



VULNERABILITY REVIEW 2018

Top Desktop Apps

Key figures and facts on vulnerabilities
affecting most common desktop applications

Published June, 2018

Contents

Introduction to the Vulnerability Review 2018 – Top Desktop Apps.....	3
The Issue of Desktop Apps.....	4
Vulnerability Update.....	6
We Divide the Products into Three Categories	10
Vendor Update – Top 50 Portfolio ⁽³⁾	11
Time-to-Patch.....	16
Appendix.....	18
Metrics Used to Count Vulnerabilities.....	19
Attack Vector.....	20
Unique and Shared Vulnerabilities.....	21
Secunia Vulnerability Criticality Classification	22
The Top 50 Software Portfolio	23
Glossary.....	25

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

Introduction to the Vulnerability Review 2018 – Top Desktop Apps

The annual Vulnerability Review analyzes the evolution of software security from a vulnerability perspective. The Top Desktop Apps issue explores vulnerabilities in the 50 most popular applications on desktops.

What does the Vulnerability Review cover?

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

Secunia Research monitors more than 55,000 applications, appliances and operating systems, and tests and verifies the vulnerabilities reported in them.

This edition focuses on a subset of this data: the Top 50 Windows Desktop Applications.

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

In the event of customers using products that aren't 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 Flexera 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.

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

The Issue of Desktop Apps

This year's edition of the *Vulnerability Review – Global Trends* will probably get some extra attention. In 2017, the exploitation of known software vulnerabilities made global headlines and put a spotlight on how organizations manage them. The WannaCry attacks and the Equifax breach—to mention the most publicized—sounded the alarm in many boardrooms and raised questions about how much effort businesses put into identifying and mitigating the exploitation risk of software vulnerabilities.

This brand-new edition of the Flexera Vulnerability Review, focuses on the most common desktop applications to give IT professionals knowledge to better evaluate strategies to keep their systems secure and their users undisturbed and productive. It helps demystifying security patching and understanding that it's possible to create a patching program that can be effective, without disturbing users or creating additional overhead.

Security patches vs. updates

Not all software updates are security related and not all security updates are equally critical, though you will find that when it comes to most common desktop apps, on average, criticality tends to be much higher when compared to all the applications that our Secunia Research team tracks. In fact, security patches make up a relatively small number of updates. This review, and the underlying data that supports it, indicate that improving the status of security patching could be simple. It's a matter of addressing three main issues:

- **Security key performance indicators (KPI) for Desktop Admins** – It's surprising the number of Desktop Management professionals who confirm that they don't have any KPI that measures the vulnerability management side of deployment and management of desktop apps. Given this reality, it's no surprise that despite the high risks associated with missing security patches, little effort is put into solving the problem.
- **Complete inventory of desktops apps** – Knowing which applications, and which versions, are installed in each machine is an enormous challenge. It's difficult to understand what level of accuracy and depth different types of system in the market provide. The most common is that the level of information provided by system management tools isn't deep enough to determine patch status. Consequently, it makes the work of patching a difficult task.
- **Security Patching Processes** – Microsoft Patch Tuesday played an important role in making patching Microsoft applications a routine for organizations. The fact that Microsoft provides patches at regular intervals helped organizations develop and follow processes for those. The same principle (patching applications at determined intervals) would help extending patching to other systems and non-Microsoft applications. It doesn't matter if many other vendors don't have regular intervals for their security patch releases. By creating a process on a regular interval, and solving the issues of collecting inventory, prioritization and sourcing patches, it's possible to address all security patches within a reasonable interval.

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

Understanding the vulnerability landscape is a great first step

The data in the review makes it possible to understand the vulnerability landscape when it comes to the most common desktop applications and shows is that it's possible to address security risks with patches for almost all vulnerabilities affecting the most common desktop applications. Explore the data and find out how it can help you rethink your patch management strategy.

What next?

What if this knowledge was integrated in a solution that supports end-to-end processes, automation of policy implementation and low risk tasks? This is where Flexera delivers tangible value. The intelligence about software vulnerabilities is at the center of our vision, solving the technological challenges of patching. Our customers patch the right things with less effort. See what our customers say [here](#).

KEY TAKEAWAYS



There is far more risk on vulnerabilities on the Top Desktop Apps.

83% of the Secunia Advisories were rated “Extremely” or “Highly” critical. This is a significant figure considering that this number is 17% when we look at all apps in our entire database. Also, 93.9% of the advisories in this group could be exploited through the internet, without interaction with the user. That means exploitation of vulnerabilities in this group can have greater impact for organizations and are easier to target.



Patching Microsoft applications is simply not enough.

65% of the vulnerabilities reported in the 50 most common desktop apps were on non-Microsoft applications, even though they represent only 33% of the apps in a Windows system. This is compelling evidence that it's urgent to move beyond patching Microsoft applications only in Windows systems.



You can patch. Ultimately, it's all about process.

94% of the advisories had a patch available at the day they became public. This figure rises to 97% within 30 days of public disclosure. Considering that we are talking about a handful of applications, we can say that improving patching and consequently reducing risk is ultimately about processes. The key is to have visibility and intelligence to help organizations gain control over their patching activities.

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

Vulnerability Update

Top 50 Portfolio¹

What is the Top 50 Portfolio?

To assess 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 2017 of the Personal Software Inspector² users' computers – with an average of 70 programs installed on them. From country to country and region to region, there are variations as to which applications are installed. For the sake of clarity, we have chosen to focus on the state of a representative portfolio of the 50 most common applications found on computers. These 50 applications are comprised of 33 Microsoft applications and 17 non-Microsoft applications.



Number of Vulnerabilities - Top 50 Portfolio

The number of vulnerabilities in the Top 50 portfolio was 1,922, discovered in 22 products from eight vendors plus the most used operating system, Microsoft Windows 7.

The number shows a 27% increase in the five-year trend, and a 3% decrease from 2016 to 2017.

Figure
1

SECUNIA ADVISORIES/ VULNERABILITIES IN TOP 50 PRODUCTS

	Secunia Advisories	Vulnerability Count	Vendors	Products
 Average 2012-16	134	1,516	7	22
Total 2017	147	1,922	8	22
 Trend 5 year	10%	27%	14%	0%
Trend 2016/17	-27%	3%	14%	-12%

Copyright © 2018 Secunia Research at Flexera | Source: Vulnerability Review 2018

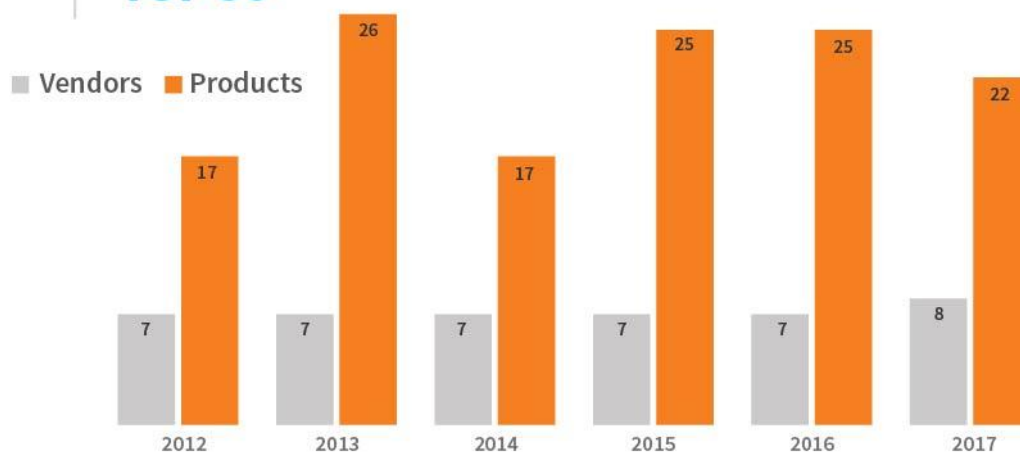
¹ Find the list of the Top 50 applications in the Appendix

² Personal Software Inspector reached End-of-service-life in April 2018 and is no longer available. More information [here](#).

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

Figure
2

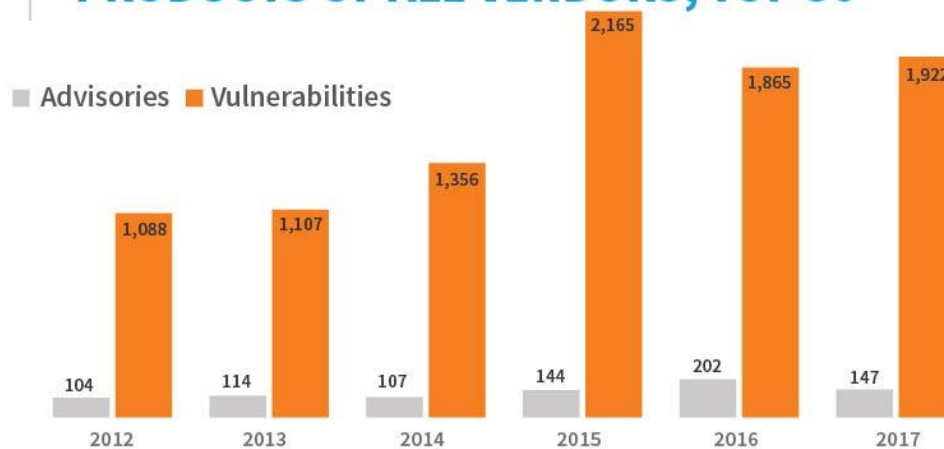
VULNERABLE PRODUCTS AND VENDORS, TOP 50



Copyright © 2018 Secunia Research at Flexera | Source: Vulnerability Review 2018

Figure
3

GLOBAL VULNERABILITIES HISTORY, ALL PRODUCTS OF ALL VENDORS, TOP 50



Copyright © 2018 Secunia Research at Flexera | Source: Vulnerability Review 2018

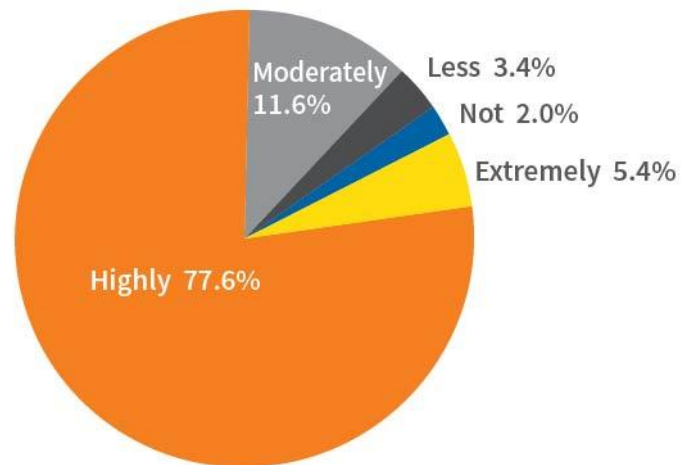
See the Appendix for methodology, including definitions of Secunia Advisories, CVEs and Vulnerabilities; criticality ratings, attack vectors.

Criticality – Top 50 Portfolio

The combined number of 'Highly Critical' and 'Extremely Critical' vulnerabilities: 83% represented the majority of vulnerabilities in the Top 50 rated by Secunia Research in 2017.

Figure
4

CRITICALITY OF ADVISORIES, TOP 50



Copyright © 2018 Secunia Research at Flexera | Source: Vulnerability Review 2018

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

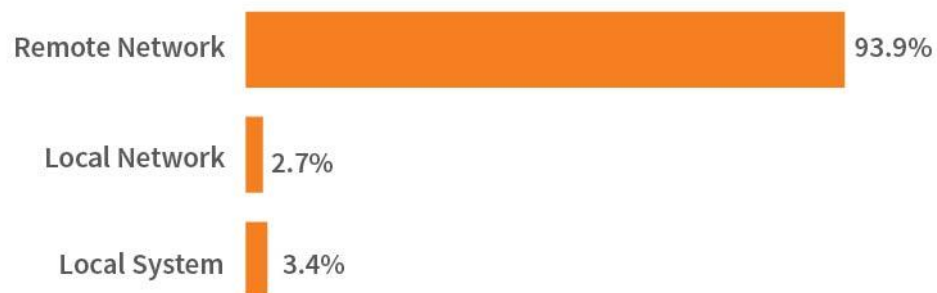
Attack Vector – Top 50 Portfolio

With a 93.9% share, the foremost attack vector available to attackers to trigger a vulnerability in the Top 50 portfolio was Remote Network. This is a significant increase compared to 2016.

Local Network saw a decrease, from 4.5% in 2016, to 2.7% in 2017. Local System recorded a steep decrease compared to last year, from 13.5%, to 3.4% in 2017.

Figure
5

ATTACK VECTOR, TOP 50



Copyright © 2018 Secunia Research at Flexera

Source: Vulnerability Review 2018

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

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 Inspector³ installed.

Non-Microsoft applications: Software from all other vendors – represents 60% of the applications on a computer with Personal Software Inspector³ installed.

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

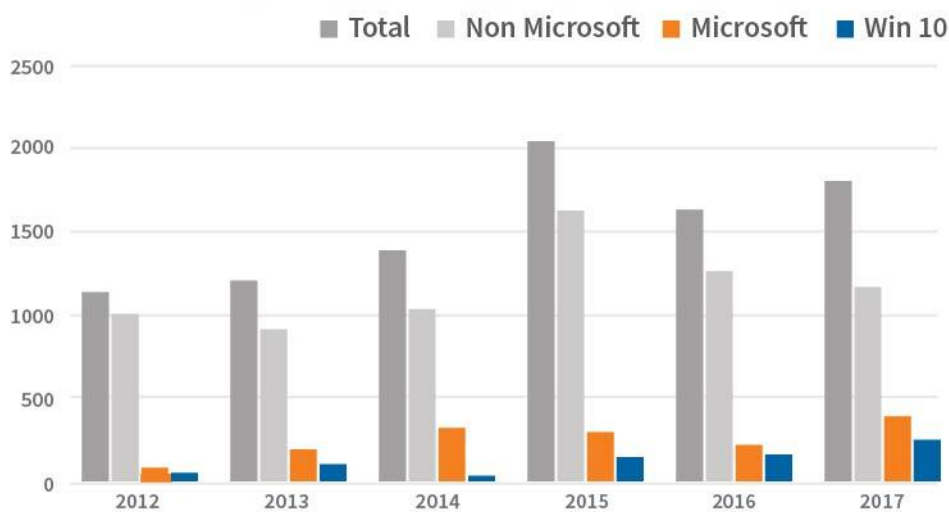
Product composition, Top 50 portfolio

Microsoft applications: Represent 65% of the Top 50 applications on a computer with Personal Software Inspector³ installed.

Non-Microsoft applications: Software from all other vendors – represents 33% of the Top 50 applications on a computer with Personal Software Inspector³ installed.

Figure
6

TOP 50 PORTFOLIO AND WINDOWS 10



Copyright © 2018 Secunia Research at Flexera | Source: Vulnerability Review 2018

³ Personal Software Inspector reached End-of-service-life in April 2018 and is no longer available. More information [here](#).

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

Vendor Update – Top 50 Portfolio

Different vendors have different security update mechanisms. Microsoft applications, which account for 67% of the applications (including Windows 10 OS) in the Top 50 portfolio, are updated automatically.

But Microsoft applications (including Windows 10 OS) are only responsible for 35% 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 in 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 2017, 65% of the vulnerabilities affecting the Top 50 applications in the representative software portfolio affected non-Microsoft applications. This means that 35% of the remaining vulnerabilities in the Top 50 applications installed on the computers of Personal Software Inspector⁴ users stem from the Windows 10 operating system (14%) and Microsoft applications (21%).

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's 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's an unrealistic assumption that an end user's 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 an impact on the total number of vulnerabilities on a typical endpoint: In 2017, 14% of vulnerabilities were reported in Windows 10, the operating system we're tracking with the Top 50 portfolio.

Microsoft applications

There were more vulnerabilities reported in Microsoft applications in 2017 compared to the previous year: up from 13.5% to 21%. The vulnerability count in Microsoft applications was 390 in 2017; in 2016 it was 219.

⁴ Personal Software Inspector reached End-of-service-life in April 2018 and is no longer available. More information [here](#).

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

Increase in vulnerabilities in Windows

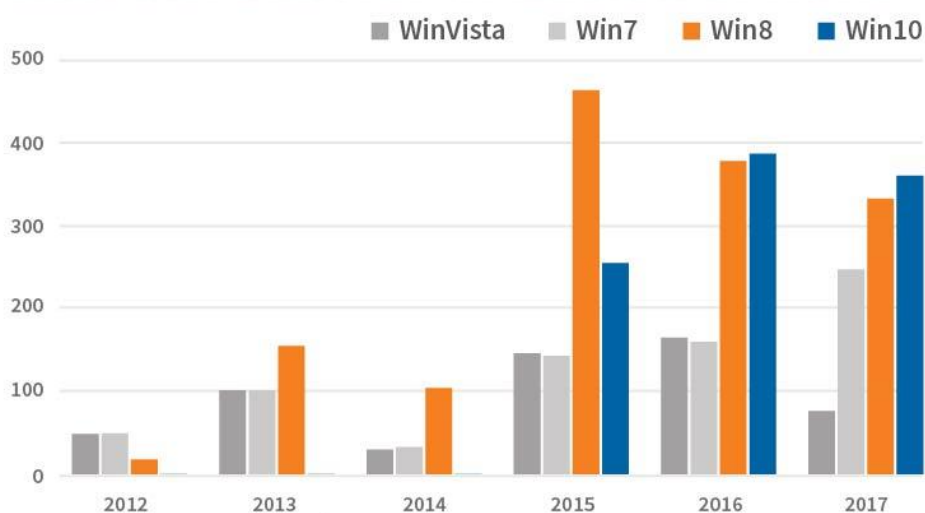
Data shows a decrease in the number of vulnerabilities recorded in all Windows operating systems except Windows 7:

- Windows 10⁵ went from 380 in 2016, to 363 in 2017.
- Windows 8⁵ went from 369 in 2016, to 335 in 2017.
- Windows 7 went from 151 in 2016, to 249 in 2017.
- Windows Vista went from 154 in 2016, to 77 in 2017.

(4): 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
7

WINDOWS DESKTOP OPERATING SYSTEMS



⁵ 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
8

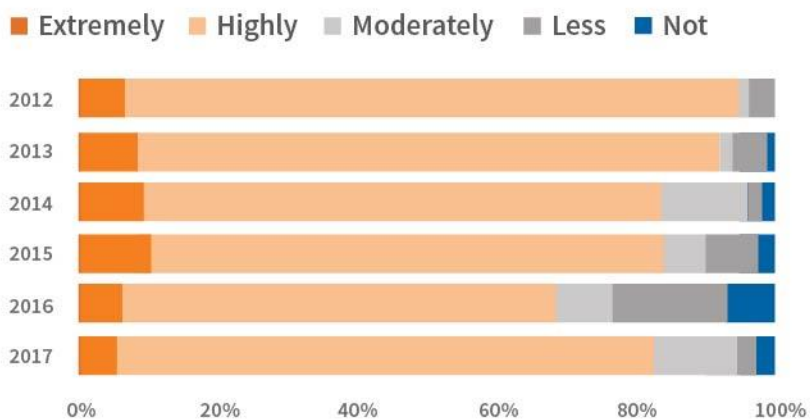
BREAKDOWN OF END-POINT VULNERABILITIES IN 2017

	WinVista	Win7	Win8	Win10
Operating System	77	249	335	363
Microsoft Programs	390	390	390	390
Non-Microsoft Programs	1,170	1,170	1,170	1,170
Total	1,637	1,808	1,894	1,922

Copyright © 2018 Secunia Research at Flexera | Source: Vulnerability Review 2018

Figure
9

CRITICALITY OF PORTFOLIO VULNERABILITIES

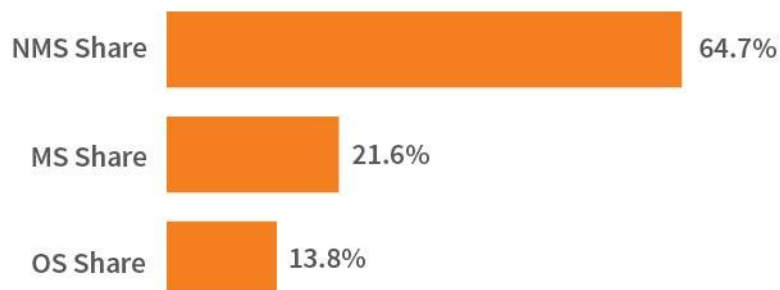


Copyright © 2018 Secunia Research at Flexera | Source: Vulnerability Review 2018

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

Figure
10

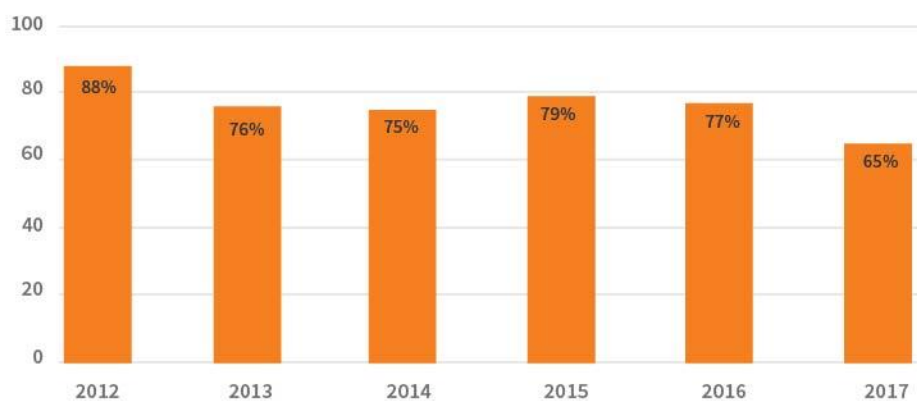
PORTFOLIO SHARE OF VULNERABILITIES BY SOURCE, TOP 50



Copyright © 2018 Secunia Research at Flexera | Source: Vulnerability Review 2018

Figure
11

SHARE OF VULNERABILITIES BY NON-MICROSOFT PROGRAMS

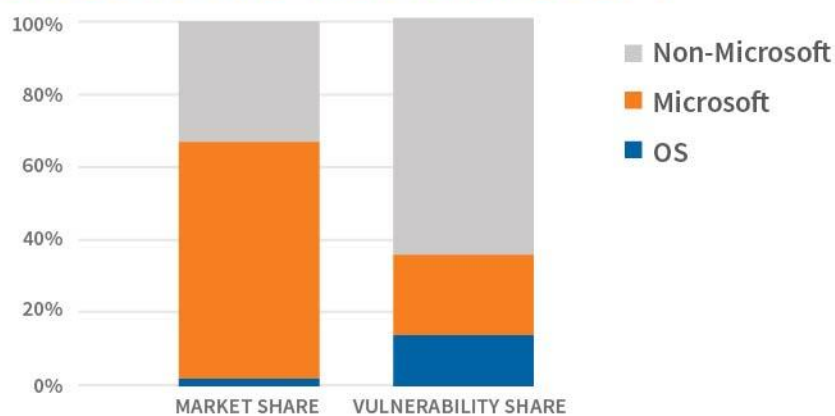


Copyright © 2018 Secunia Research at Flexera | Source: Vulnerability Review 2018

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

Figure
12

MARKET SHARE/VULNERABILITY SHARE, MICROSOFT AND NON-MICROSOFT



Copyright © 2018 Secunia Research at Flexera | Source: Vulnerability Review 2018

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

Time-to-Patch

In the Top 50 applications, 93.9% of vulnerabilities had a patch available on the day of disclosure. This number is a notch higher than the 92.5% time-to-patch rate that was recorded in 2016.

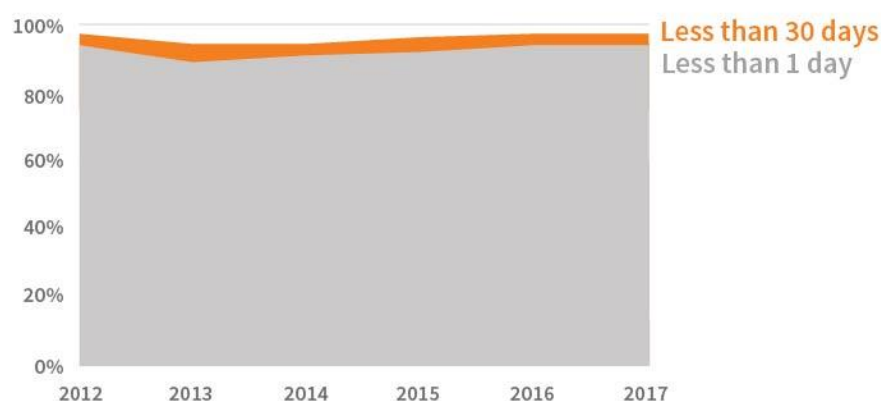
The 2017 results remain positioned at the higher end of the scale, indicating that it's still possible to remediate the majority of vulnerabilities with a patch.

However, there are still 6.1% of vulnerabilities that remain without a patch for longer than the day of disclosure.

Consequently, and particularly for organizations with a vast array of endpoints to manage (including devices not regularly connected to corporate networks), the fact that a percentage of vulnerabilities don't have patches at the first day of disclosure means that a variety of mitigating efforts are required to ensure sufficient protection, in support of patch management efforts.

Figure
13

PATCH AVAILABILITY FOR VULNERABILITIES IN THE TOP 50 PORTFOLIO, HISTORICALLY



Copyright © 2018 Secunia Research at Flexera

Source: Vulnerability Review 2018

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.

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

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 2015, 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 isn’t 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’s reasonable to assume that a security conscious user can be tricked into performing certain actions.

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

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 aren't 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 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 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 doesn't 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 doesn't 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 aren't 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 2017 and the number of vulnerabilities affecting the program in 2016 and 2017.

The ranking and market share is derived from anonymous scans of Personal Software Inspector⁶ in December 2017. Note that the sum of the vulnerabilities in this table doesn't reflect the total number of vulnerabilities in the portfolio as many products share vulnerabilities.

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

Rank	Type	Product	Share	Advs	Vulns
1	ms	Microsoft XML Core Services (MSXML)	99,3%	0	0
2	ms	Microsoft .NET Framework	99,2%	5	8
3	ms	Microsoft Visual C++ Redistributable	99,1%	0	0
4	ms	Microsoft Windows Media Player	97,9%	0	0
5	ms	Microsoft Windows Malicious Software Removal Tool	97,6%	0	0
6	ms	Microsoft Internet Explorer	97,1%	10	80
7	ms	Windows PowerShell	97,0%	0	0
8	ms	Microsoft Malware Protection	96,3%	4	16
9	ms	Microsoft XPS-Viewer	93,6%	0	0
10	nms	Adobe Flash Player	91,6%	12	70
11	ms	Microsoft Word	72,7%	7	59
12	ms	Microsoft Excel	72,5%	5	44
13	ms	Microsoft PowerPoint	71,1%	2	39
14	nms	Google Chrome	70,3%	15	297
15	ms	Microsoft Silverlight	67,5%	2	3
16	nms	Mozilla Firefox	64,2%	20	305
17	nms	Mozilla Maintenance Service	63,4%	0	0
18	nms	Oracle Java JRE	60,6%	4	72
19	nms	Adobe Acrobat	59,2%	7	328
20	ms	Microsoft Outlook	58,5%	5	57
21	ms	Microsoft OneDrive (formerly SkyDrive)	58,4%	0	0
22	ms	Microsoft Publisher	57,1%	1	1
23	ms	Microsoft Access	56,3%	0	0
24	ms	Microsoft Edge	52,8%	11	200
25	ms	Microsoft Visual Studio	50,3%	0	0
26	ms	Microsoft OneNote	49,7%	2	35
27	ms	Driver Package Installer (DPInst)	49,3%	0	0
28	ms	Microsoft Visio Viewer	48,7%	0	0
29	nms	Realtek AC 97 Update and remove driver Tool	48,0%	0	0
30	ms	Microsoft Windows Defender	47,3%	3	15

⁶ Personal Software Inspector reached End-of-service-life in April 2018 and is no longer available. More information [here](#).

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

31	nms	VLC Media Player	45,9%	3	8
32	nms	CCleaner	43,5%	1	1
33	nms	Apple Bonjour for Windows	42,1%	0	0
34	ms	Skype for Windows	40,0%	0	0
35	ms	Microsoft SQL Server	39,5%	1	1
36	ms	comdlg32 ActiveX Control	39,1%	0	0
37	ms	Windows DVD Maker	37,7%	0	0
38	ms	Windows Live Movie Maker	36,0%	0	0
39	nms	7-zip	36,0%	0	0
40	ms	Windows Media Center	35,5%	0	0
41	nms	Adobe AIR	34,4%	0	0
42	nms	Apple iTunes	33,8%	7	89
43	ms	Windows Live Photo Gallery	33,5%	0	0
44	ms	MSCOMCT2 ActiveX Control	32,8%	0	0
45	nms	Realtek Voice Manager	30,3%	0	0
46	ms	Windows Live Mail	30,0%	0	0
47	nms	NVIDIA Display Server	29,5%	0	0
48	nms	Malwarebytes Anti-Malware	27,9%	0	0
49	ms	Windows Live Writer	27,6%	0	0
50	nms	Google Earth	26,9%	0	0
OS	ms	Microsoft Windows 10	N/A	35	363

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

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's publicly known.

ABOUT FLEXERA

Flexera is reimagining the way software is bought, sold, managed and secured. We make the business of buying and selling software more transparent, secure and effective.

www.flexera.com

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



Flexera

300 Park Blvd., Suite 500

Itasca, IL 60143

USA

Itasca (Global Headquarters):

+1 800-374-4353

United Kingdom (Europe, Middle East Headquarters)

+44 370-871-1111

+44 870-873-6300

Japan (Asia, Pacific Headquarters)

+81 3-4360-8291

Australia

+61 3 9895 2000

www.flexera.com

©2018 Flexera Software LLC. All rights reserved. All other brand and product names are trademarks, registered trademarks, or service marks of their respective owners.

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