Flexera

VULNERABILITY REVIEW 2018

Global Trends

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

Index

Appendix

Introduction to the Vulnerability Review 2018 – Global Trends

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, and maps the security threats to IT infrastructures.

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.

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

The Vulnerability Database covers vulnerabilities that can be exploited in all types of products—including software, hardware and firmware.

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 vulnerability risk posed in their environment. The Secunia Advisory descriptions include criticality, attack vector and solution status.

How do we count vulnerabilities?

Research houses in the vulnerability management space adopt different approaches to counting vulnerabilities.

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. We provide verified intelligence listing all products affected by a given vulnerability.

Software Vulnerabilities in the Spotlight

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.

Why do we see known-vulnerabilities at the center of incidents?

This spotlight on vulnerability management showed us that many organizations still don't have processes and procedures in place to reduce the number of system vulnerabilities. It also exposed the fact that a gap remains between identifying vulnerable applications and fixing them. This gap gives attackers plenty of time to navigate systems, grow privileges, move, spy and steal.

Intelligence and processes

One of the most common trends we see when high-profile vulnerabilities and breaches become public, is that a sense of urgency arises, and many businesses drop activities to figure out how to put out fires. This approach is inefficient because it impacts productivity and because it isn't processes-driven, requiring great effort to achieve few results. Furthermore, once the hype has passed, organizations frequently forget the problem and go back to their old habits, until the next big vulnerability initiates a new fire.

In light of the surge in exploitation of unpatched vulnerabilities, we see an increasing pressure on businesses to find better approaches to mitigation. One critical element for a better approach is intelligence about vulnerabilities, which helps understand risk and determine how to prioritize and mitigate threats. The others are the operational processes to continuously drive reduction in the number of unknown and non-mitigated risks, and avoid disruption when big breaches hit the media.

Vulnerability Review 2018 – Global Trends provides data on vulnerabilities, enabling you to understand the vulnerability landscape and devise strategies to secure what matters for your business.

KEY TAKEAWAYS

An all-time high of nearly 20,000 vulnerabilities were documented in 2017. This is compelling evidence that the challenge of reducing risk is becoming more difficult. The only way a business can protect itself today is to ensure that vulnerabilities are visible, prioritized and remediated with optimized processes.

Patches are available for 86 percent of known vulnerabilities at the day of disclosure. This confirms that businesses must maintain continuous visibility of software assets and the vulnerabilities affecting them, and have optimized processes to ensure critical issues are addressed before exploitation risk increases.

Zero-Day vulnerabilities—those exploited prior to public disclosure—remain rare: 14 out of 19,954. This highlights the fact that there is time to remediate most vulnerabilities before exploitation risk increases.

Vulnerability Update

By the Numbers

Vulnerabilities detected: All products

The absolute number of vulnerabilities detected was 19,954, discovered in 1,865[(1)] applications from 259 vendors. The number shows a 38% increase in the five-year trend, and a 14% increase from 2016 to 2017.

Since 2016, the number of vendors behind the vulnerable products has increased by 3% and the number of vulnerable products has decreased by 13%.

The substantial drop in numbers of products during the years 2016 and 2017 is a result of Secunia Research's decision to focus on the products and vendors present in the environments of Flexera's Software Vulnerability Management customers.

As a result, a number of products and vendors *not* used in customer environments are no longer tracked systematically.

Figure 1

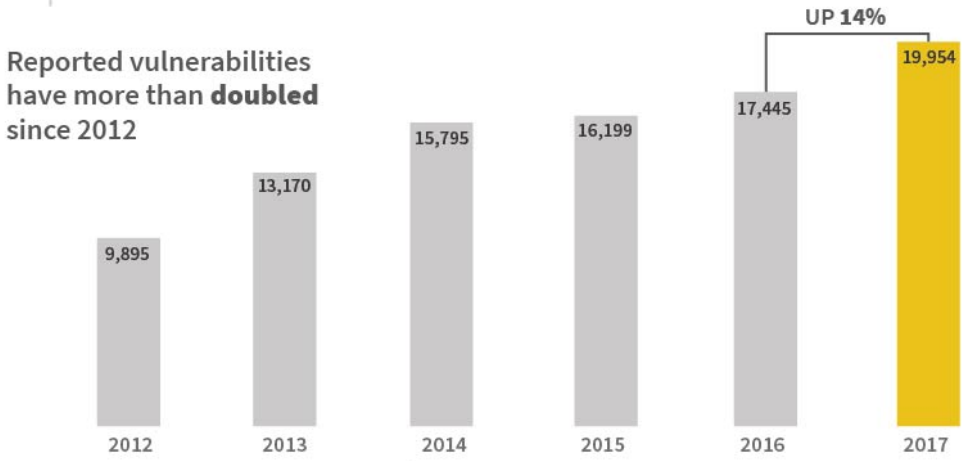
SECUNIA ADVISORIES/ VULNERABILITIES IN ALL PRODUCTS

	Secunia Advisories	Vulnerability Count	Vendors	Products
Average 2012-16	3.500	14.501	446	2.965
Total 2017	3.266	19.954	259	1.865
Change (past 5 years)	-7%	38%	-42%	-37%
Change (2016 to 17)	-4%	14%	3%	-13%

 | *Source: Vulnerability Review 2018*

Figure 2

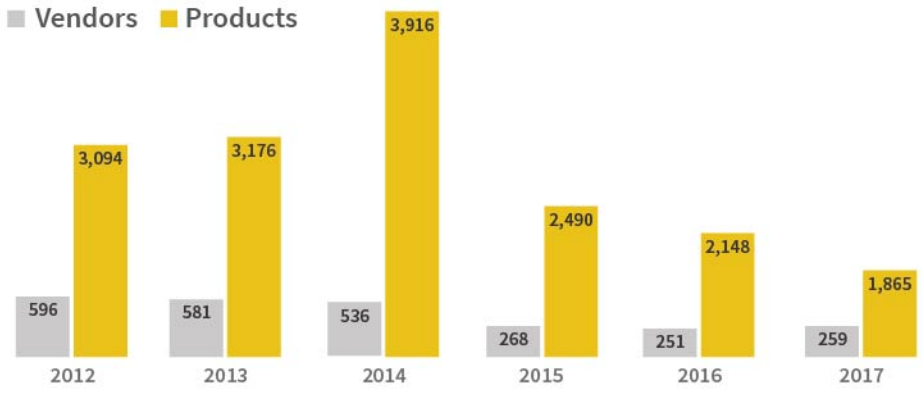
GLOBAL VULNERABILITIES REPORTED FOR ALL PRODUCTS OF ALL VENDORS



 | *Source: Vulnerability Review 2018*

Figure 3

VULNERABLE PRODUCTS AND VENDORS



 | *Source: Vulnerability Review 2018*

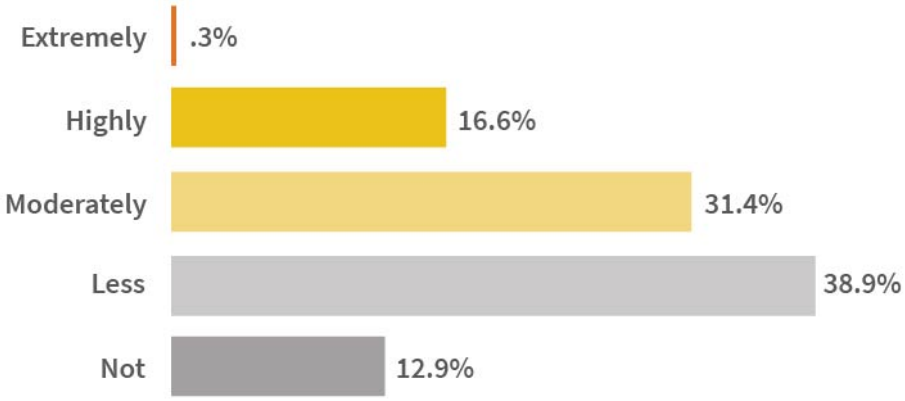
Advisory criticality: All products

16.6% of vulnerabilities in 2017 were rated as *Highly Critical*, and 0.3% as *Extremely Critical*.

There were no notable changes in criticality levels between 2016 and 2017.

Figure 4

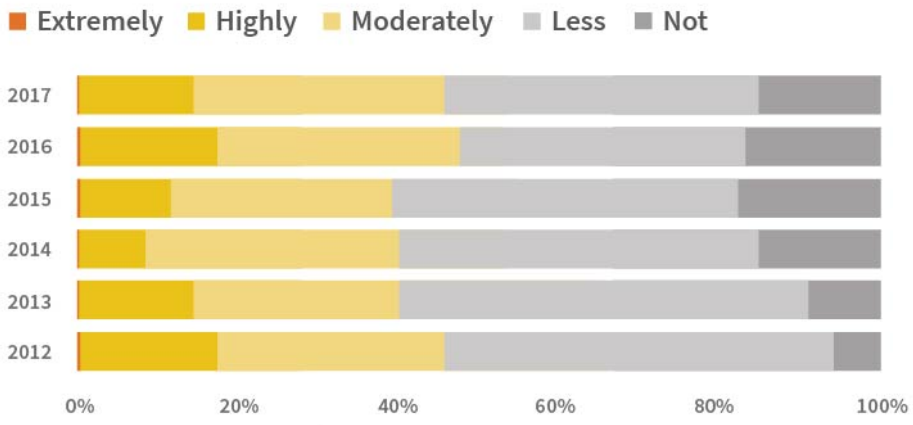
ADVISORY CRITICALITY BREAKDOWN



 | *Source: Vulnerability Review 2018*

Figure 5

CRITICALITY OF PORTFOLIO VULNERABILITIES



 | *Source: Vulnerability Review 2018*

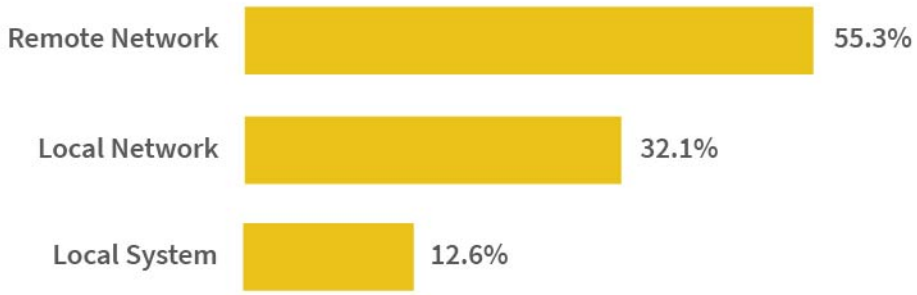
Attack vector: All products

With a 55.3% share, the primary attack vector used to trigger a vulnerability for all products in 2017 was again via remote network. This is a slight drop from 55.9% in 2016. The fact that over half of all vulnerabilities could be exploited remotely is an element of concern for the security of systems.

The proportion of vulnerabilities with attack vector “local network” has increased, from 31.5% in 2016, to 32.1% in 2017. ”Local system” remained at the same level (12.6%) in 2017.

Figure 6

ATTACKS BY VECTOR



 | *Source: Vulnerability Review 2018*

Time-to-Patch

In 2017, 86% of all vulnerabilities had a patch available on the day of disclosure—slightly higher compared to 81% in 2016.

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

It's, 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 2017 time-to-patch results show that 14% of all vulnerabilities were without patches for longer than the first day of disclosure.

This percentage is a representative proportion of software products that aren't patched immediately, 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), 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.

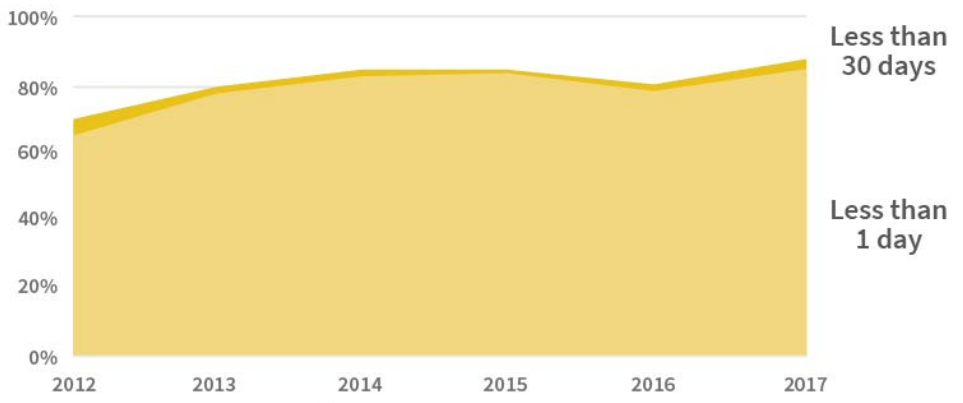
Cooperation between vendors and researchers

That 86% of vulnerabilities in all products, in our database 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 71% recorded in 2012. The most likely explanation for the continuously improving time-to-patch rate is that researchers continue to coordinate their vulnerability reports with vendors and vulnerability programs, resulting in immediate patch availability for the majority of cases.

30 days after the day of disclosure, 87% of vulnerabilities have a patch available. If a patch is not available on the first day, the vendor doesn't prioritize patching the vulnerability.

Figure 7

PATCH AVAILABILITY FOR VULNERABILITIES IN ALL PRODUCTS, HISTORICALLY



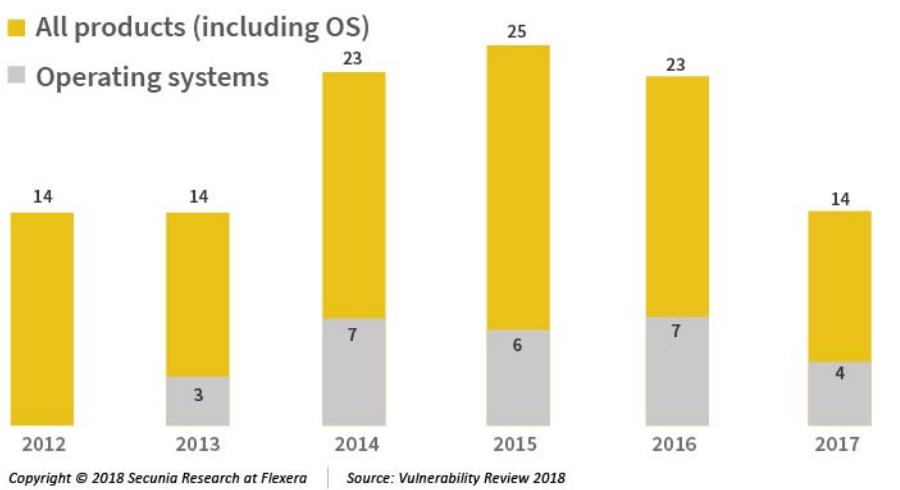
 | Source: Vulnerability Review 2018

Zero-Day Vulnerabilities

The number of zero-day vulnerabilities discovered in 2017 decreased compared to 2016, with 14 zero-day vulnerabilities in all products in 2017, compared to 23 in 2016.

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

Figure 8



Appendix & Glossary

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 Common Vulnerabilities and Exposures (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 than expected vulnerability counts when basing

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.

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 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 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).

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 view the software industry as a supply chain, and make the business of buying and selling software and technology asset data more profitable, secure, and effective. Our Monetization and Security solutions help software sellers transform their business models, grow recurring revenues and minimize open source risk. Our Vulnerability and Software Asset Management (SAM) solutions strip waste and unpredictability out of procuring software, helping companies buy only the software and cloud services they need, manage what they have, and reduce compliance and security risk. Powering these solutions and the entire software supply chain, Flexera has built the world's largest and most comprehensive repository of market intelligence on technology assets. In business for 30+ years, our 1200+ employees are passionate about helping our 80,000+ customers generate millions in ROI every year. Visit us at www.flexera.com.

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