15	31%	47%	0%	39%

* 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



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

FIGURE 9: SECUNIA ADVISORIES/VULNERABILITIES IN TOP 50 PRODUCTS

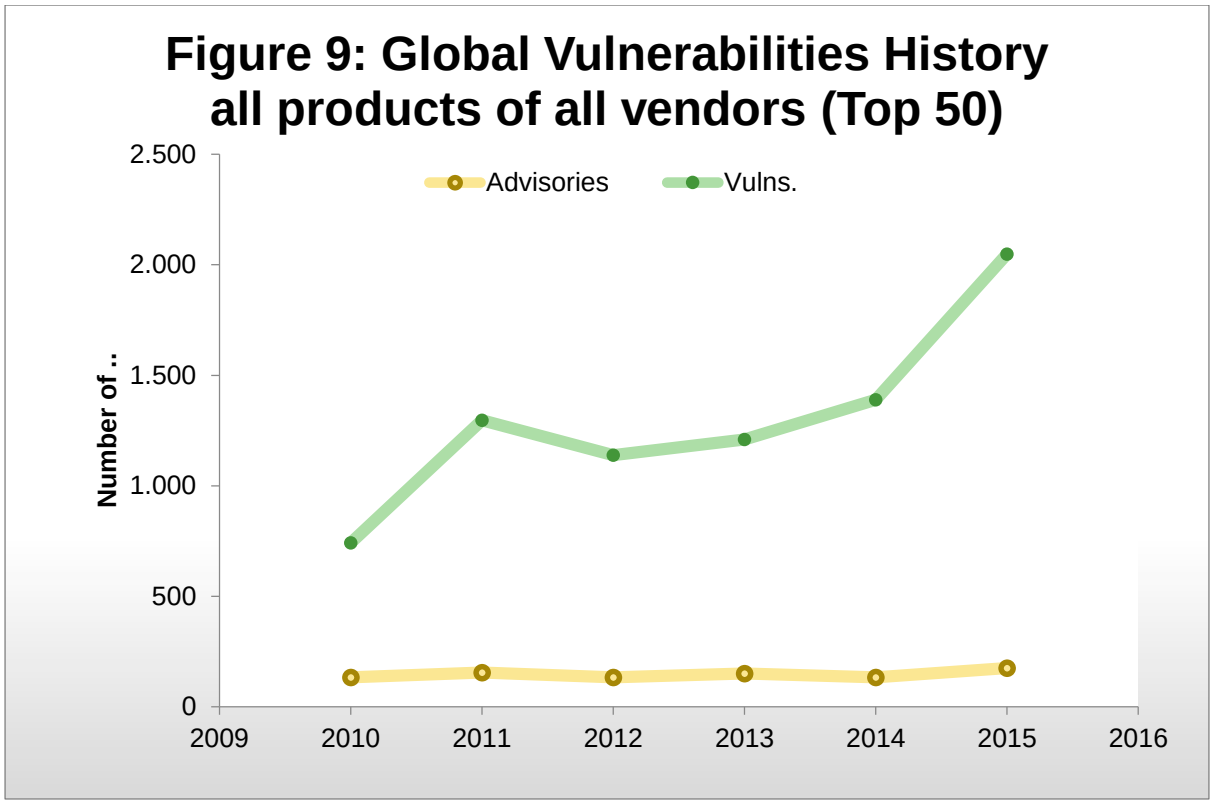
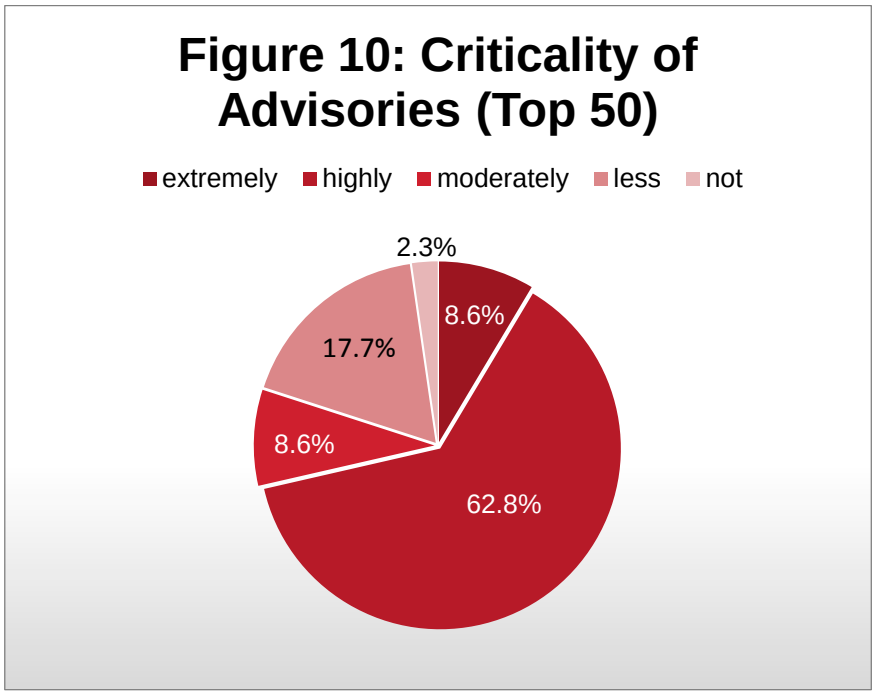
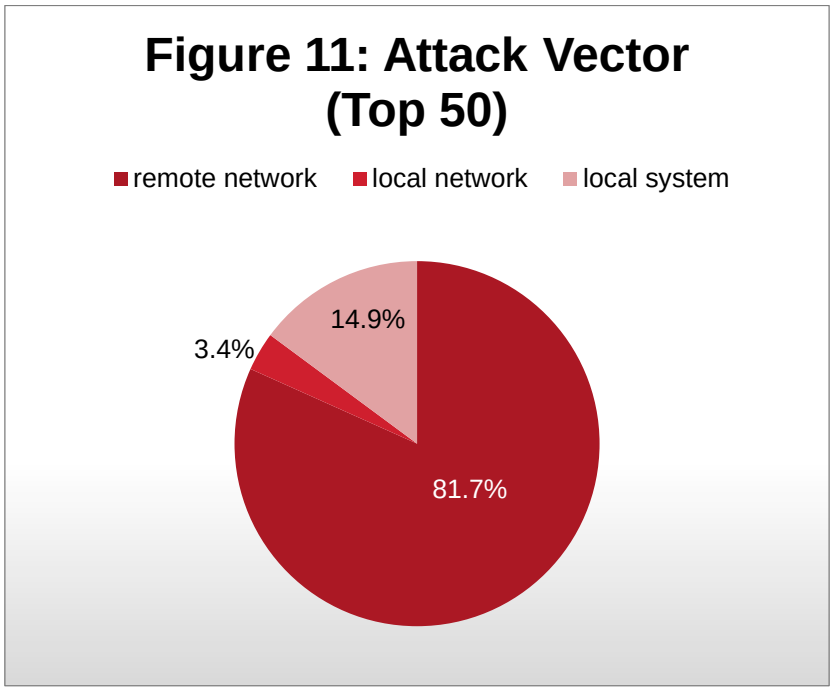


FIGURE 10: CRITICALITY, TOP 50



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

FIGURE 11: ATTACK VECTORS, TOP 50



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

Vendor Update – Top 50 Portfolio(2)

Different vendors have different security update mechanisms. Microsoft applications, which account for 67% of the applications (including Windows 7 OS) in the Top 50 portfolio, are updated automatically.
But Microsoft applications (including Windows 7 OS) are only responsible for 21% of the vulnerabilities discovered in the Top 50 portfolio. Therefore, the non-Microsoft applications in your system - your corporate environment or your private PC – play a significant role your security efforts.

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 2015, 79% of the vulnerabilities affecting the Top 50 applications in the representative software portfolio affected non-Microsoft applications. This means that 21% of the remaining vulnerabilities in the Top 50 applications installed on the computers of Personal Software Inspector users stem from the Windows 7 operating system (7%) and Microsoft applications (14%).

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 21% – a fifth – 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.

Microsoft applications
There was a lesser share of vulnerabilities reported in Microsoft applications (excluding Windows7) in 2015 compared to the previous year: down from 23.0% to 14.3%. The vulnerability count in Microsoft *applications* was 296 in 2015; in 2014 it was 320.

Operating systems
The choice of operating system had an impact on the total number of vulnerabilities on a typical endpoint: In 2015, 7% of vulnerabilities in the Top 50 portfolio were reported in Windows 7, the operating system we are tracking with the Top 50 portfolio.

Increase in vulnerabilities in Windows
Data shows an increase in in the number of vulnerabilities recorded in all Windows operating systems:

- Windows 10[1] which was released in 2015, had 256 vulnerabilities.
- Windows 8[2] went from 105 in 2014, to 466 in 2015.
- Windows 7 went from 33 in 2014, to 144 in 2015.
- Windows Vista went from 30 in 2014, to 146 in 2015.
- Windows XP went End of Life in April 2014, and therefore new vulnerabilities in the OS are not recorded. Secunia Research data indicates that globally, 11.8% of end users were still using Windows XP in December 2015.

The increase in vulnerabilities in Windows operating systems brings the numbers up to levels similar to the years preceding 2014.

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

(1) Windows 8 and Windows 10 are bundled with Adobe Flash, adding Flash's to the number of vulnerabilities reported in Windows 8 and upwards.

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

FIGURE 12: VULNERABILITIES IN TOP 50 PORTFOLIO, HISTORICALLY

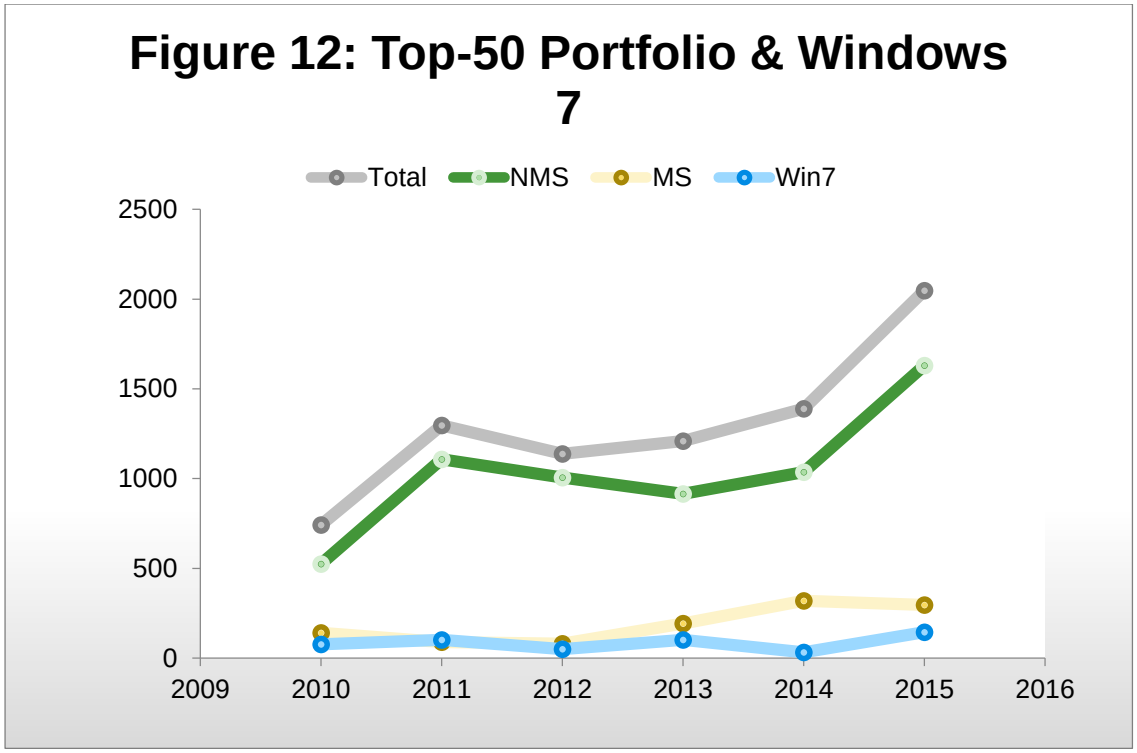
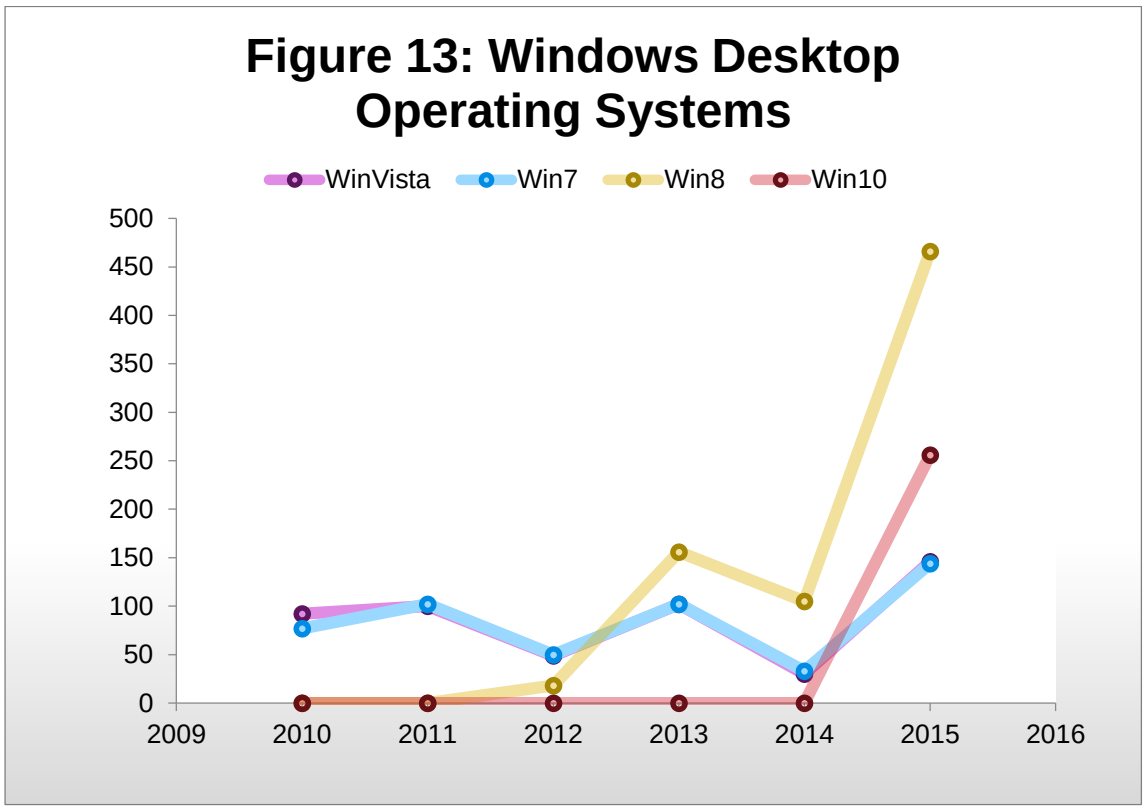


FIGURE 13: VULNERABILITIES IN WINDOWS OPERATING SYSTEMS, HISTORICALLY



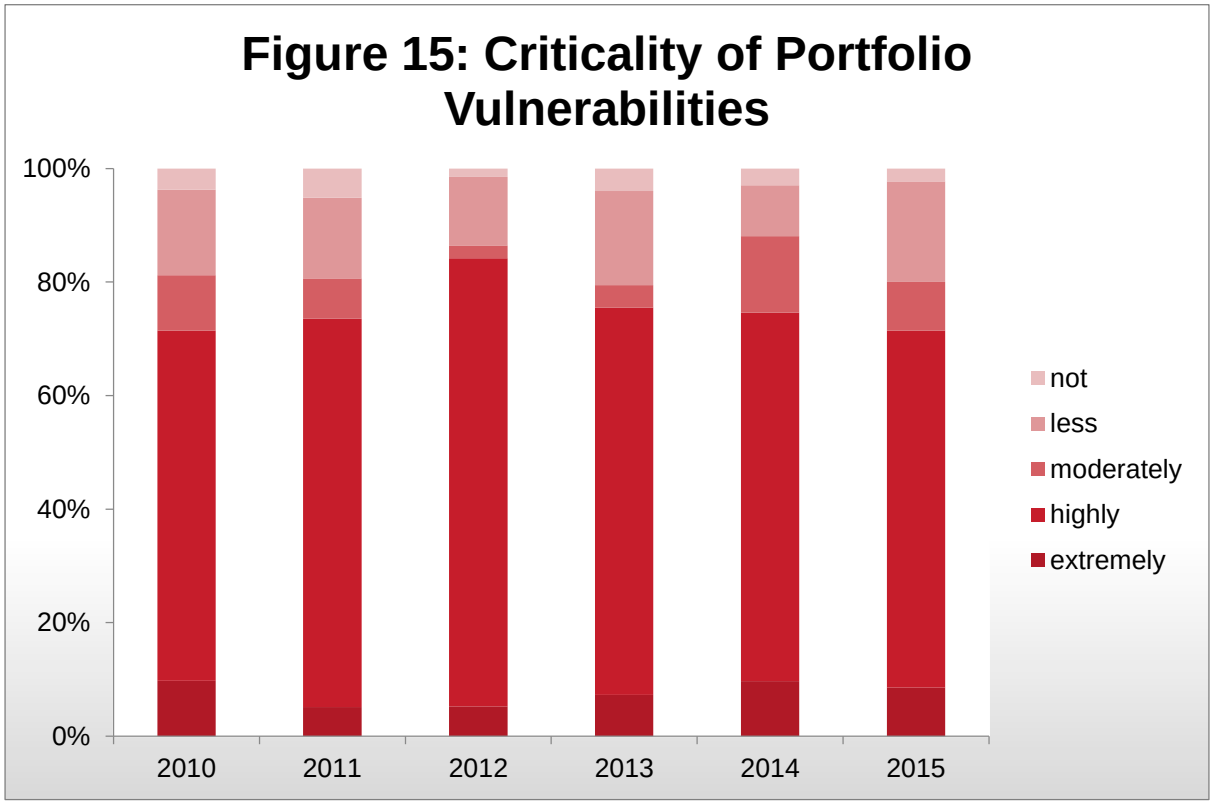
See the Appendix for methodology, including definitions of Secunia Advisories, CVEs and Vulnerabilities; criticality ratings, attack vectors.

FIGURE 14: VULNERABILITIES IN TOP 50 IN 2014

Breakdown of end-point vulnerabilities in 2015				
	WinVista	Win7	Win8*	Win10*
Operating System	146	144	466	256
Microsoft Programs	296	296	296	296
Non-Microsoft Programs	1,630	1,630	1,630	1,630
Total	**2,051**	**2,048**	**2,372**	**2,165**

*: Windows 8 and Windows 10 are bundled with Adobe Flash, adding Flash's to the number of vulnerabilities reported in Windows 8 and upwards.

FIGURE 15: CRITICALITY OF VULNERABILITIES IN TOP 50, HISTORICALLY



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

FIGURE 16: SHARE BY SOURCE, TOP 50

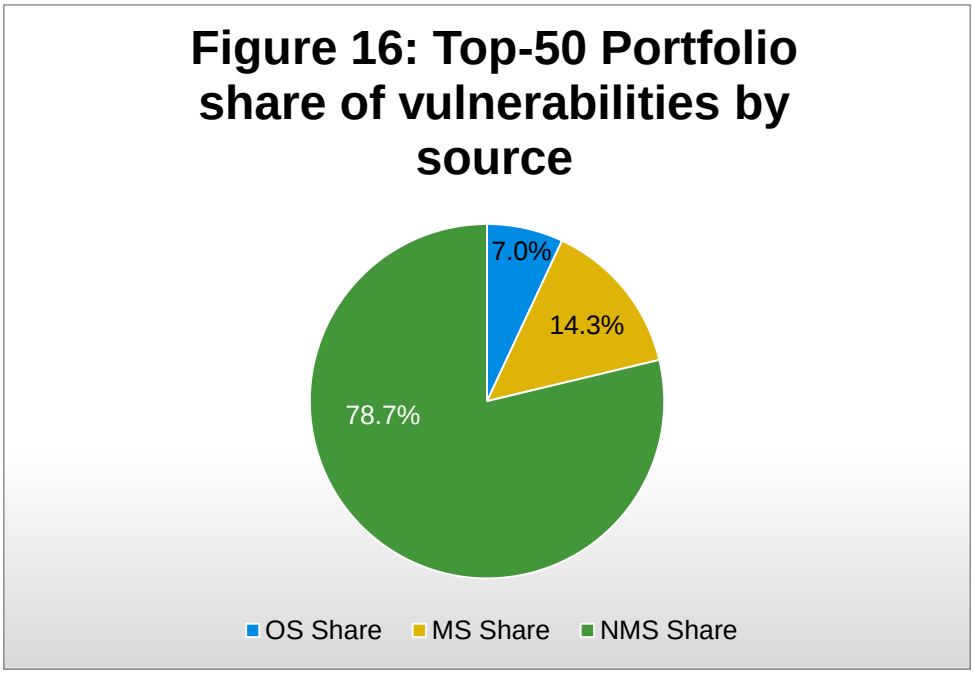
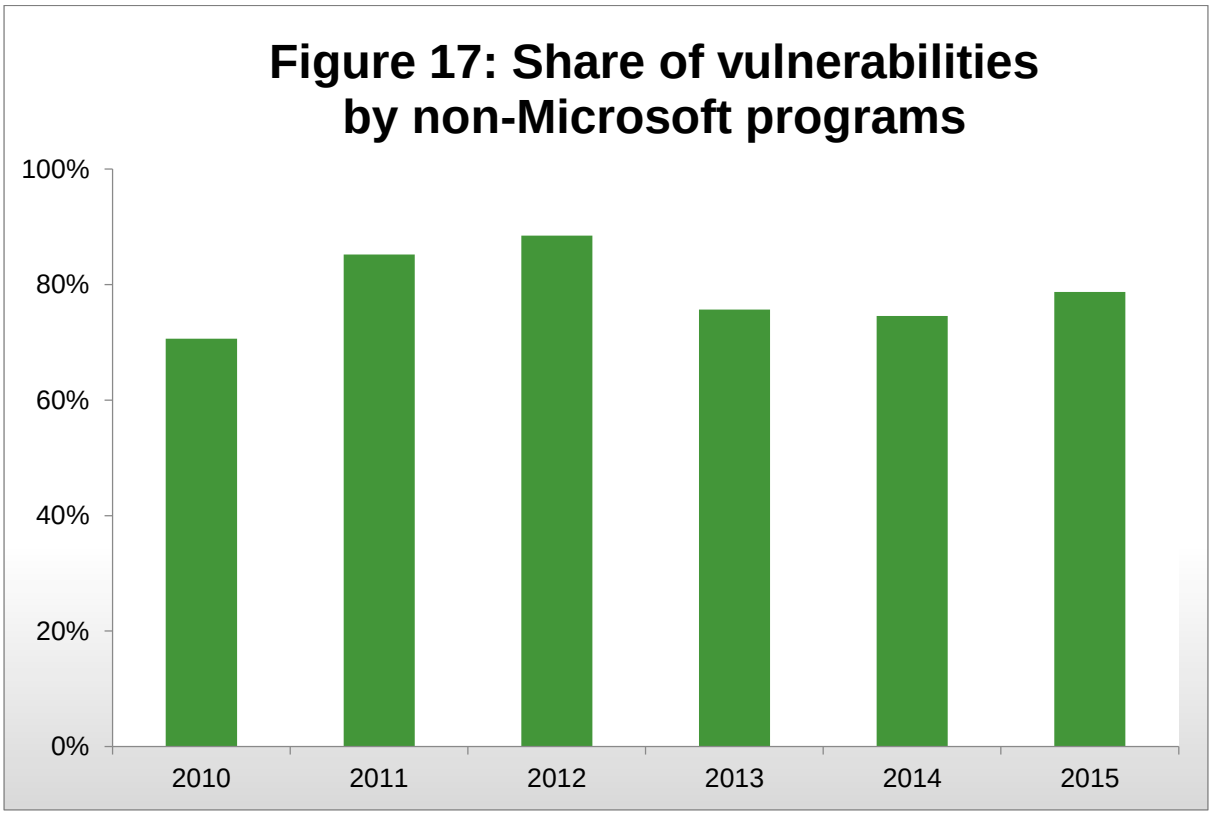
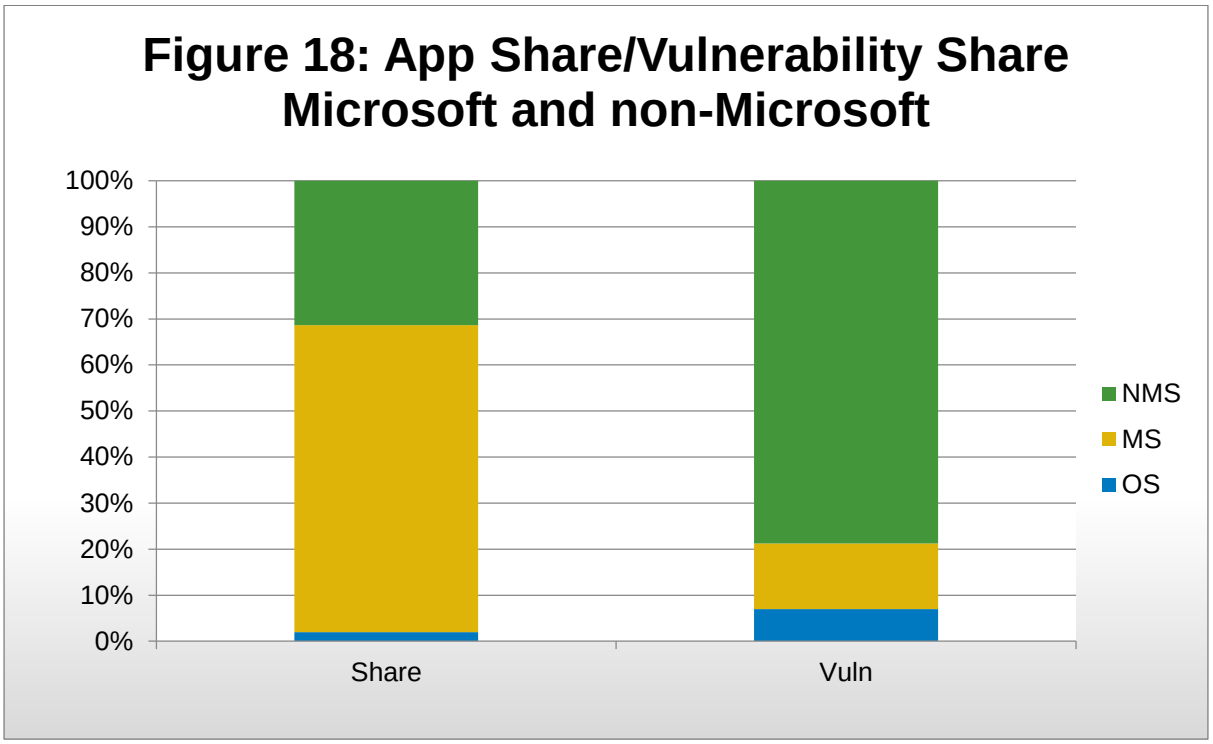


FIGURE 17: SHARE OF NON-MICROSOFT VULNERABILITIES IN TOP 50, HISTORICALLY



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

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[(2)]

In 2015, 83.6% of all vulnerabilities had a patch available on the day of disclosure - on a par with the 82.8% in 2014.*

In the Top 50 applications, 84.6% of vulnerabilities had a patch available on the day of disclosure. This number is slightly lower compared to the 86.6% time-to-patch rate that was recorded in 2014.*

The 2015 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 2015 time-to-patch results show that one sixth of vulnerabilities (16.4% of all vulnerabilities / 15.4% in the Top 50 portfolio) 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 83.6% of vulnerabilities in 'All' products, and 84.6% 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 2010 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, 84.7% 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.

---

2 *The Time-to-Patch numbers released from 2014 onwards are not directly compatible with the numbers released in previous years. We have applied a different method from 2014 because an increasing number of vendors, particularly browser vendors, started to upgrade to new major versions, rather than patch existing versions*

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

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

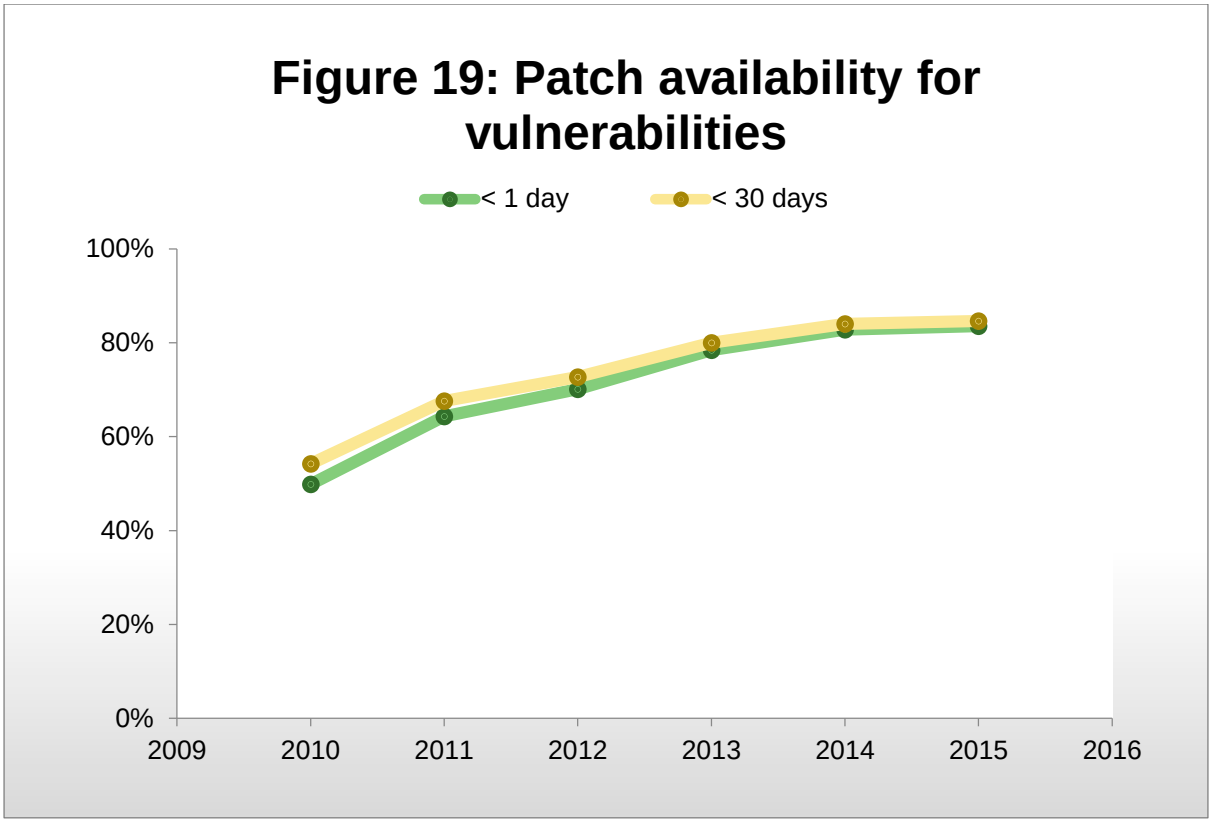
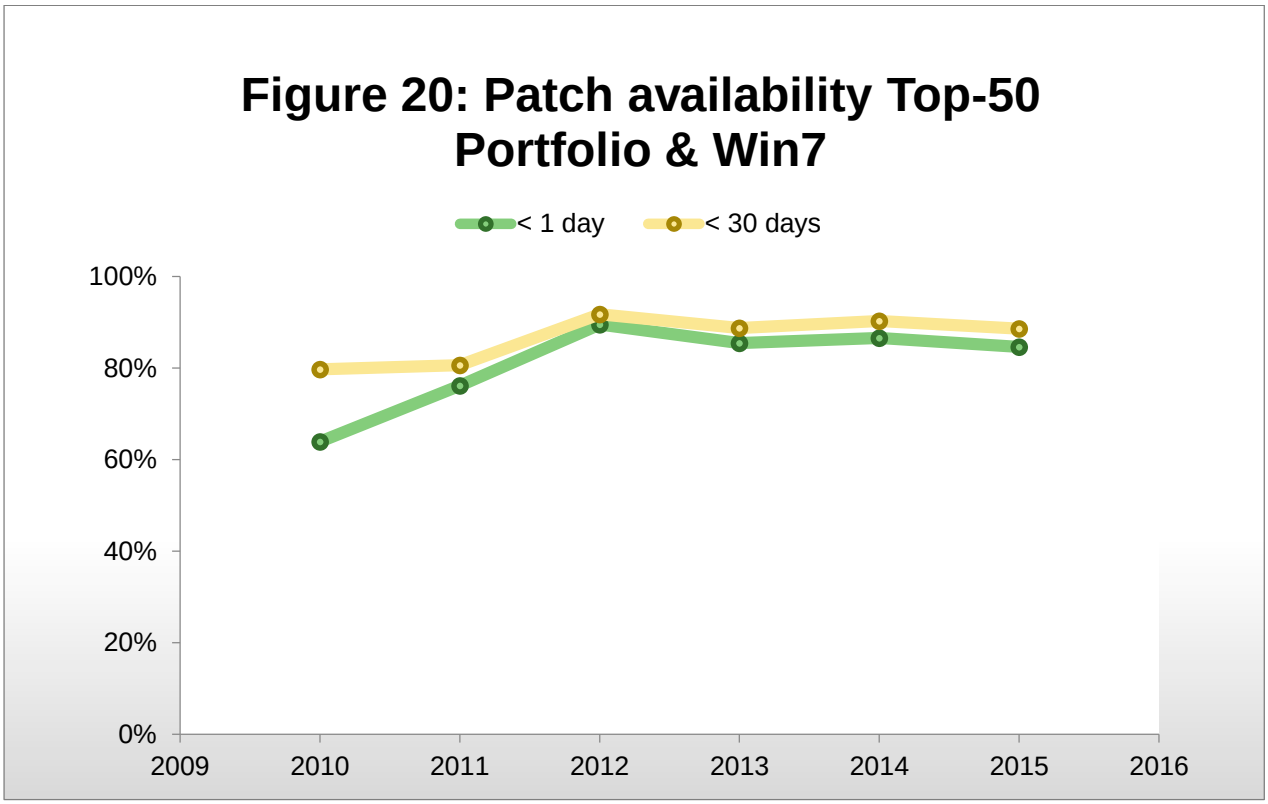


FIGURE 20: PATCH AVAILABILITY FOR VULNERABILITIES IN TOP 50 PRODUCTS, HISTORICALLY



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

Zero-Day Vulnerabilities

The number of zero-day vulnerabilities discovered in 2015 was the same as in 2014 – 25 zero-day vulnerabilities in 'All' products.

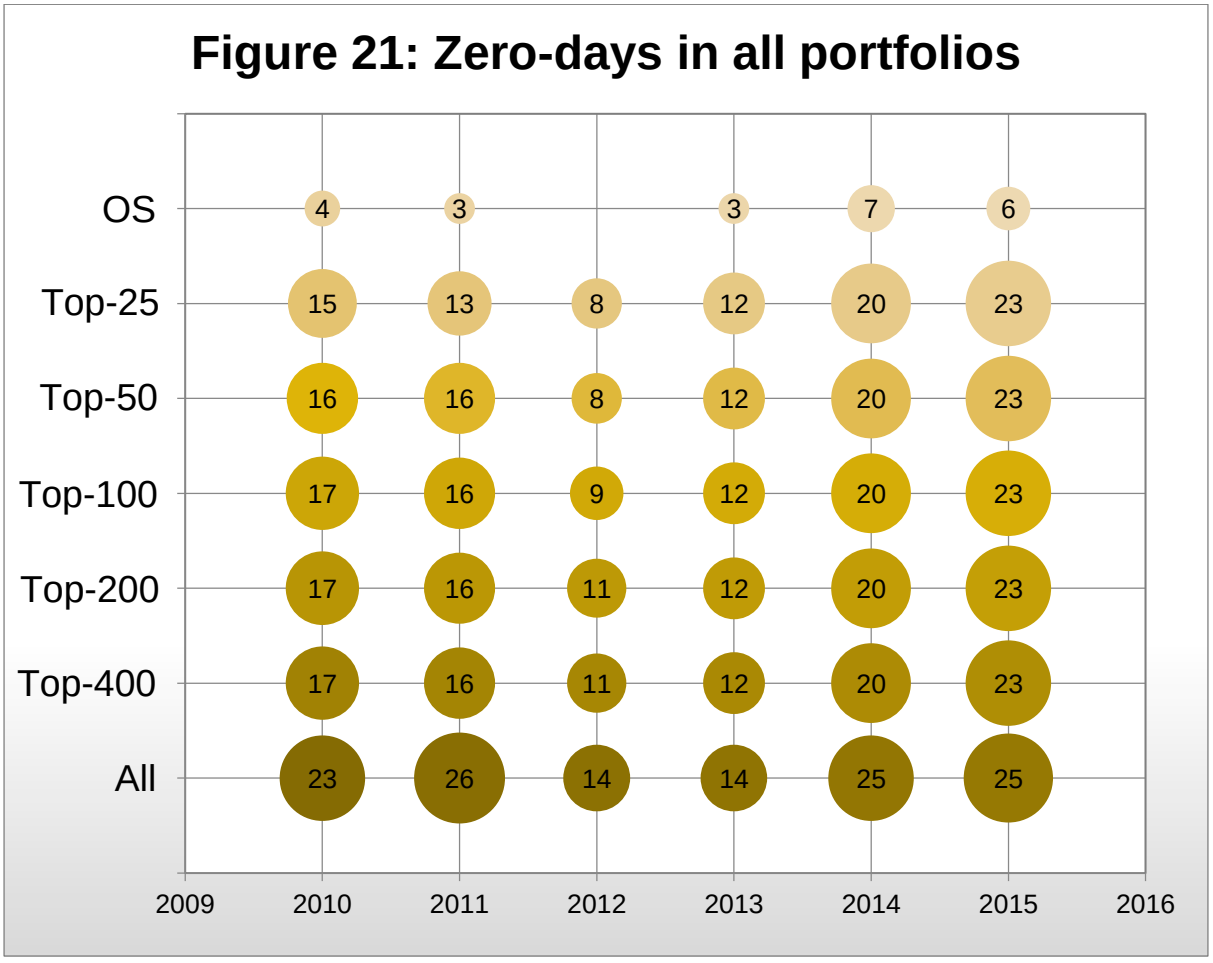
23 of the 25 zero-day vulnerabilities were discovered in the Top 50 portfolio, compared to 20 the year before.

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 have been discovered two years in a row is significant, given the role zero-day vulnerabilities play as potential attack vectors in Advanced Persistent Threat attacks

.

FIGURE 21: ZERO-DAY VULNERABILITIES REGISTERED BY SECUNIA RESEARCH IN 2015



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

Browser Security

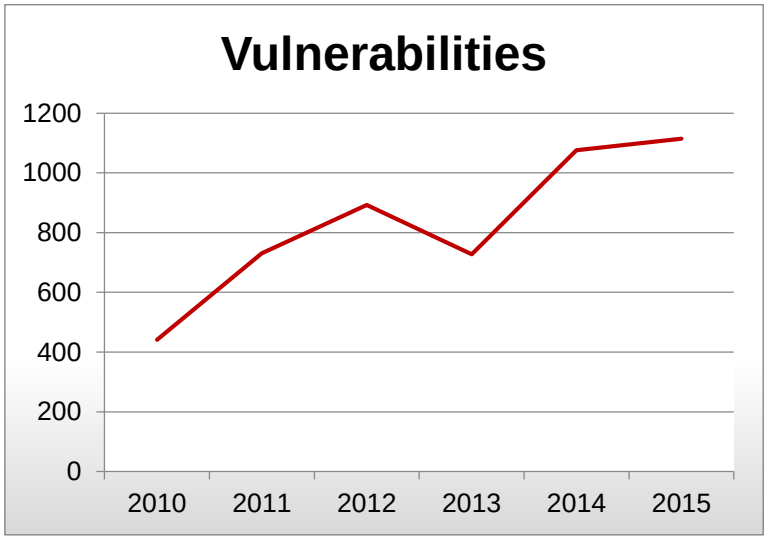
This snapshot of browser security outlines the evolution of vulnerabilities relating to the five most popular browsers (Google Chrome, Mozilla Firefox, Internet Explorer, Opera and Safari[3]). Overall, data shows that there were 1,114 vulnerabilities in these browsers in 2015 compared to 1,076 in 2014 – a year-on-year increase of 4%. The majority of these vulnerabilities were rated as 'Highly Critical'. Although Apple Safari for Windows is categorized as end-of-life by Secunia Research, because it has not received maintenance and development for a period of three years, it is still found on 7% of PCs, making it the fifth most popular browser on computers with Personal Software Inspector installed.

Figure 23 illustrates the distribution of vulnerabilities across the five browsers in 2015, including their market share, exposure level and patch status. For Apple Safari, the number of vulnerabilities and patch status are not shown, as Secunia Research does not track vulnerabilities/patch state in end-of-life products. End-of-life products are by definition insecure, because they are no longer supported by the vendor and do not receive security updates.

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 axis 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 more victims.
The calculation of the yearly average is based on Personal Software Inspector data.

Importantly, even though Internet Explorer has a market share of 99%, Firefox and Chrome are actually installed on 64% and 66% of the scanned systems with the Personal Software Inspector 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



[1] Apple Safari for Windows is end-of-life. As the product is therefore no longer supported by the vendor, Secunia Research no longer tracks vulnerabilities in it.

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

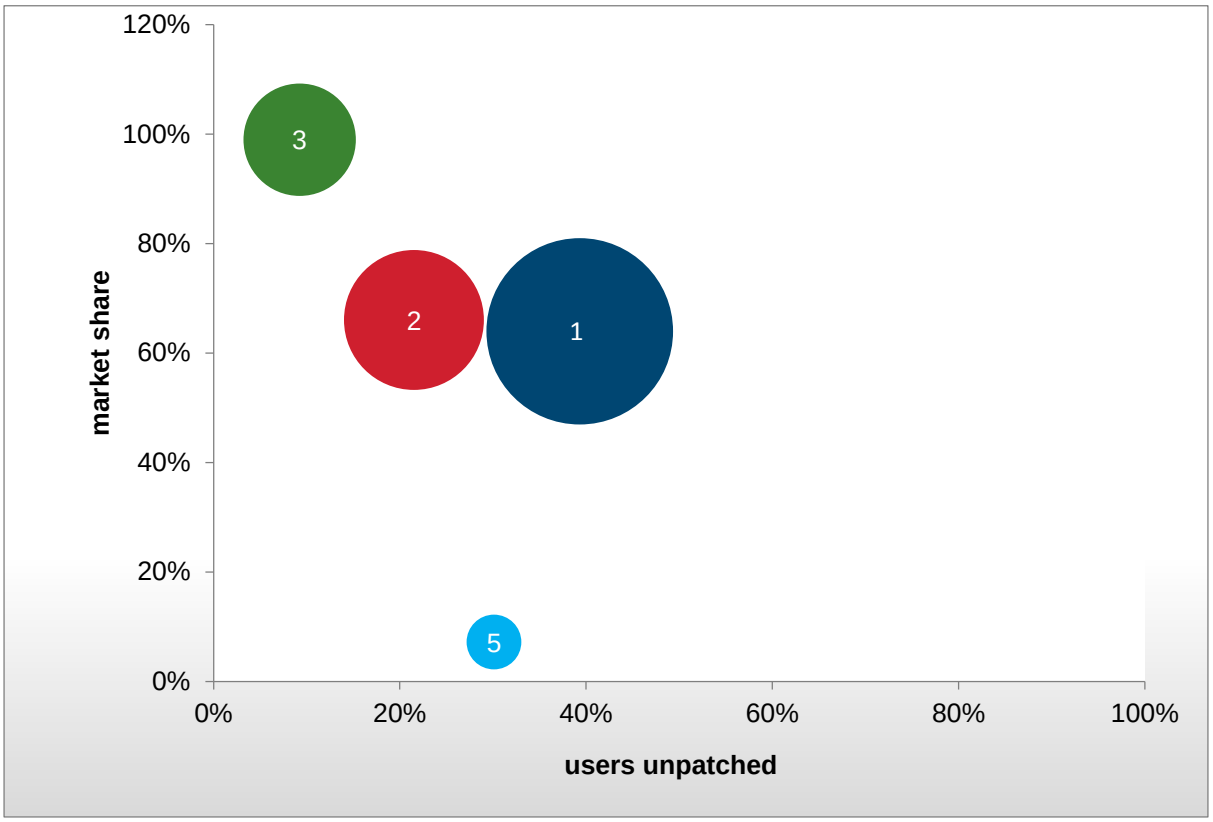


FIGURE 24: VULNERABILITIES IN THE 5 MOST POPULAR BROWSERS

Program	Unpatched	Market share	Vulns
1 Mozilla Firefox	39%	64%	254
2 Google Chrome	22%	66%	516
3 Microsoft Internet Expl	9%	99%	197
4 Apple Safari	End-of-Life*	7%	0*
5 Opera	30%	7%	16

Vulns indicate number of new vulnerabilities in the last 12 months. Market share is percentage of Personal Software Inspector users with the product installed on their PC.

*Apple Safari for Windows is end-of-life. As the product is therefore no longer supported by the vendor, Secunia Research no longer tracks vulnerabilities on it.

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

PDF Readers

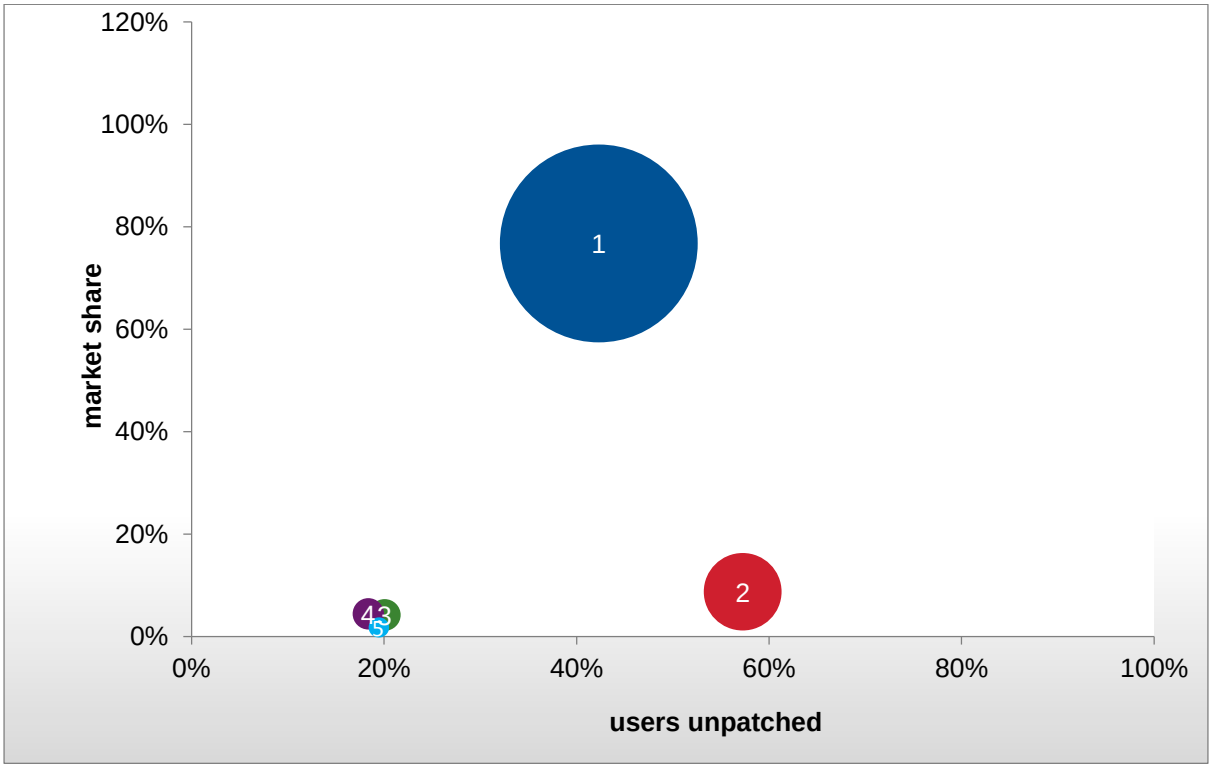
This snapshot of the security status of PDF readers outlines the evolution of vulnerabilities relating to the five most popular products (Adobe Reader, Foxit Reader, PDF-XChange Viewer, Sumatra PDF and Nitro PDF Reader). There has been an increase in the overall number of vulnerabilities in these PDF readers, with 147 vulnerabilities identified in 2015 (45 in 2014). The majority of these vulnerabilities were rated as either 'Highly Critical' or 'Extremely Critical'

Figure 25 below illustrates the distribution of vulnerabilities across the five PDF readers in 2015, 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 axis 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 Personal Software Inspector data.

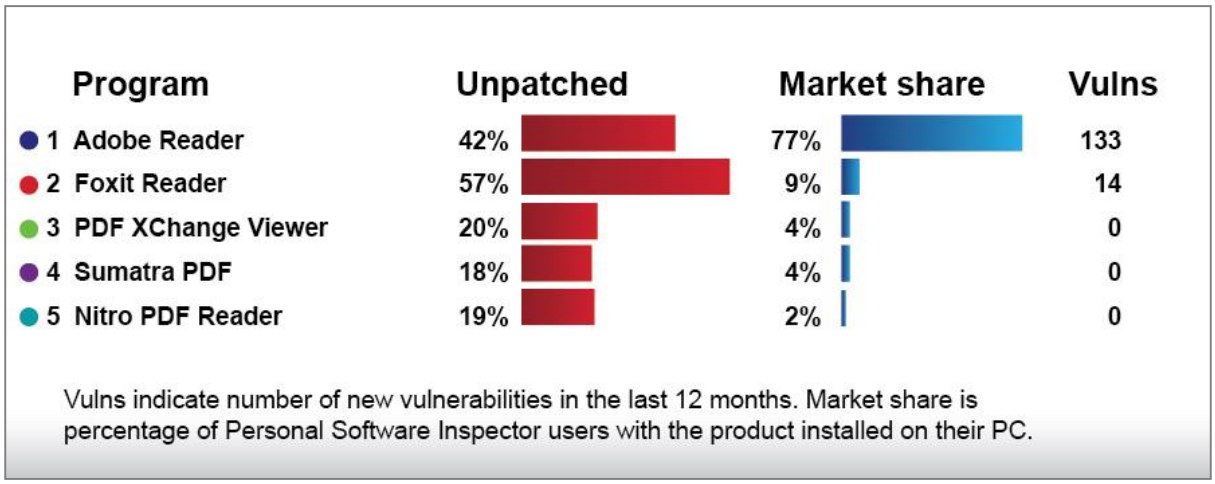
Installed on 77% of PCs, Adobe Reader has the lion share of the market and the largest amount of vulnerabilities: 133 in 2013 – with 42% of its users leaving it unpatched despite this fact. While the only other PDF with reported vulnerabilities, Foxit Reader, only had 14, more than half of the users – 57% - failed to patch it. Even though the remaining three PDF readers are listed as having 0 vulnerabilities they will 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



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

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



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

Appendix
& Glossary

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

Appendix

Secunia Research Software Vulnerability Tracking Process

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

NOTE: From 2016, the MITRE CVE only provides coverage of products on the CVE Published Priorities list. For more information, go to www.cve.mitre.org

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

Attack Vector

The attack vector describes the way an attacker can trigger or reach the vulnerability in a product. Secunia Research 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

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.

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.

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

Secunia Research 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).

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

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 2015 and the number of vulnerabilities affecting the program in 2014 and 2015.
The ranking and market share is derived from anonymous scans of Personal Software Inspector in December 2015. 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 (#33) share code components and thereby also share numerous vulnerabilities.

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

RANK	TYPE	PRODUCT	SHARE	VULNS
1	MS	Microsoft Windows Script Control	99,9%	0
2	MS	Microsoft XML Core Services (MSXML)	99,9%	2
3	MS	Microsoft .NET Framework	99,6%	29
4	MS	Microsoft Windows Media Player	99,2%	1
5	MS	Microsoft Internet Explorer	99,1%	197
6	MS	Microsoft Visual C++ Redistributable	99,0%	0
7	NMS	Adobe Flash Player	95,0%	457
8	MS	Windows PowerShell	90,9%	0
9	MS	Microsoft Silverlight	86,0%	23
10	MS	Microsoft Windows Defender	82,8%	0
11	NMS	Adobe Reader	81,1%	133
12	MS	Windows DVD Maker	78,2%	0
13	MS	Microsoft XPS-Viewer	77,6%	0
14	NMS	Oracle Java JRE	76,7%	81
15	MS	Microsoft Word	74,3%	45
16	MS	Microsoft Excel	73,8%	52
17	MS	Microsoft PowerPoint	72,0%	31
18	MS	Windows Media Center	70,2%	3
19	NMS	Google Chrome	67,3%	516
20	NMS	Mozilla Firefox	65,5%	254
21	MS	Microsoft Visio Viewer	61,1%	0
22	MS	Chess Titans	61,0%	0
23	MS	Driver Package Installer (DPInst)	59,0%	0
24	NMS	Mozilla Maintenance Service	58,1%	0
25	MS	Microsoft SQL Server	58,0%	3
26	MS	Microsoft Outlook	56,7%	1
27	NMS	Realtek AC 97 Update and remove driver Tool	55,6%	0
28	MS	Microsoft Access	54,5%	8
29	MS	Microsoft Publisher	54,3%	7
30	MS	comdlg32 ActiveX Control	53,1%	0
31	NMS	CCleaner	49,6%	0
32	MS	Windows Live Mail	49,3%	0
33	NMS	Adobe AIR	49,1%	306
34	MS	Windows Live Movie Maker	49,1%	0

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

35	MS	MSCOMCT2 ActiveX Control	48,9%	0
36	NMS	Apple Bonjour for Windows	46,9%	0
37	MS	Windows Live Writer	46,8%	0
38	NMS	Apple QuickTime	46,7%	18
39	NMS	Realtek Voice Manager	45,3%	0
40	MS	Windows Live Photo Gallery	44,1%	0
41	MS	Windows Live Messenger	43,5%	0
42	NMS	Apple iTunes	42,8%	130
43	NMS	VLC Media Player	41,4%	9
44	MS	Microsoft PowerPoint Viewer	39,9%	2
45	MS	Windows Live Essentials	39,5%	0
46	NMS	Google Earth	36,8%	0
47	MS	Skype for Windows	36,4%	0
48	MS	Microsoft OneNote	34,5%	7
49	NMS	InstallShield Update Service	33,2%	0
50	NMS	HP Product Detection ActiveX Control	31,9%	0
OS	MS	Microsoft Windows 7	N/A	144

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 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.

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

About Flexera Software

Flexera Software helps application producers and enterprises manage application usage and increase the value they derive from their software. Our next-generation software licensing, compliance, security and installation solutions are essential to ensure continuous licensing compliance, optimize software investments and future-proof businesses against the risks and costs of constantly changing technology. Over 80,000 customers turn to Flexera Software as a trusted and neutral source for the knowledge and expertise we have gained as the marketplace leader for over 25 years and for the automation and intelligence designed into our products. For more information, please go to: **www.flexerasoftware.com**

Flexera Software, LLC.
(Global Headquarters),
+1 800-809-5659

United Kingdom (Europe,
Middle East Headquarters):
+44 870-871-1111
+44 870-873-6300

Australia (Asia,
Pacific Headquarters):
+61 3-9895-2000

For more locations visit:
www.flexerasoftware.com