VULNERABILITY REVIEW 2020

GLOBAL TRENDS

KEY FIGURES AND FACTS ON VULNERABILITIES FROM A GLOBAL INFORMATION SECURITY PERSPECTIVE

FLEXERA™

Re-use

We encourage the re-use of data, charts and text published in this report under the terms of this Creative Commons Attribution 4.0 International License.

You are free to share and make commercial use of this work as long as you attribute the Vulnerability Review 2020 as stipulated in the terms of the license.

Introduction to the Vulnerability Review 2020 – 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, exploits, 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 62,000 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 environments. The Secunia Advisory descriptions include criticality, attack vector, exploitability 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 in which the vulnerability appears. 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 media

Every year, it seems that new exploitations of known software vulnerabilities are making global headlines. In 2017, we saw the WannaCry attacks and the Equifax breach, and 2019 included the Capital One and First American data breaches. They're becoming so common that it is no longer a question of if, but when will our vulnerabilities be attacked. It is more important than ever to stay on top of these exposures as they proliferate—from the simplest patches to the migration of servers.

As the costs of exposures continue to rise, businesses are tasked with ongoing efforts towards identifying and mitigating the exploitation risk of software vulnerabilities.

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

Increased attention on vulnerability management has revealed:

- Many organizations still don't have processes and procedures in place to reduce system vulnerabilities

- A gap remains between identifying vulnerable applications and fixing them, which 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 it isn't process-driven. So much effort is required 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 starts a new fire.

In light of the surge in exploitation of unpatched vulnerabilities, we see increased 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 2020 – Global Trends provides data on vulnerabilities, enabling you to understand the vulnerability landscape and devise strategies to secure what matters for your business.

Out of 2,867 advisories, 53.09 percent contained vulnerabilities that have already been exploited. Since more than half of all known advisories provided by Secunia Research contained exploited vulnerabilities, it's all the more important to prioritize mitigation efforts with threat intelligence.

More than 80 percent of vulnerabilities have patches available on the day of disclosure. This confirms 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: 20 out of 13,319. This highlights the fact there is time to remediate most vulnerabilities before exploitation risk increases.

Source: Flexera Vulnerability Review 2020

Vulnerability update by the numbers

Vulnerabilities detected: All products

The absolute number of vulnerabilities detected was 13,319, which were discovered in 1,607 applications from 249 vendors. This shows a 23.06 percent decrease in the five-year trend and a 22.37 percent decrease from 2018 to 2019.

Since 2018, the number of vendors behind the vulnerable products has increased by 3.32 percent and the number of vulnerable products has decreased by 9.62 percent.

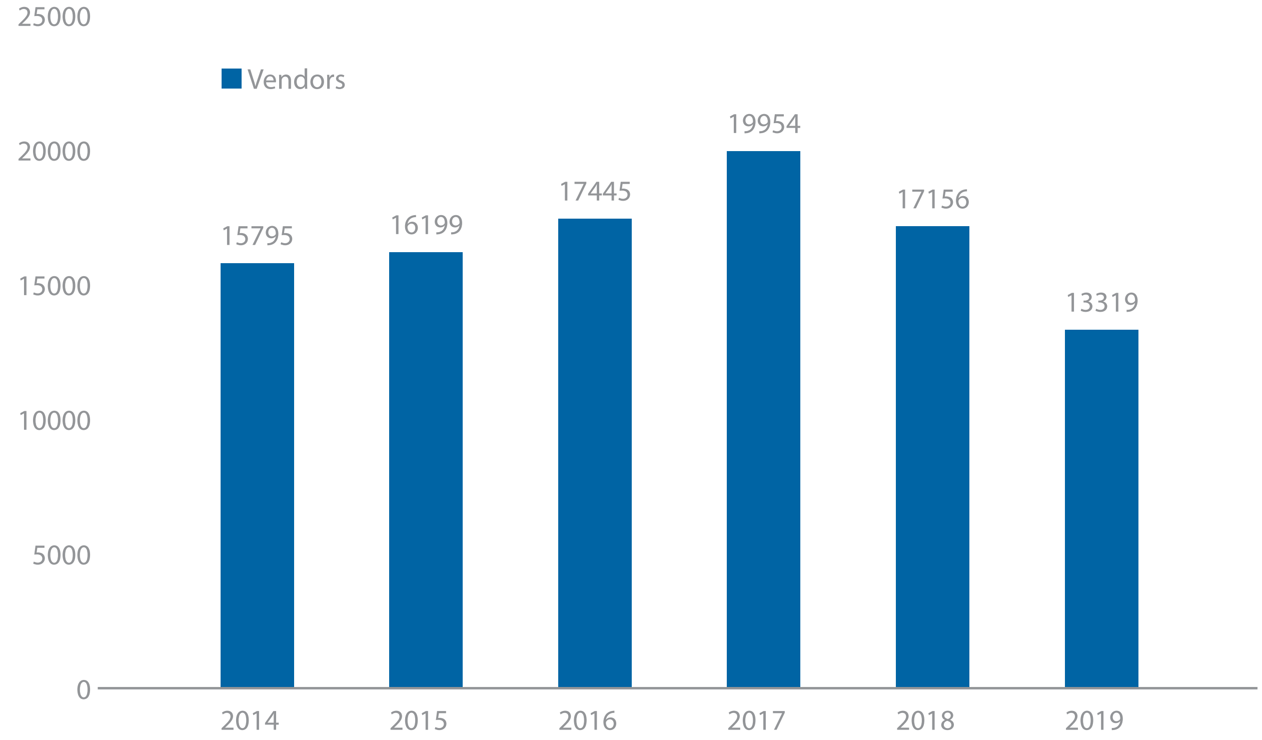
As a result, a number of products and vendors not used in customer environments are no longer tracked systematically.

The substantial drop in numbers of products during 2018 and 2019 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 and not an indicator of a change in the security landscape.

	Secunia Advisories	Vulnerability Count	Vendors	Products
Averages 2014-18	3503	17310	311	2439
Total 2019	2867	13319	249	1607
Change (past 5 years)	-18.16%	-23.06%	-19.94%	-34.12%
Change (2018 to 19)	-9.19%	-22.37%	3.32%	-9.62%

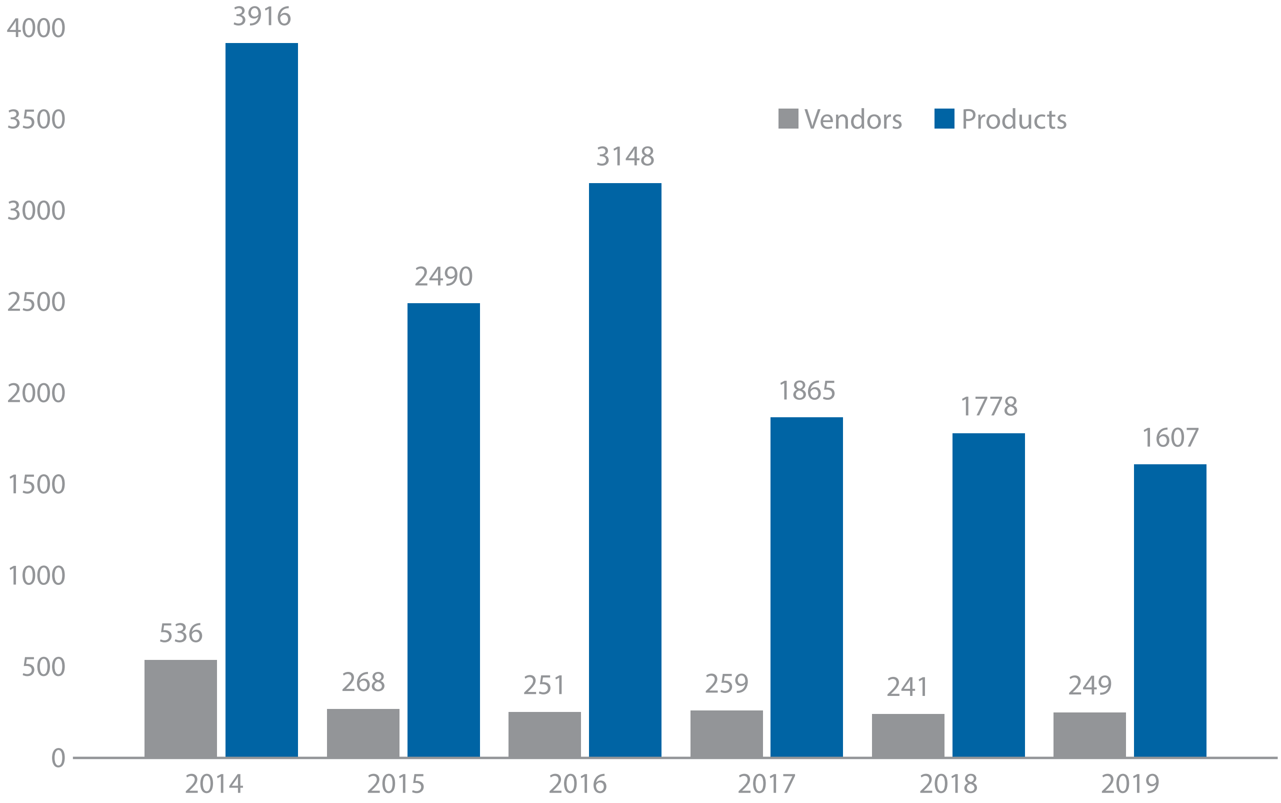
Source: Flexera Vulnerability Review 2020

Global Vulnerabilities Reported For All Products of All Vendors



Source: Flexera Vulnerability Review 2020

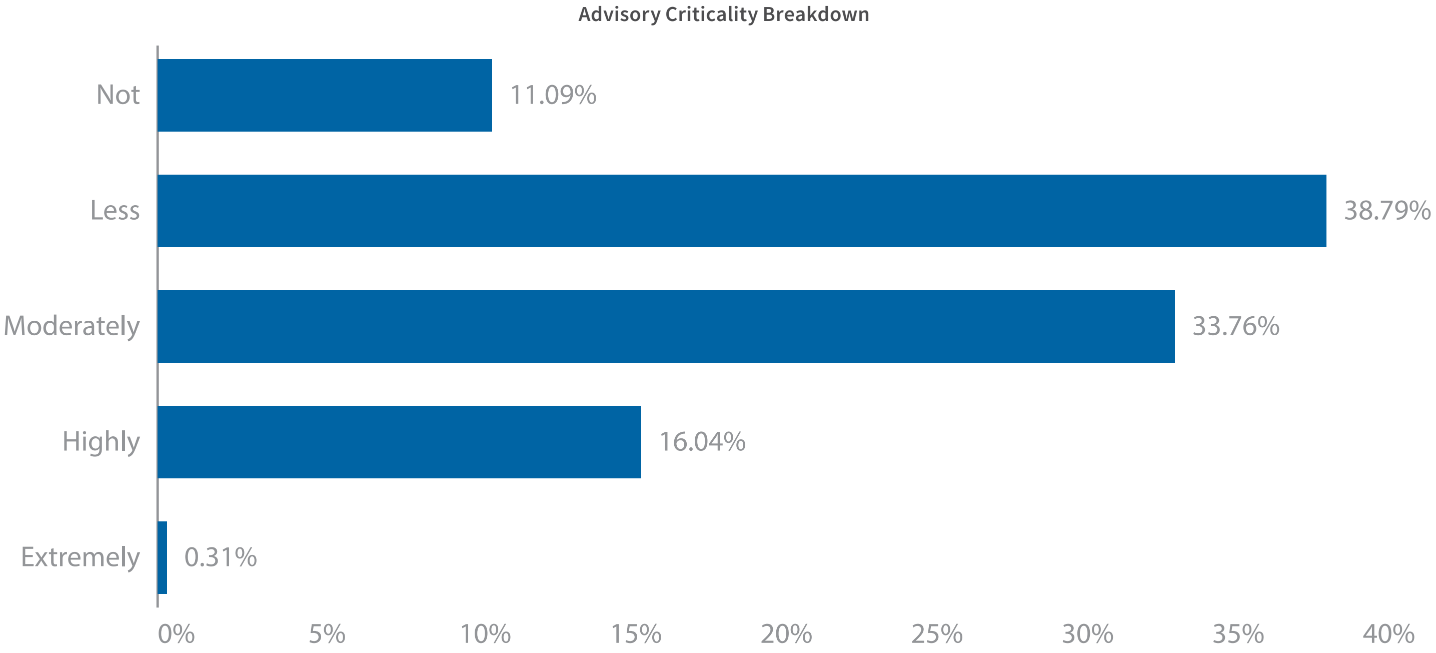
Vulnerable Products and Vendors



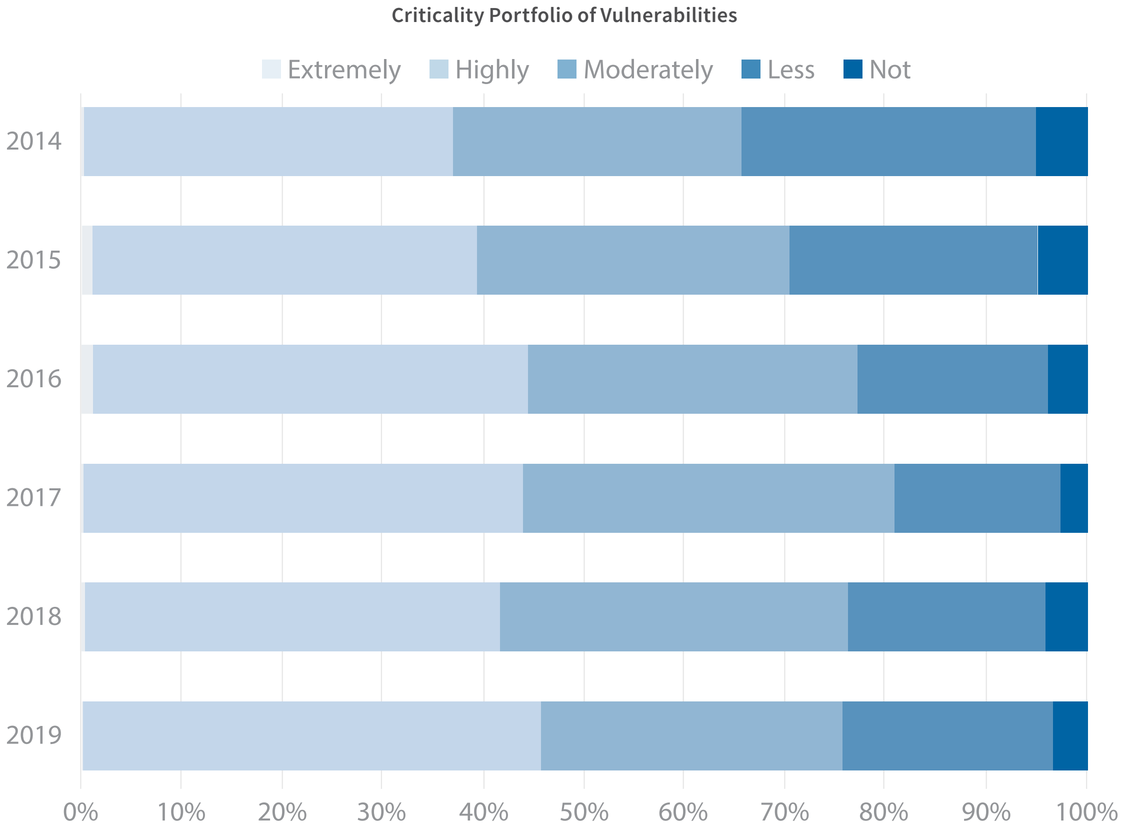
Source: Flexera Vulnerability Review 2020

Advisory criticality: All products

16.04 percent of vulnerabilities in 2019 were rated as highly critical, and 0.31 percent as extremely critical. There were minimal increases in advisory criticality between 2018 and 2019.



Source: Flexera Vulnerability Review 2020



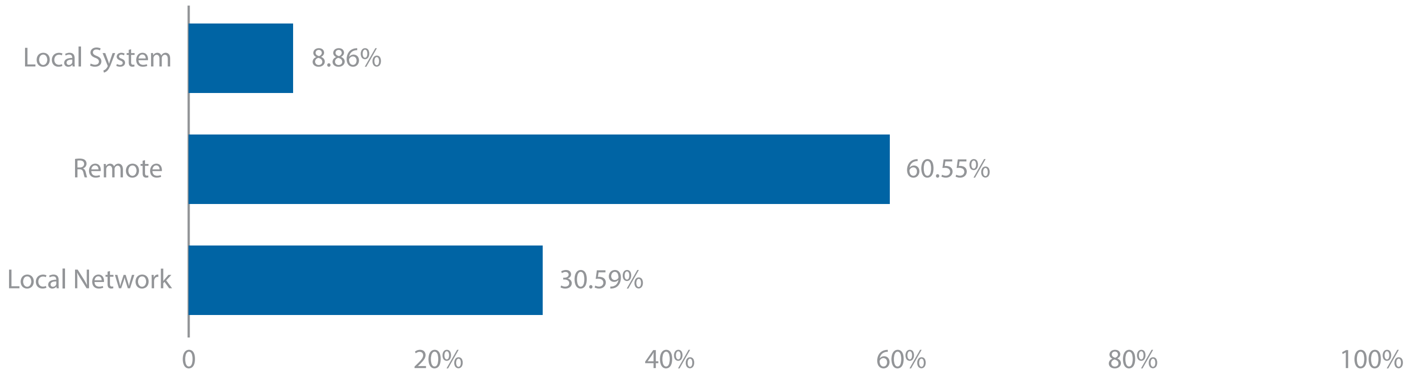
Source: Flexera Vulnerability Review 2020

Attack vector: All products

With a 60.55 percent share, the primary attack vector used to trigger a vulnerability for all products in 2019 was again via remote network. This is a slight increase of 5.25 percent since 2018. 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 decreased, from 32.94 percent in 2018, to 30.59 percent in 2019. Local system decreased by 1.09 percent (to 8.86 percent of all vulnerabilities) in 2019.

Attacks by Vector



Source: Flexera Vulnerability Review 2020

Time-to-patch

In 2019, 83.9 percent of all vulnerabilities had a patch available on the day of disclosure—slightly lower compared to 84.43 percent in 2018. In the case of Secunia advisories, patches were available for 80.75 percent of advisories at the time of release, an increase from 79.28 percent in 2018.

The 2019 results remain positioned at the high end of the scale, indicating that it is still possible to remediate the majority of vulnerabilities.

It is 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 2019 time-to-patch results show that 16 percent of all vulnerabilities were without patches for longer than the first day of disclosure.

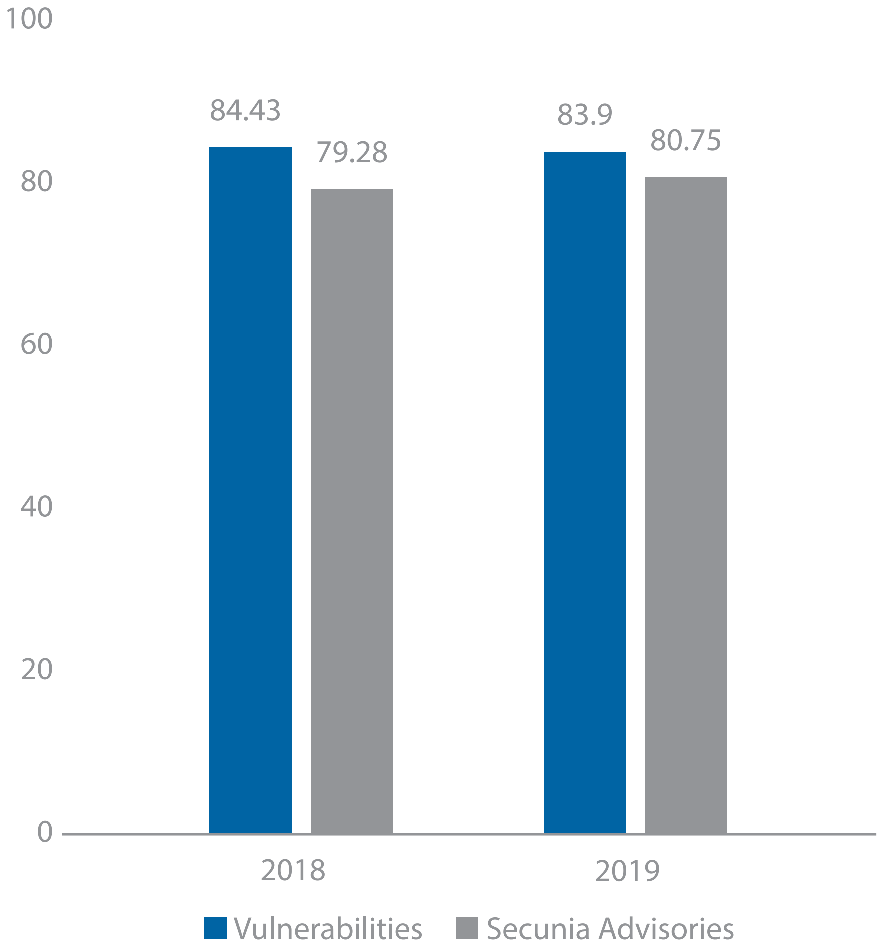
This percentage is a representative proportion of software products that aren’t patched immediately due to a lack of vendor resources, uncoordinated releases or—more rarely—zero-day vulnerabilities.

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 the first day of disclosure means a variety of mitigating efforts are required to ensure sufficient protection in support of patch management efforts.

Cooperation between vendors and researchers

The fact that 83.9 percent 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 that includes a low of 71 percent 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.

Patch Availability on Day of Disclosure

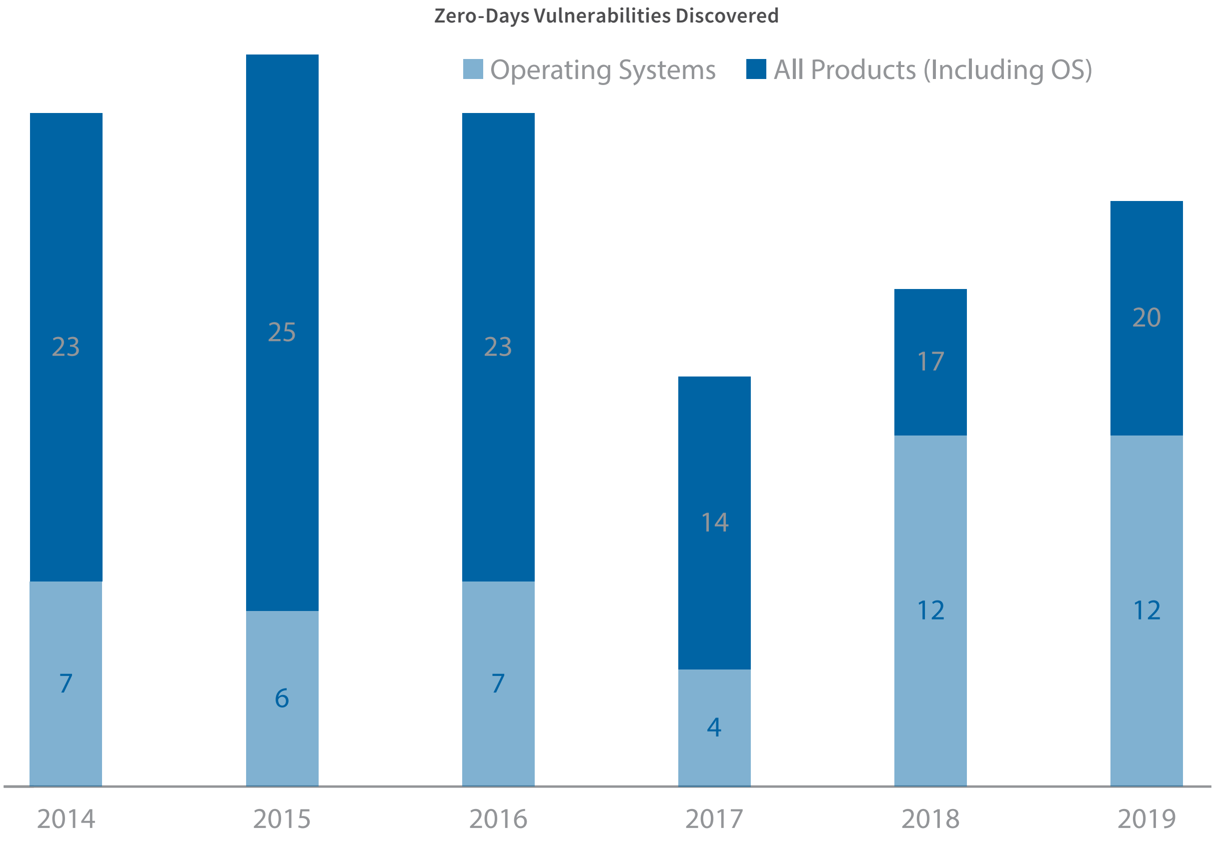


Source: Flexera Vulnerability Review 2020

Zero-day vulnerabilities

The number of zero-day vulnerabilities discovered in 2019 increased compared to 2018, with 20 zero-day vulnerabilities in all products in 2019, compared to 17 in 2018.

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



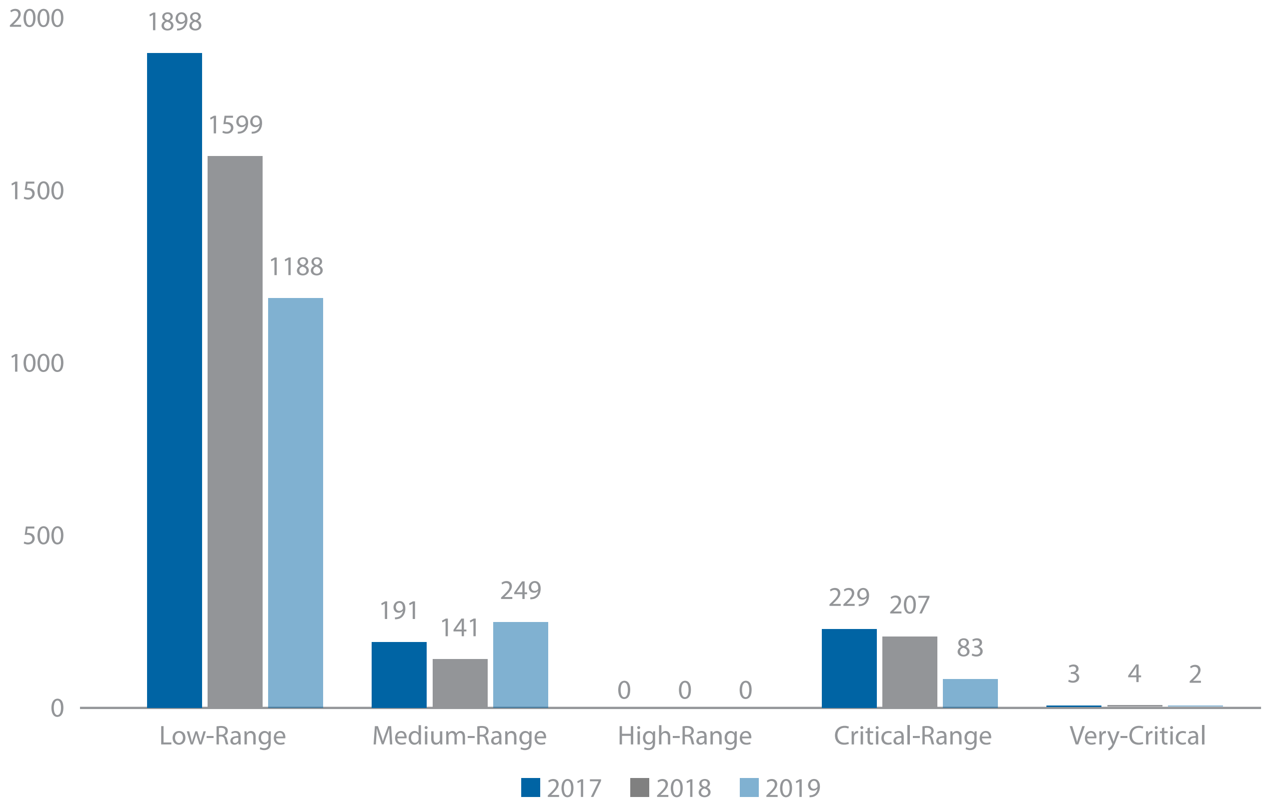
Source: Flexera Vulnerability Review 2020

Prioritizing with threat intelligence

Threat intelligence raises a team's ability to focus on vulnerabilities that matter most by exposing which of them are actually being exploited in the wild.

Of vulnerabilities exploited in 2019, 53.09 percent included a positive threat score vs. 46.91 percent of those that were exploited without a threat score. It's important to note that vulnerability scoring is separate from whether or not the exposure is likely to be exposed. What this number tells us is that if the vulnerability were to be exploited, what would be the level of damage inflicted from an exploit.

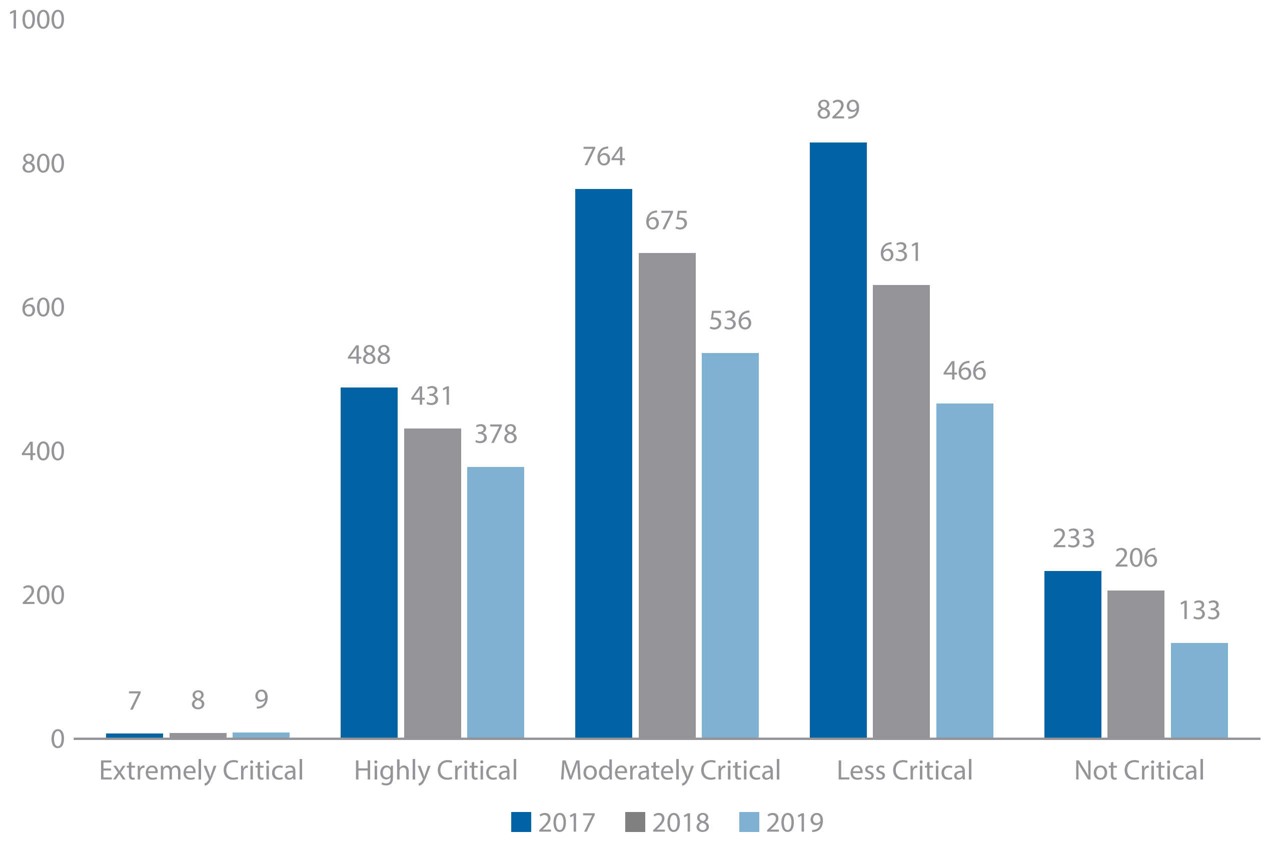
Vulnerabilities Exploited by Threat Score



Source: Flexera Vulnerability Review 2020

The number of exploits by advisory criticality showed that 78.06 percent of vulnerabilities exploited in 2019 were from low-range threat scores. Many programs focused solely on high-range to very critical threat scores would have missed out on the majority of vulnerabilities in need of remediation by simply overlooking low-range scores.

Number of Exploits by Advisory Criticality



Source: Flexera Vulnerability Review 2020

At 18.70 percent and 16.25 percent, exploits by advisory criticality was highest at the moderately critical and less critical levels for advisories in 2019. Similar to low-range criticalities with exploits by advisory, exploits tend to live in the lower ranges where teams are focusing less attention.

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.”

Localsystem

Localsystem describes vulnerabilities where the attacker is required to be a local user on the system to trigger the vulnerability.

From local network

From local network describes vulnerabilities where the attack vector requires an attacker to be situated on the same network as a vulnerable system (not necessarily a LAN).

This category covers vulnerabilities in certain services such as DHCP, RPC and administrative services, which should not be accessible from the Internet, but only from a local network and optionally a restricted set of external systems.

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

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 vulnerability that is actively exploited by hackers before it's publicly known.

NEXT STEPS

For more information on how we can help you defend against vulnerabilities, visit us online.

LEARN MORE

ABOUT FLEXERA

Flexera helps executives succeed at what once seemed impossible: getting clarity into, and full control of, their company's technology "black hole." From on-premises to the cloud, Flexera helps business leaders turn IT insight into action. With a portfolio of integrated solutions that deliver unparalleled technology insights, spend optimization and agility, Flexera helps enterprises optimize their technology footprint and realize IT's full potential to accelerate their business. For over 30 years, our 1300+ team members worldwide have been passionate about helping our more than 50,000 customers fuel business success. To learn more, visit **flexera.com**