FLEXERA™ 2022
Software Vulnerability and Threat Intelligence Report

Jeroen Braak
Based on data from Secunia Research

flexera™

Reuse

Contents

Introduction

This *Flexera 2022 Software Vulnerability & Threat Intelligence Report* is based upon data from the Flexera Secunia Research Team who produces valuable advisories leveraged by users of Flexera's Software Vulnerability Research and Software Vulnerability Manager solutions.

The report analyzes the evolution of software security from a vulnerability, threat intelligence and patch perspective.

The report presents global data on the prevalence of vulnerabilities, exploits, the availability of patches and maps the security threats to IT infrastructures.

What does the report cover?

The annual Vulnerability Review is based on data from Flexera's Secunia Research. Secunia Research monitors more than 66,000 applications, appliances and operating systems, and tests and verifies the vulnerabilities reported in them.

The systems and applications monitored by Secunia Research are in use in the environments of the customers of Flexera 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.

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 to author security advisories which provide valuable details by following consistent and standard processes that have been refined over the years.

Whenever a new vulnerability is reported, it's verified and a Secunia Advisory is published. A Secunia Advisory provides details, including description of the vulnerability, risk rating, impact, attack vector, recommended mitigation, credits, references and more, including additional details discovered during verification and testing, thus providing the information required to make appropriate decisions about how to protect systems.

Click here to learn more about Secunia Advisories and their contents.

2022 summary

Total advisories: **7,097** ↑ **(2021 : 6,153)**

2022 was a busy year for cybersecurity, a record-breaking number of advisories were reported, and many significant vulnerabilities were the cause of data breaches, ransomware attacks and other types of threats.

Top 3 most critical vulnerabilities:

1. **Log4Shell/Log4j** (CVE-2021-44228), even with its disclosure in December 2021, many organizations are still struggling to identify and patch the vulnerability.
2. **Spring4Shell** (CVE-2022-22965), still many systems remain unpatched despite the risk.
3. **ProxyNotShell** (CVE-2022-41040 and CVE-2022-41082) in Exchange

Interesting facts and trends:

- **2022** is the year with the **most** recorded Secunia Advisories since 2002
- Average **threat score** of 2022: **13.66** (click here to learn how we calculate this)
- Average **CVSS3 score** of 2022: **7.35**
- Fewer **extreme critical** advisories have been reported in 2022: **44 (**2021: 60)
- **85** advisories reported a **zero-day** vulnerability (2021: 81)
- More than **50 percent** of all **advisories** are for vulnerabilities in **Unix/Linux** operating systems
- More than **50 percent** of all **rejected advisories** are also for **Unix/Linux** operating systems
- Almost **79 percent** of all **networking**-related advisories are for **Cisco, NetApp** and **Juniper**
- About Microsoft:
  - **Four percent** of all **advisories** were for **Microsoft**, which put them in **eighth place** in vendor ranking
  - More than **56 percent** of all **zero-days** were related to **Microsoft** products (**first place**).
- **None** of the top four vendors with the most advisories (**SUSE, IBM, Red Hat, Ubuntu**) had any **zero-day** reported in 2022

- **Log4j:**
  - **131** advisories were related to **Log4j**
  - Last advisory was released in November (**eleven months later**) for **IBM Security QRadar SIEM 7.x**
    62 Log4j related advisories were linked to **IBM products**
    33 of them were rejected advisories for various reasons, including "the respective product does not have the vulnerable log4j component..."
- Less than **11 percent** of all advisories had a high to critical threat score which means that there was evidence of exploitation
  - Using threat intelligence will help you prioritize what needs immediate **patching**

Software Vulnerability and Patch Management are becoming increasingly important. Due to the ongoing Russia-Ukraine conflict, attacks on critical infrastructures in many countries are increasing. Back in 2019 (just before COVID-19), patching was recommended within 30 days (or 14 days for CVSS score of seven or higher). Right now, hackers can deploy exploits **within one week** and even within **24 hours**. This means organizations need even better prioritization to quickly patch vulnerabilities (especially those with associated threats).

Advisories breakdown

Compared to previous years

2022 total advisory count: **7,097 ↑ (2021 : 6,153)**

As expected, 2022 had the highest number of advisories since Secunia started writing these.

#	Year	# of advisories
1	2022	7097
2	2020	7065
3	2016	6348
4	2017	6262
5	2021	6153
6	2018	6101
7	2014	6004
8	2015	5934
9	2019	5837
10	2006	5262

Figure 1: Top ten years with most advisories

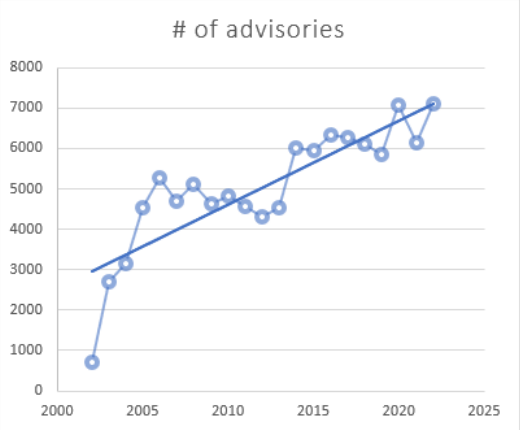
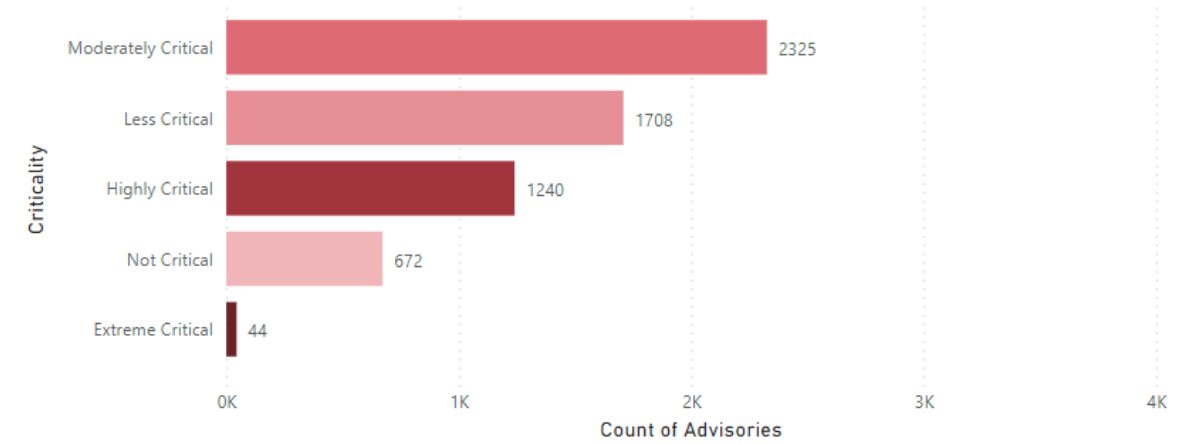


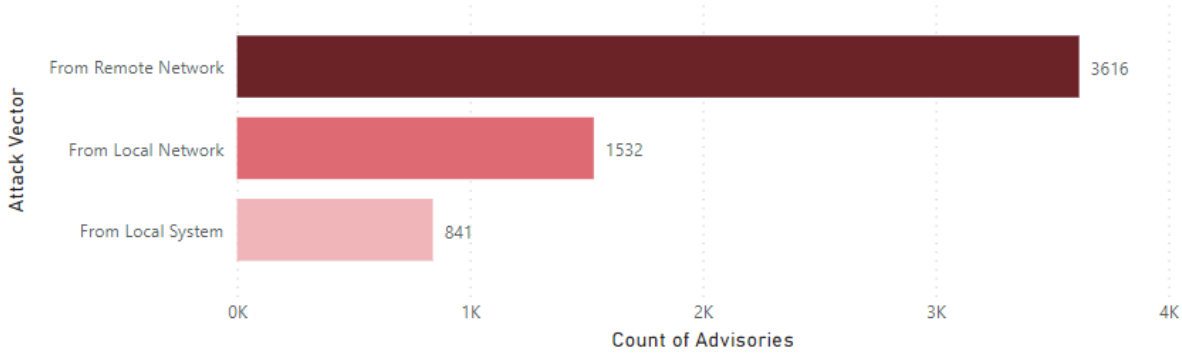
Figure 2: Chart with advisory trendline over the years

This year:	#	Change (last year)
Total # of advisories	7,097	↑ (6,153)
Unique vendors	279	↑ (263)
Unique versions	1,801	↑ (1,784)
Rejected advisories *	1,108	↑ (1,042)
		↑ increased ↓lower ↔ same

1,108 advisories *have received the "rejected" status which means in general that the vulnerability requires one or more violations of security best practices (e.g., product not securely configured or not used securely) or that it was "too weak of a gain" (e.g., administrative, local users already being too privileged so that additional gain becomes neglectable).*

Advisory criticality and attack vector





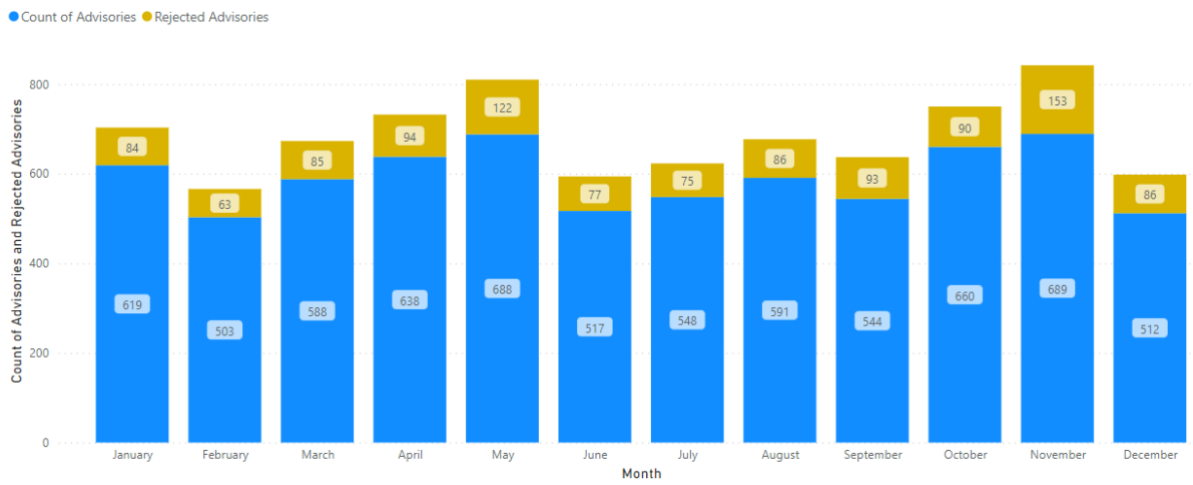
More information about the variables used in the above charts:

Attack vector (from where)

Criticality (severity)

Though not in the chart, Secunia Research also provides information about the **impact** or **consequence** when a vulnerability has been exploited. There are twelve values that can be used (most advisories have one or more). Read more here.

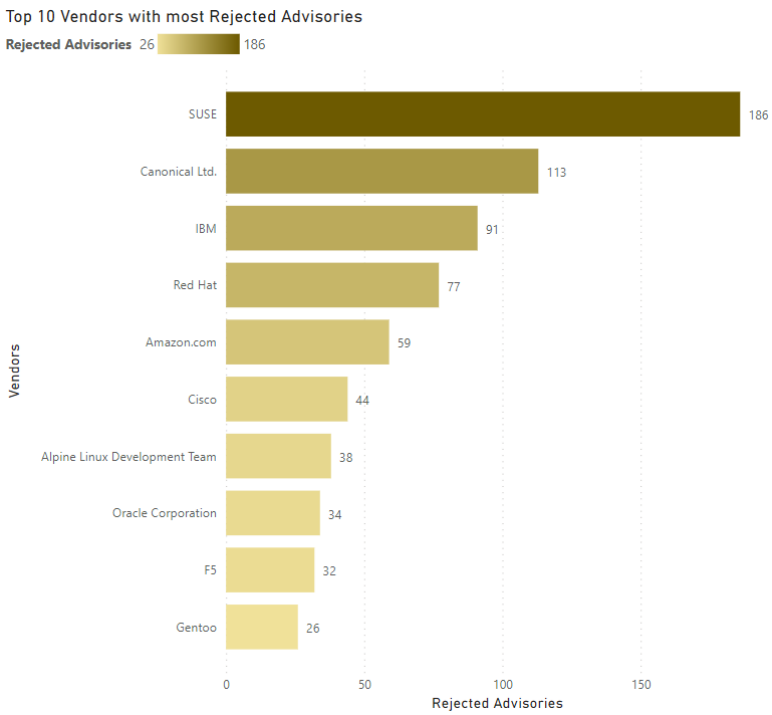
Advisories and rejected advisories

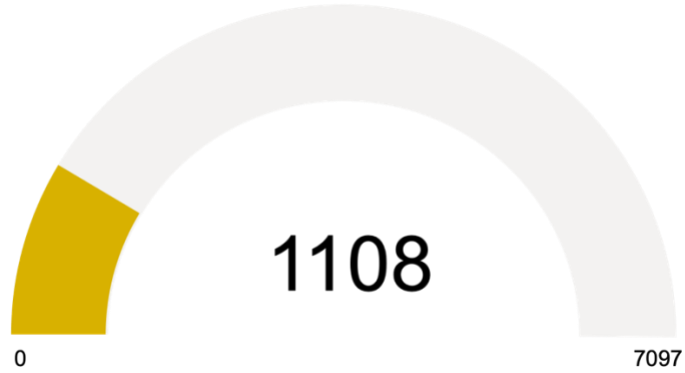


Rejected advisories

There are a lot of vulnerabilities posted to the National Vulnerability Database, by a lot of people and companies. They're not always valid, they're not always assigned proper criticality, and in some cases, a vulnerability may be legitimate but not provide the attacker any benefit.

The Flexera Secunia Research team evaluates vulnerabilities from hundreds of sources, rescores them when necessary and even rejects vulnerabilities not worth your attention. Rejection advisories help you reduce the volume of vulnerabilities to be mitigated by helping you focus only on those that present reasonable risk to your environment.





An advisory may be rejected for many reasons; the most common are:

- **No reachability**
  The vulnerability cannot be exploited because the affected systems cannot be reached by an attacker.
- **No gain**
  The vulnerability may be reached, but without any gain for the attacker.
- **No exploitability**
  The vulnerability cannot be exploited because, for example, policy forbids installation of the affected software.
- **Dependent on other**
  The vulnerability cannot be exploited by itself but depends on another vulnerability being present.

Addressing awareness with vulnerability insights

Prevelance:

- How many systems would benefit from any given security update?
- Does it pose a risk? Is it on all systems? Patch

Asset sensitivity:

- What systems would result in the most risk if compromised?
- Is it a high-risk device? Patch

Criticality:

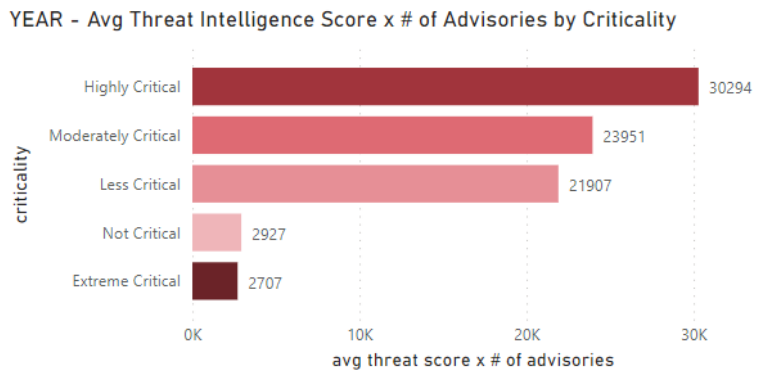
- The most popular method of thoughtful prioritization.
- If exploited, how bad could it affect your security?
  Is it designated to be of a high criticality? Patch

Threat intelligence:

- The newest and most impactful method focuses on the likelihood of exploitation.
- Is it likely to be exploited? Patch

How do we know that more insights/data is needed?

Focusing on advisories with CVSS 7 or higher would address about 50 percent of exploits. Most exploits are CVSS scored between four and seven. Focusing on vulnerabilities for the top 20 vendors would address only about 20 percent.



Take away 1:

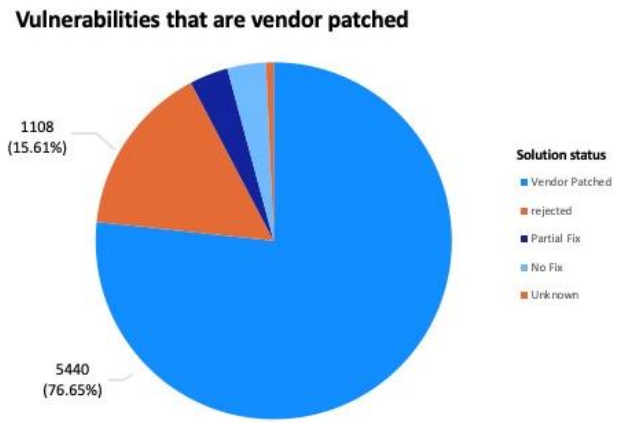
High and extreme critical advisories are not necessarily those presenting the most risk. Leverage threat intelligence to better prioritize what demands your most urgent attention. Create a scoring mechanism that considers multiple variables.

Secunia criticality	avg. cvss score	avg. threat score	# advisories
Extreme Critical	9.00	61.52	44
Highly Critical	9.31	24.43	1240
Less Critical	6.73	12.83	1780
Moderately Critical	7.42	10.30	2325
Not Critical	4.91	4.36	672
Total	**7.35**	**13.66**	**5989**

[More about Secunia Criticality (severity) scoring]

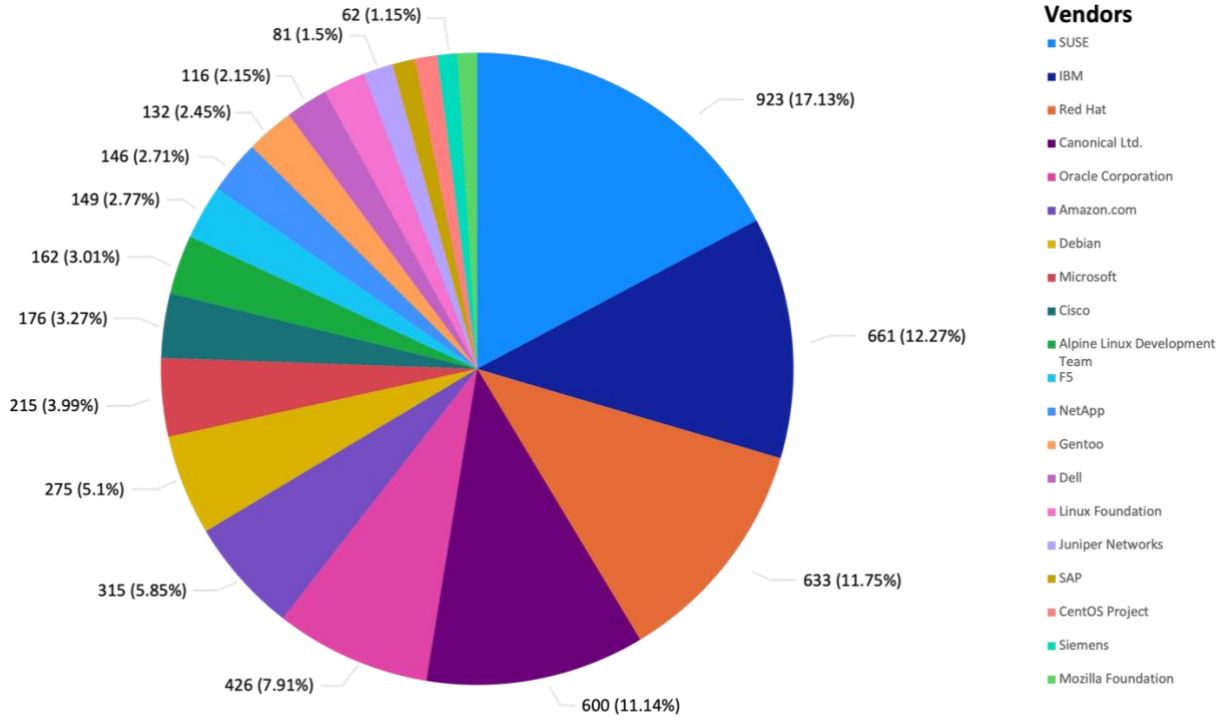
Take away 2:

Most vulnerabilities have a patch available (typically within 24 hours after disclosure).



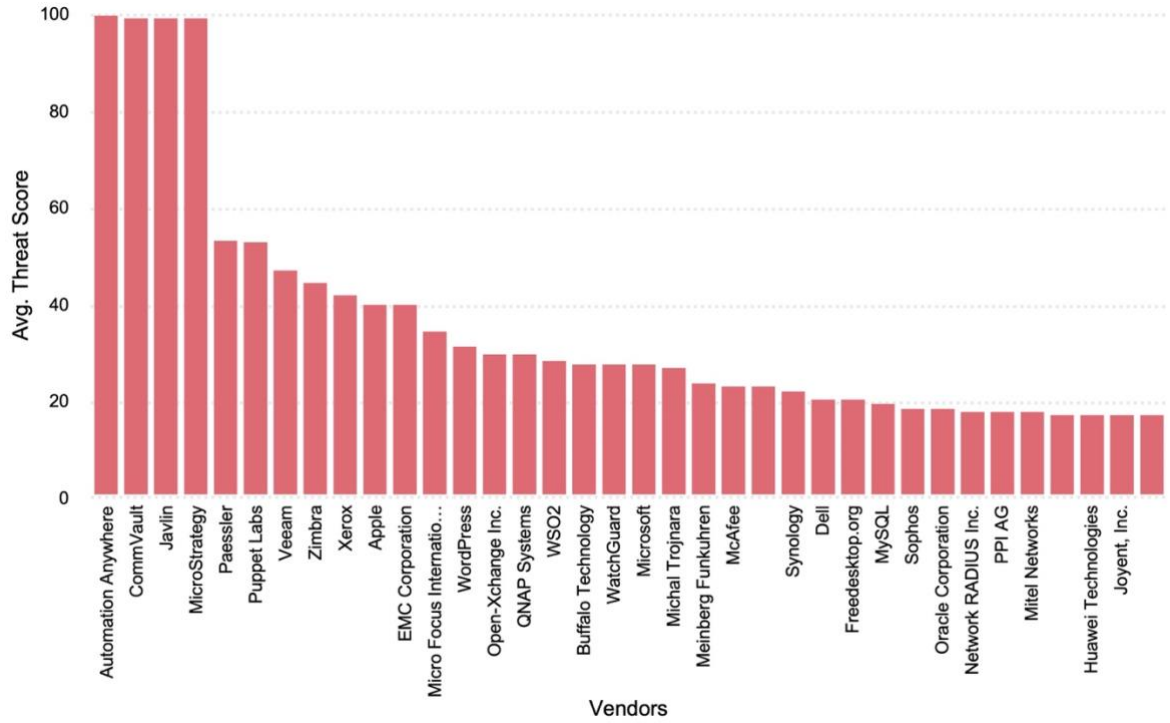
Vendor view

Top vendors with most advisories

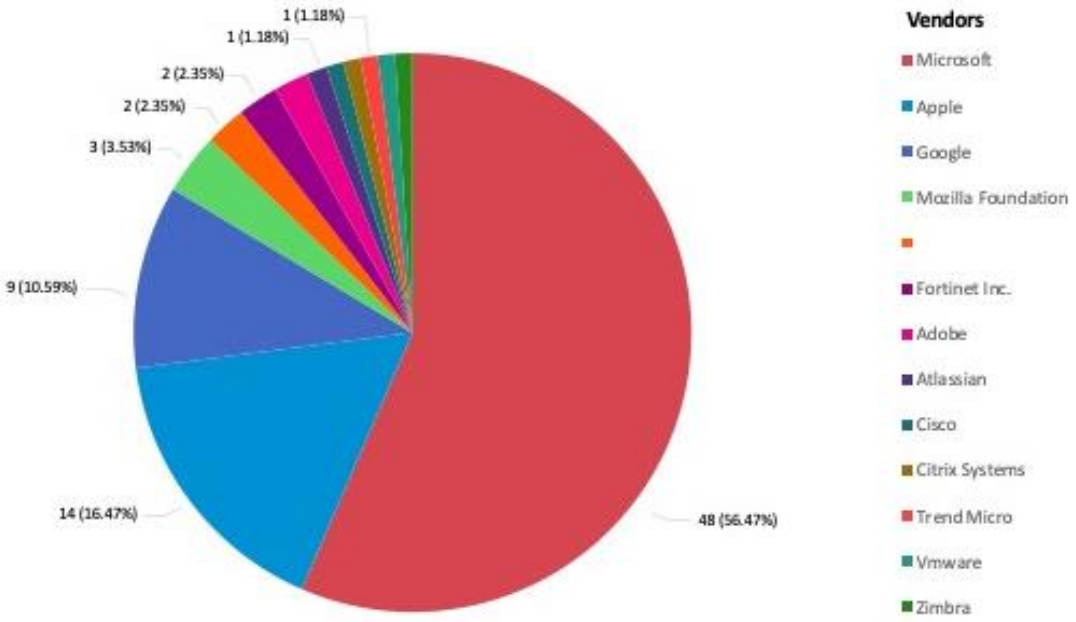


**Canonical Ltd. = Ubuntu*

Top vendors with highest average threat score



Top vendors with zero-days



Top ten products with the most zero-days reported in 2022

Place	# of Zero-days	Product family
1	38	Microsoft Windows
2	9	Google Chrome
3	9	Microsoft Edge (Chromium-Based)
4	7	Apple macOS
5	5	Apple iOS
6	2	Apple Safari
7	2	Mozilla Firefox
8	2	Fortinet FortiOS
9	1	Apex Central
10	1	Atlassian Confluence

Browser-related advisories

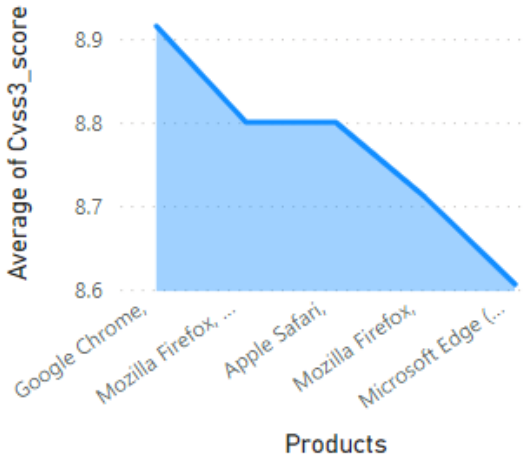
Advisories per browser

Products	Count of Advisories	avg. threat score	Avg. CVSS3 score
Google Chrome	33	18.94	8.92
Microsoft Edge (Chromium-Based),	33	18.55	8.61
Mozilla Firefox,	30	14.10	8.71
Apple Safari,	9	35.22	8.80
Mozilla Firefox, Mozilla Firefox,	1	6.00	8.80
Total	**7.35**	**13.66**	**5989**

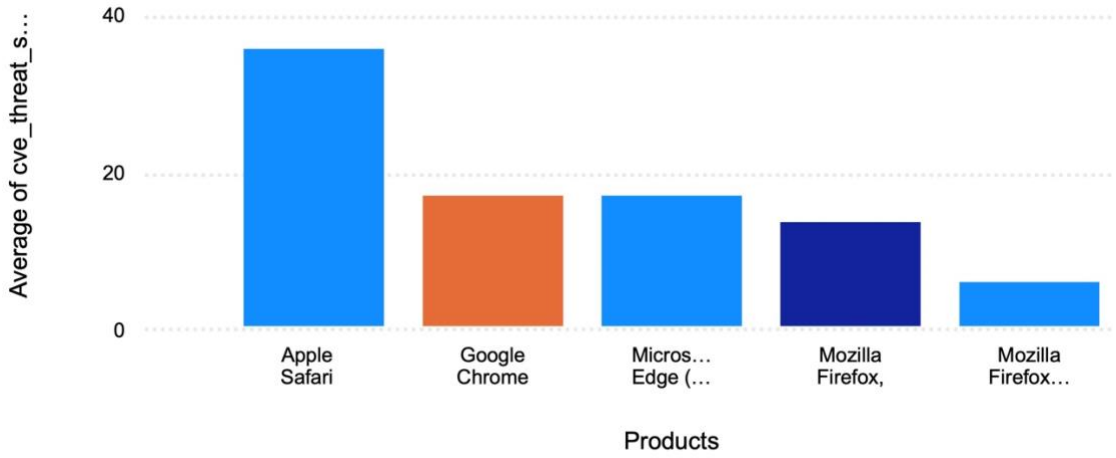
Browser zero-day vulnerabilities

Products	Count of Advisories
Google Chrome	9
Microsoft Edge (Chromium-Based),	9
Apple Safari,	2
Mozilla Firefox,	2
Total	**22**

Average CVSS (criticality) score per browser

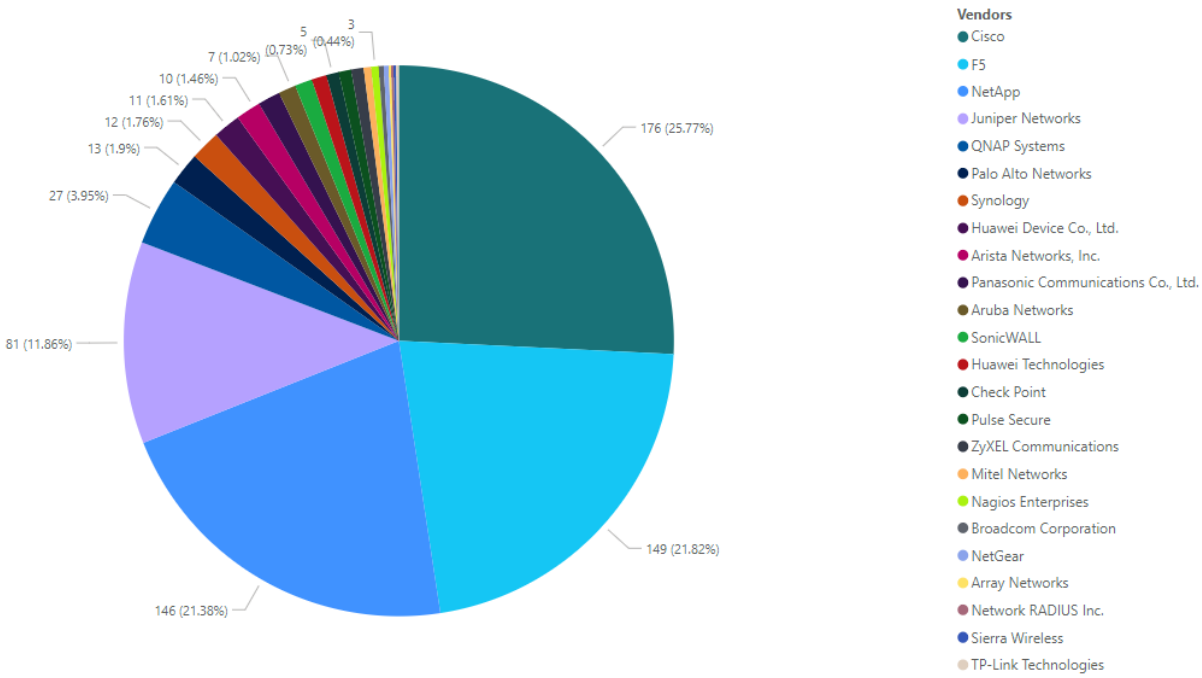


Average threat score per browser

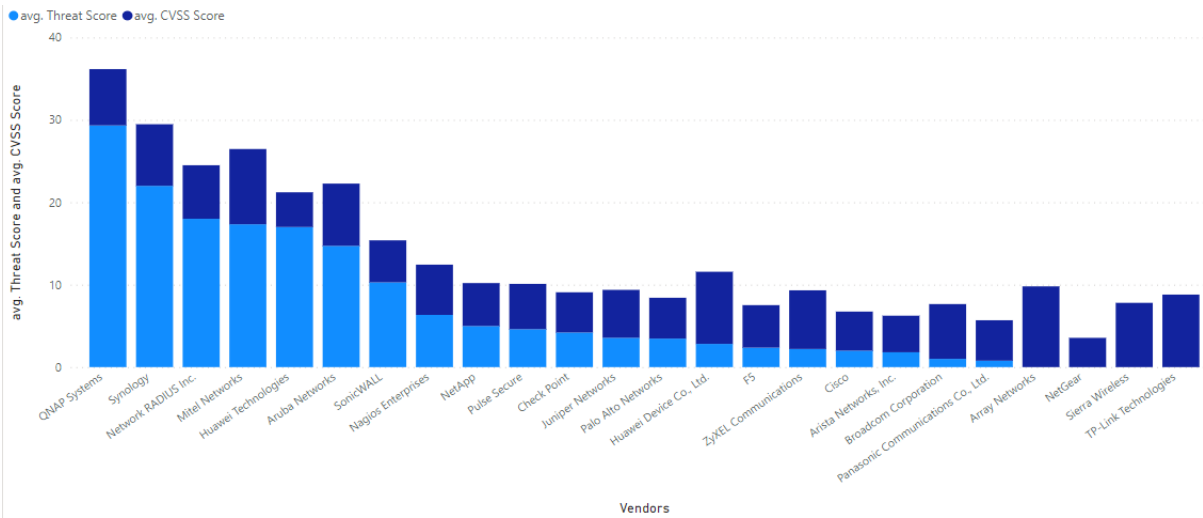


Networking-related advisories

Number of advisories per networking-related vendor



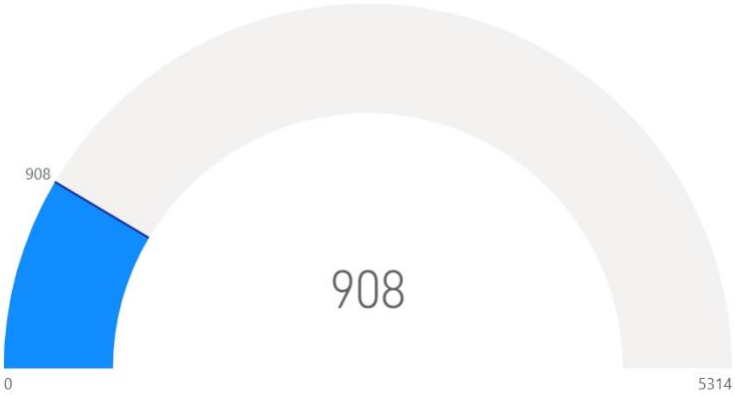
Average threat and CVSS score per networking-related vendor



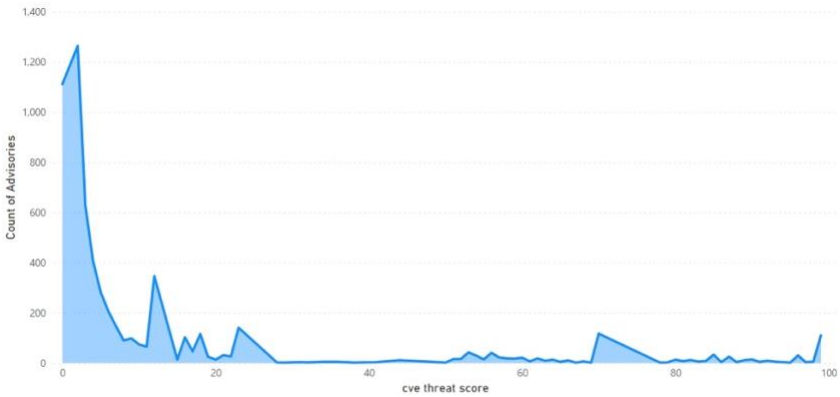
Threat intelligence

A look at threat intelligence-related data

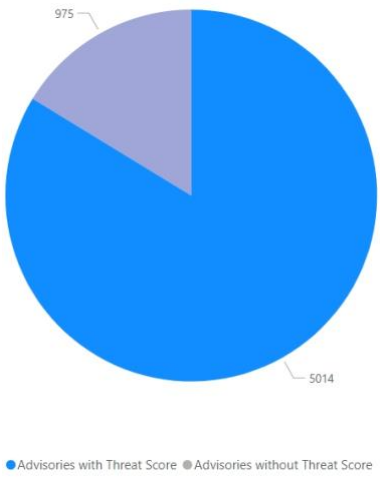
Count of malware-exploited CVEs



Count of advisories by CVE threat score

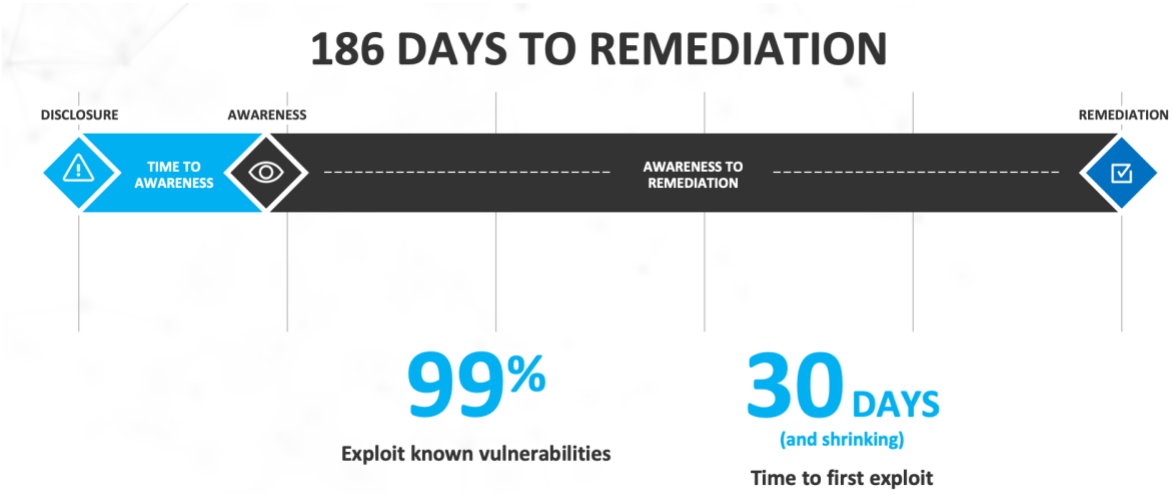


Threat intelligence advisory statistics:



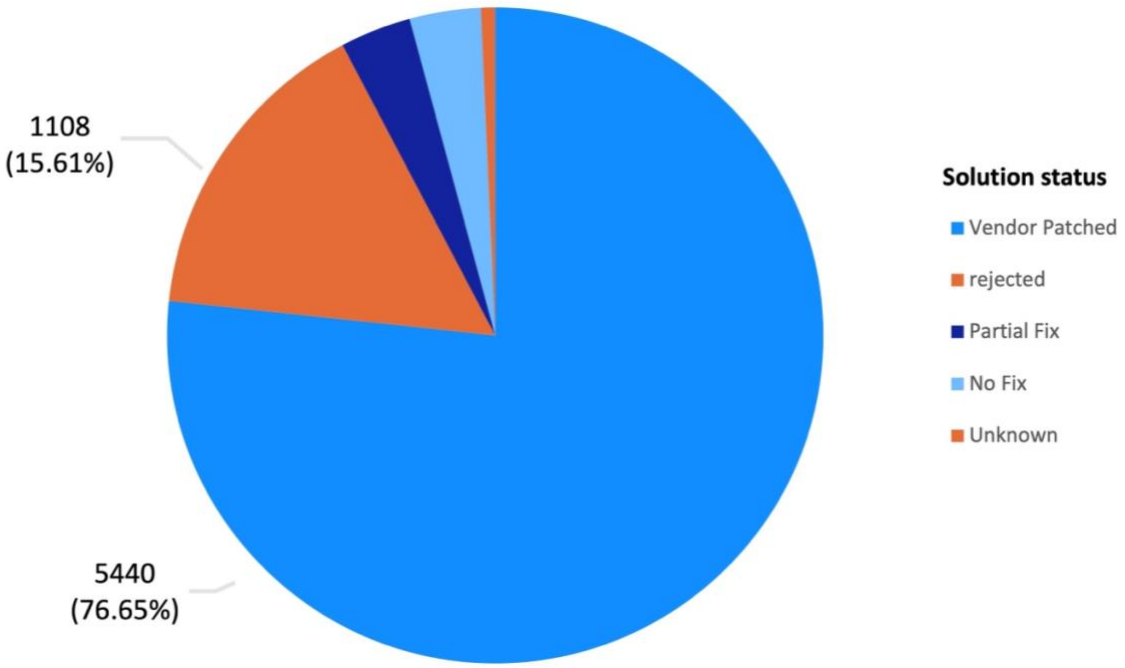
Patching

Most of 2022's vulnerabilities were vendor patched. In fact, most vulnerabilities are patched within 24 hours after disclosure.



The challenge remains that organizations don't have full visibility or awareness when a vulnerability is disclosed (time to awareness). Another big challenge is time to remediation (the time from having this information, correlating that with your environment and initiating the process to get the software updated to a secure version).

Vulnerabilities that are vendor patched

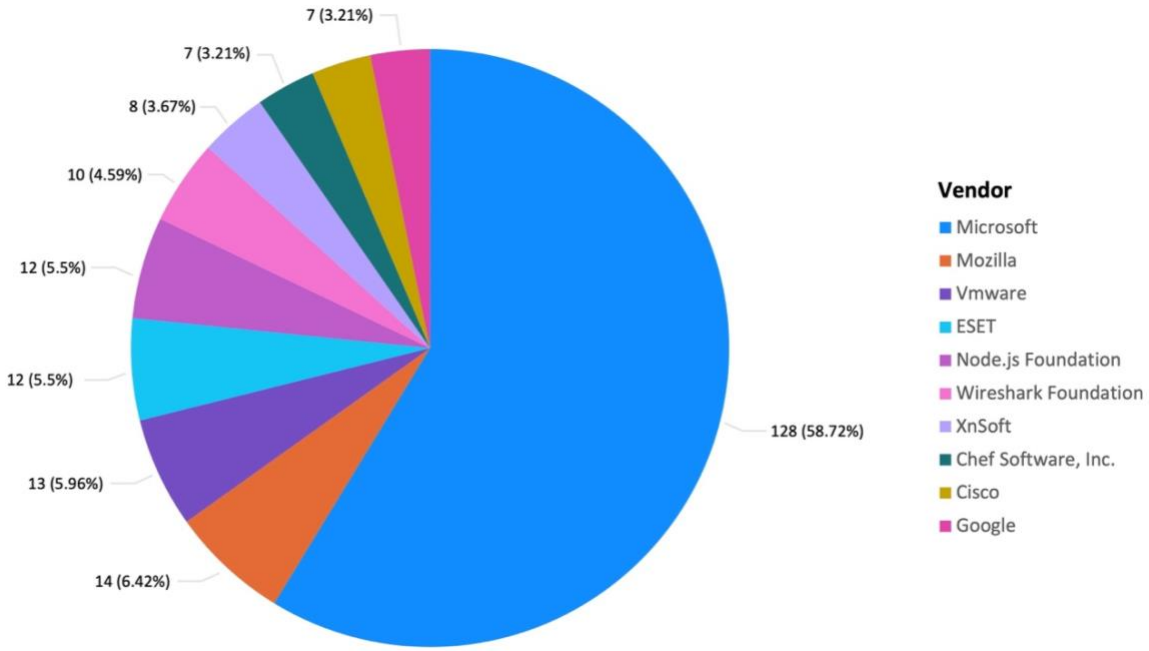


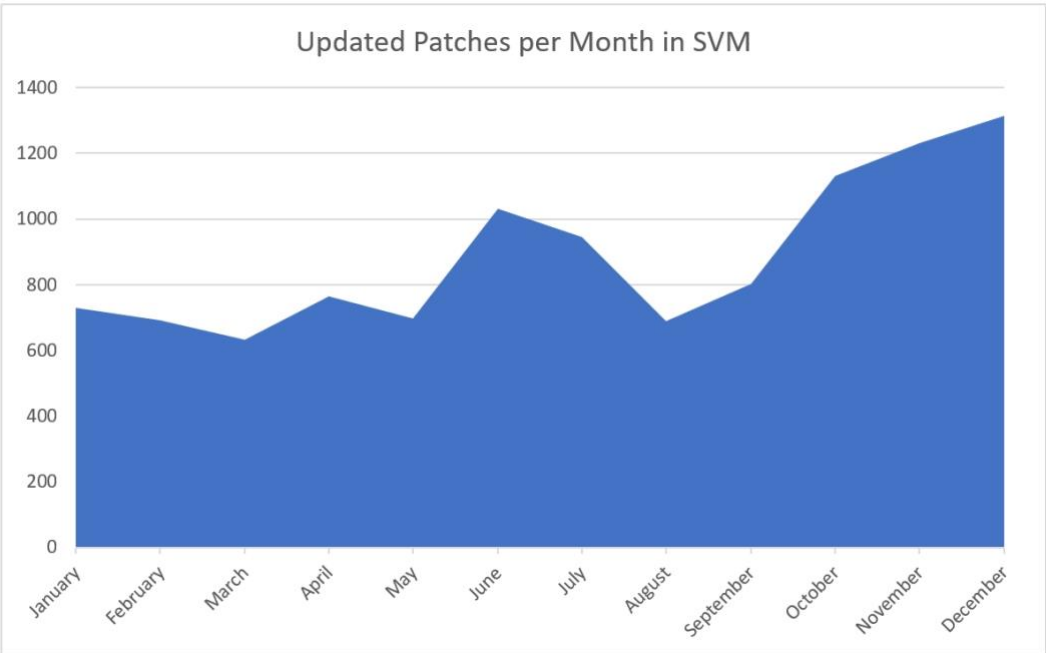
SVM patch statistics

Flexera has the largest third-party patch catalog in the world. This helps you act quicker and save time by offering an integrated approach to effectively locate, prioritize and quickly remediate threats to lower the risk to your organization.

Updated patches per month in SVM

(Patches per vendor)





How other Flexera solutions can help

To see how other Flexera solutions can help customers get immediate visibility of the impact of vulnerabilities, please go to this main article on the Community Hub where you can find complete details across all Flexera solutions.

About Flexera

Flexera delivers SaaS-based IT management solutions that enable enterprises to accelerate digital transformation and multiply the value of their technology investments. We help organizations ***inform their IT*** with definitive visibility into complex hybrid IT ecosystems, providing unparalleled IT insights that allow them to seize technology opportunities. And we help them ***transform their IT*** with tools that deliver actionable intelligence across an ever-increasing range of dimensions to effectively manage, govern and optimize their hybrid IT estate.

More than 50,000 customers subscribe to our technology value optimization solutions, delivered by 1,300+ passionate team members worldwide. To learn more, visit **flexera.com**