FLEXERA™ 2024

Annual Software Vulnerability and Threat Intelligence Report

Jeroen Braak

Based on data from Secunia Research

flexera™

Reuse

We encourage the reuse 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 *Flexera 2024 Software Vulnerability and Threat Intelligence Report* as stipulated in the terms of the license.

Contents

Introduction

This *Flexera 2024 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 71,000 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, and 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.

The anatomy of a security advisory

A security advisory is a summary of the work that Secunia Research performs to communicate standardized, validated and enriched vulnerability research on a specific software product version.

We issue Secunia Research criticality ratings and common vulnerability scoring system (CVSS) metrics after a distinct analysis in the advisories. This dual rating method allows for a much-improved means of prioritizing by criticality—delivering a review that includes product context and related security best practices.

A *rejection advisory* issued by the research team means we've determined it's not worthy of your attention. This advisory comes if a vendor issues an advisory acknowledging vulnerability that we don't believe to be valid—and would have a product solution we aren't recommending or exceeding already. We send that out to save you considerable time.

If someone other than the vendor issues an advisory that we don't believe to be valid, we discard it. We take that action so you don't waste your time processing inconsequential vulnerability information. Check out this infographic.

Anatomy of a security advisory

The Anatomy of a Security Advisory

Advisories provided by Flexera's Secunia Research team cover all security vulnerabilities associated with a specific version of a product. The advisories help simplify the prioritization of patches.

Criticality
Flexera's Secunia Advisories include CVSS scores and five-scale criticality ratings. Using both scores ensures you're getting more precise prioritization.

Threat score
Patch those vulnerabilities that are most likely to be exploited by leveraging our constantly updated scoring system.

Impact
What's the impact of the vulnerabilities covered by an advisory? Possible values include *brute force*, *denial of service* and others.

Solution
The solution may be *vendor patched*, *a partial fix* or could list possible values of *no fix* or *vendor workaround*.

Attack vector
The attack vector may be *local system*, *local network* or *remote*. This is key to assessing priority and applicability for environment.

More
Many other details are provided. Get more info about specifics within a Secunia Advisory and its possible values in our "The Anatomy of a Security Advisory" article.

2024 summary

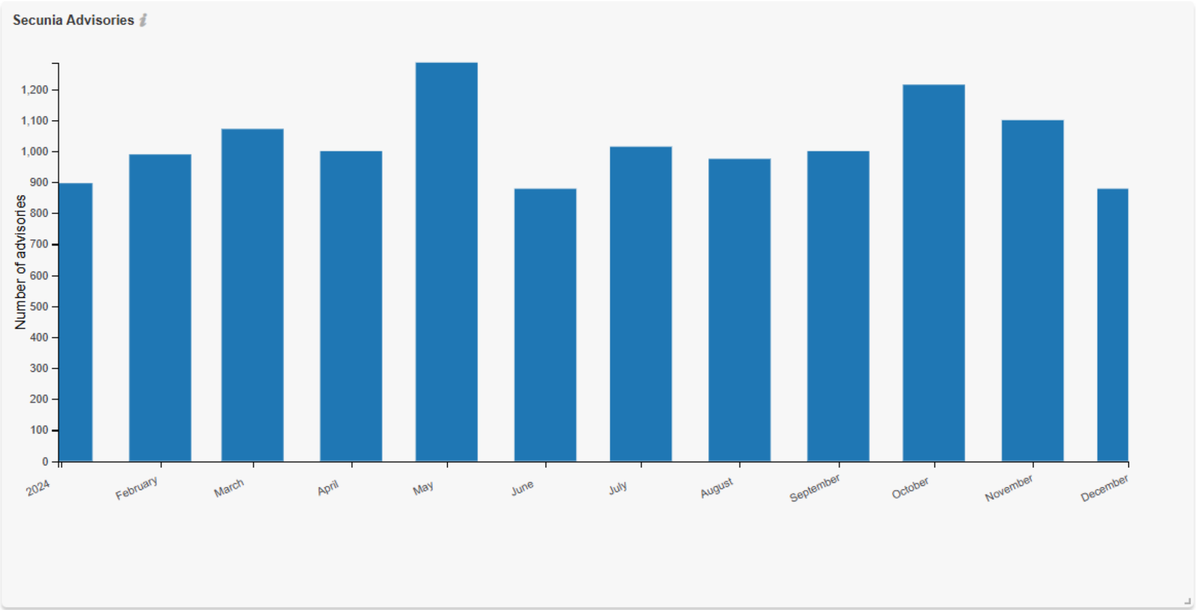
Total advisories: **12,318 ↑ (2023: 7,097)**

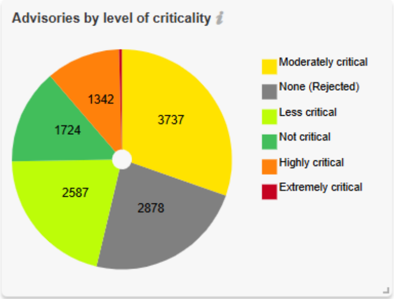
2024 is another record year for highest number of advisories issued by the Secunia Research team. This was a busy year for cybersecurity, not only a record-breaking number of advisories and vulnerabilities were reported, but also many significant vulnerabilities were the cause of data breaches, ransomware attacks and other types of threats that impacted many organizations worldwide.

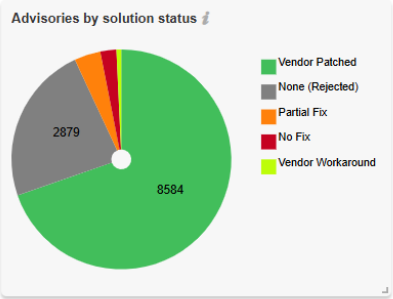
Interesting facts and trends

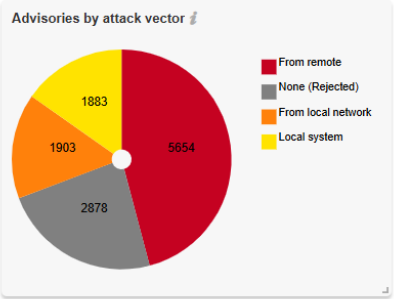
- **2024** is the year with the **most** recorded Secunia Advisories since 2002
- **NVD** published **over 40,000 CVEs** in 2024, an increase of almost **39%** compared to 2023 (28,817 CVEs)
- Average **threat score** went down: ↓ **12.19** (2023: 15.68) (click here to learn how we calculate this)
- Average **CVSS3 score** just slightly lower: ↓ **7.04** (2023: 7.28)
- **Less extreme critical** advisories have been reported in 2024: **50 (**2023: 74)
- **83** advisories reported a **zero-day** vulnerability (2023: 130)
- More than **50%** of all **advisories** are **Unix/Linux** operating systems vulnerabilities
- More than **80%** of all **rejected advisories** are also **Unix/Linux** operating systems related
- Little over **58%** of all **networking-**related advisories are for **Cisco, F5** and **Juniper**
- About Microsoft:
- **2.91%** of all **advisories** were for **Microsoft**, which put them **9th (2023: 8th place)** in vendor ranking.
    - **56.63%** ↓ (2023: **57.6 percent)** of all **zero-days** were related to **Microsoft** products (**first place**).
- **None** of the top four vendors with the most advisories (**Red Hat, SUSE, Linux Foundation, Oracle**) had any **zero-days** reported in 2024

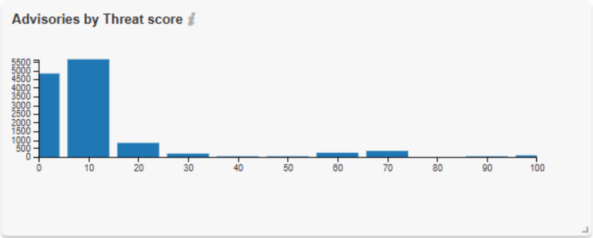
Software vulnerability mitigation and ratch management are becoming increasingly important. Due to the use of AI and the ongoing conflicts in the world, attacks on critical infrastructures in many countries are increasing. Back in 2019 (just before COVID), patching was recommended within 30 days (or 14 days for CVSS score of seven or higher). Today, 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).

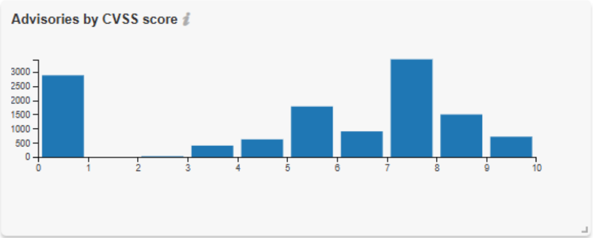












The growing challenges with NVD in 2024

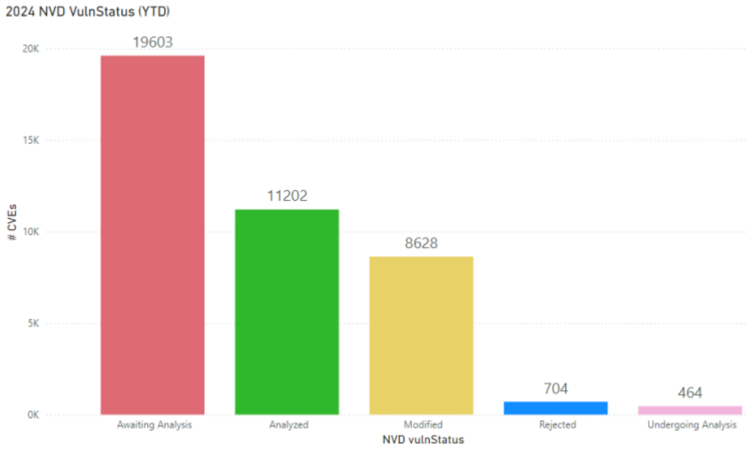
An average of 150 CVEs are disclosed per business day. As global tensions escalate and AI empowers malicious actors to craft and deploy exploits within minutes, timely and accurate vulnerability intelligence is more critical than ever.

For years, many organizations have leaned on the National Vulnerability Database (NVD) as a key resource for vulnerability management. However, recent developments have exposed significant limitations within the NVD, pushing businesses to seek out more reliable and effective alternatives.

The decline of NVD: A data-driven crisis

In 2024 the backlog within the NVD grew drastically, casting doubt on its ability to keep pace with the demands of modern cybersecurity.

Persistent API performance issues, including recent outages, have rendered automated data retrieval and integrations unreliable. This further complicates vulnerability management workflows for organizations dependent on the NVD.



The human and business costs of NVD challenges

For organizations relying on the NVD, these delays and inaccuracies translate into significant risks.

Extended risk windows: The lag in vulnerability analysis prolongs the time it takes to detect, prioritize and remediate vulnerabilities. With some exploits weaponized in as little as 1-7 days after disclosure, the risk window is dangerously wide.

Resource strain: Security teams often resort to manual research and cross-referencing, sapping valuable resources that could otherwise be directed toward proactive measures.

Compliance challenges: Delayed and incomplete data impacts an organization's ability to meet regulatory requirements, such as NIS2, DORA, ISO, CRA or other industry-specific mandates.

Rethinking vulnerability intelligence: Why free isn't always reliable

The NVD, a free database managed by the U.S. government, has long been a go-to resource for organizations. However, its unverified, unanalyzed, and often incomplete data poses significant risks to effective cybersecurity. **Flexera's Software Vulnerability Research** provides a trusted alternative, offering thoroughly researched, validated, and enriched data. Since 2002, the research has provided reliable vulnerability intelligence without disruptions, ensuring organizations can depend on accurate and actionable insights to stay secure.

Advisories breakdown

Compared to previous years

2024 total advisory count: 12,318 ↑ (2023: 9,402)

As expected, 2024 had the highest number of advisories since Secunia started reporting them.

#	Year	# of advisories
1	2024	12318
2	2023	9402
3	2022	7097
4	2020	7065
5	2016	6348
6	2017	6262
7	2021	6153
8	2018	6101
9	2014	6004
10	2015	5934

Figure 1: Top ten years with most advisories

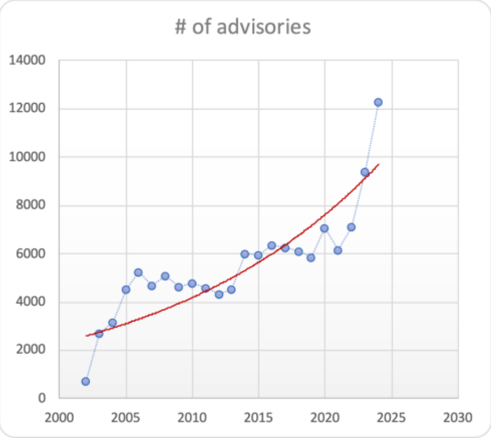


Figure 2: Chart with advisory trendline over the years

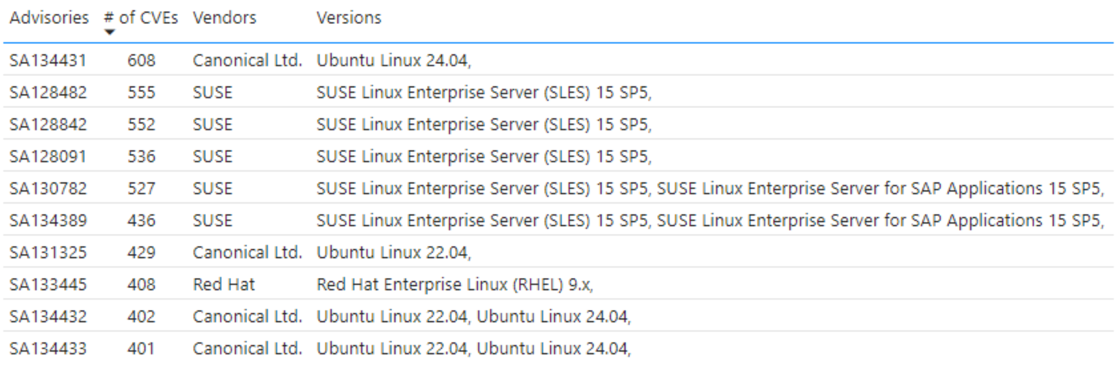
This year:	#	Change (last year)
Total # of advisories	**12,318**	↑ (9,402)
Advisories with criticality	**9,441**	↑ (7,902)
Rejected advisories *	**2,877**	↑ (1,500)
Unique vendors	**292**	↑ (291)
Unique products	**1,560**	↑ (1,437)
Unique versions	**1,710**	↓ (1,794)
		↑ increased ↓lower ↔ same

*****2,877 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).*

Advisories versus CVEs and vice versa

Secunia Research focuses on delivering verified, tested and enriched vulnerability information per product or product group. This can result in CVEs being reported for many advisories and vice versa.

Top 10 advisories with most CVEs attached



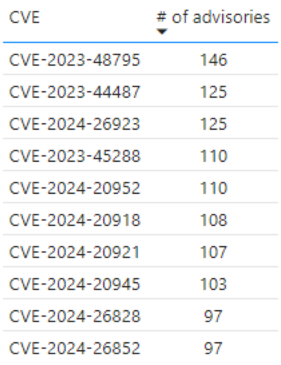
Advisories	# of CVEs	Vendors	Versions
SA134431	608	Canonical Ltd.	Ubuntu Linux 24.04,
SA128482	555	SUSE	SUSE Linux Enterprise Server (SLES) 15 SP5,
SA128842	552	SUSE	SUSE Linux Enterprise Server (SLES) 15 SP5,
SA128091	536	SUSE	SUSE Linux Enterprise Server (SLES) 15 SP5,
SA130782	527	SUSE	SUSE Linux Enterprise Server (SLES) 15 SP5, SUSE Linux Enterprise Server for SAP Applications 15 SP5,
SA134389	436	SUSE	SUSE Linux Enterprise Server (SLES) 15 SP5, SUSE Linux Enterprise Server for SAP Applications 15 SP5,
SA131325	429	Canonical Ltd.	Ubuntu Linux 22.04,
SA133445	408	Red Hat	Red Hat Enterprise Linux (RHEL) 9.x,
SA134432	402	Canonical Ltd.	Ubuntu Linux 22.04, Ubuntu Linux 24.04,
SA134433	401	Canonical Ltd.	Ubuntu Linux 22.04, Ubuntu Linux 24.04,

Top 10 CVEs mentioned with most advisories attached

(These are CVEs mentioned in advisories that were published in 2024. This means that older CVEs can be included in the below statistics.)

This means that many products are affected by these CVEs.

Below is a great example of a CVE and different results for CVSS scoring, which confirms that CVSS scoring should not be your only variable to assign urgency or priority.



CVE	# of advisories
CVE-2023-48795	146
CVE-2023-44487	125
CVE-2024-26923	125
CVE-2023-45288	110
CVE-2024-20952	110
CVE-2024-20918	108
CVE-2024-20921	107
CVE-2024-20945	103
CVE-2024-26828	97
CVE-2024-26852	97

Filling the gaps – vulnerability ratings and product context

Especially with the perceived absence of NVD, the availability of vulnerability ratings at no cost largely depends on the vendors respective maintainers of products.

We witnessed first-hand what happens if one of the dominant maintainer's won't provide an exploitability analysis or a CVSS score.

The Linux Foundation CNA (CVE numbering authority) bases its CVE assignments for the Linux Kernel and the resulting security advisories largely on the impact of a potential vulnerability. However, as every vulnerability analyst knows, exploitability matters. Is there a vector to exploit a potential vulnerability with a gain for the potential attacker?

As a result of the lack of quality of such vulnerability reports, vendors of products using the Linux Kernel scramble to derive their own vulnerability ratings. Take CVE-2024-26923 for example:

Scoring from	CVSS 3.1 Base Score	CVSS 3.1 Metric
Linux Foundation	Not available	Not available
NVD	Not available	Not available
SUSE	7	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
Amazon	5.5	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
Red Hat	7	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
Oracle	7	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
Canonical Ltd.	7.8	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Vulert	7.8	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Vulncheck	Not available	Not available
Vulmon	Not available	Not available

** Information as of January 27, 2025*

The analysis of Secunia Research derives a CVSS score on a per product basis for any valid vulnerabilities. Any crucial missing information from vendor reporting will be derived from the information available.

In this case, the CVE is related to a dangling pointer and requiring a difficult to exploit race condition involving the garbage collection (GC), which makes it less likely to be able to exploit this vulnerability for a full-fledged privilege escalation. Thus, in the base Linux Kernel itself we rated the vulnerability with an unknown impact coming from an attacker who is a local user on the operating system (CVSS:3.1 Base Score 4.9 / CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L).

Nevertheless, the situation for SUSE, Red Hat, etc. may differ e.g., due to how their own kernel is configured and compiled and which parts of the original Linux Kernel code base is used.

Therefore, Secunia Research has the capabilities to rate the very same vulnerability differently depending on the actual product exposing the vulnerability. The product context matters! The CVSS scores provided by each vendor are considered as a data point for the respective Secunia Advisories related to the vendor.

Advisory criticality and attack vector

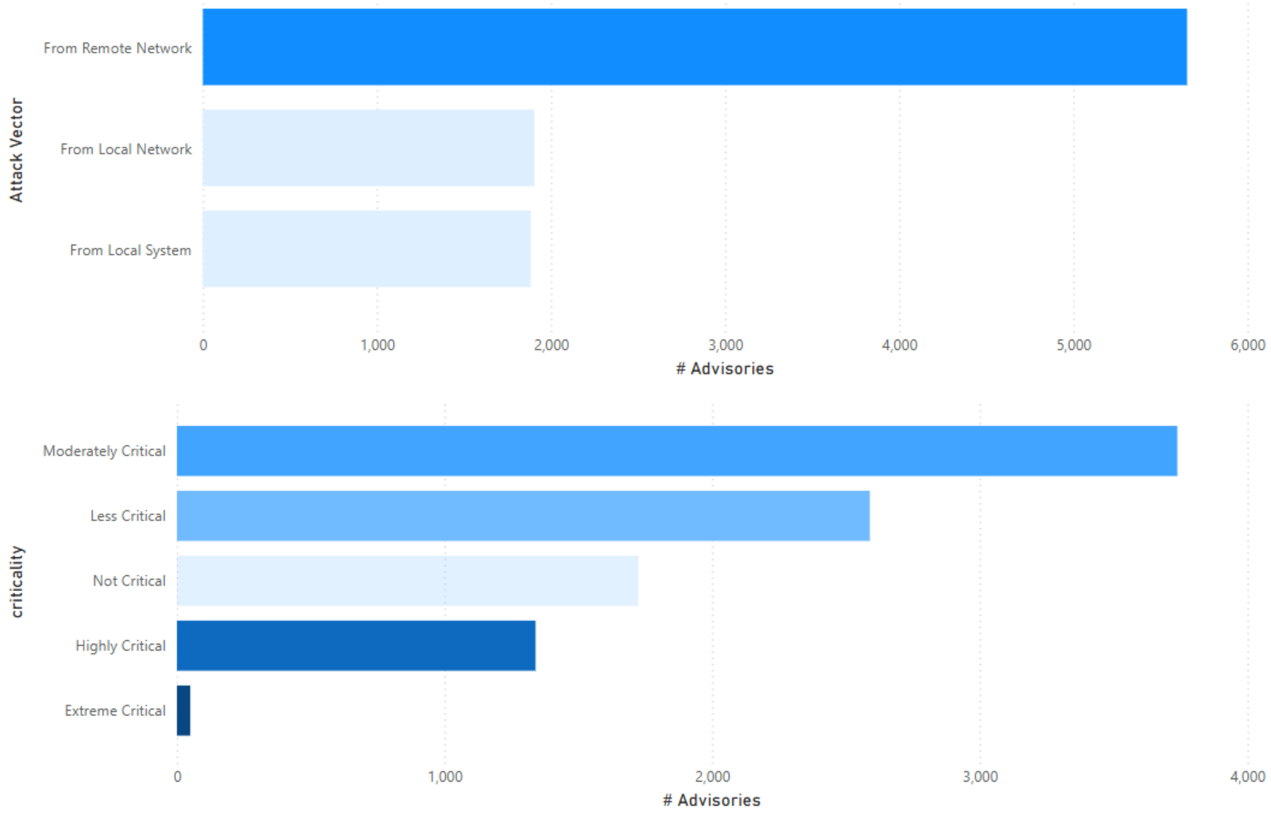


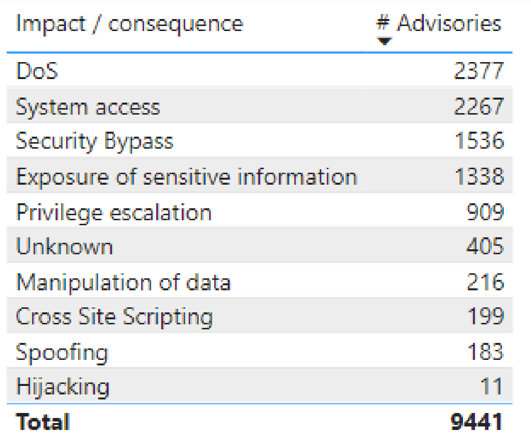
Figure 3 : Overview criticality and attack vector

More information about the variables used in the above charts:

- Attack vector (from where)
- Criticality (severity)

Though not shown in the chart, Secunia Research also provides information about the **impact** or **consequence** when a vulnerability has been exploited. There are 12 values that can be used (most advisories have one or more). Read more here.

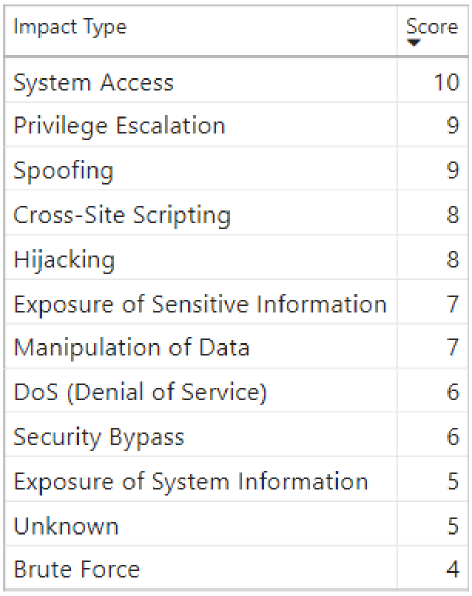
Advisories and impact (Consequence of exploited)



Impact / consequence	# Advisories
DoS	2377
System access	2267
Security Bypass	1536
Exposure of sensitive information	1338
Privilege escalation	909
Unknown	405
Manipulation of data	216
Cross Site Scripting	199
Spoofing	183
Hijacking	11
Total	**9441**

Prioritizing vulnerabilities based on the potential consequence is a crucial aspect of effective cybersecurity management.
The use of a scoring mechanism allows organizations to systematically assess and prioritize vulnerabilities, ensuring that the most critical issues are addressed first.

Below is an example of a scoring table that can be used in a prioritization process.



Impact Type	Score
System Access	10
Privilege Escalation	9
Spoofing	9
Cross-Site Scripting	8
Hijacking	8
Exposure of Sensitive Information	7
Manipulation of Data	7
DoS (Denial of Service)	6
Security Bypass	6
Exposure of System Information	5
Unknown	5
Brute Force	4

Impact (Consequence)
The following are Consequence values.

Brute Force
Used in cases where an application or an algorithm allows an attacker to guess passwords in an easy manner.

Cross-Site Scripting
Cross-Site Scripting vulnerabilities allow a third party to manipulate the content or behavior of a web application in a user's browser, without compromising the underlying system. Different Cross-Site Scripting related vulnerabilities are also classified under this category, including “script insertion” and “cross-site request forgery”.
Cross-Site Scripting vulnerabilities are often used against specific users of a website to steal their credentials or to conduct spoofing attacks.

DoS (Denial of Service)
This includes vulnerabilities ranging from excessive resource consumption (for example, causing a system to use a lot of memory) to crashing an application or an entire system.

Exposure of Sensitive Information
Vulnerabilities where documents or credentials are leaked or can be revealed either locally or remotely.

Exposure of System Information
Vulnerabilities where excessive information about the system (for example. version numbers, running services, installation paths, and similar) are exposed and can be revealed from remote and, in some cases, locally.

Hijacking
Covers vulnerabilities where a user session or a communication channel can be taken over by other users or remote attackers.

Manipulation of Data
This includes vulnerabilities where a user or a remote attacker can manipulate local data on a system, but not necessarily be able to gain escalated privileges or system access.
The most frequent type of vulnerabilities with this impact are SQL-injection vulnerabilities, where a malicious user or person can manipulate SQL queries.

Privilege Escalation
Covers vulnerabilities where a user can conduct certain tasks with the privileges of other users or administrative users.
This typically includes cases where a local user on a client or server system can gain access to the administrator or root account, thus taking full control of the system.

Security Bypass
Covers vulnerabilities or security issues where malicious users or people can bypass certain security mechanisms of the application.
The actual impact varies significantly depending on the design and purpose of the affected application.

Spoofing
Covers various vulnerabilities where it is possible for malicious users or people to impersonate other users or systems.

System Access
Covers vulnerabilities where malicious people are able to gain system access and execute arbitrary code with the privileges of a local user.

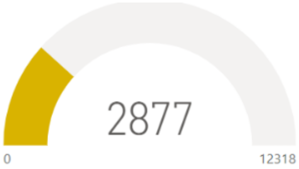
Rejection advisories

There are many vulnerabilities posted in the NVD, by many vendors and CNA's. They are not always valid and they are not always assigned proper criticality ratings. In some cases, a vulnerability may be legitimate but does 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.

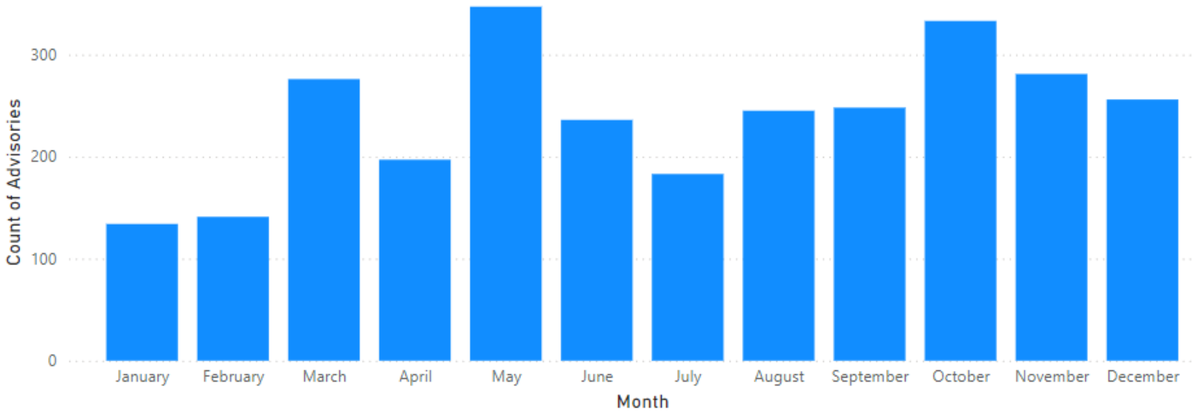
For example, NERC (North American Electric Reliability Corporation), may require reporting not only the vulnerabilities covered by the normal advisories but also vulnerabilities, which our Research Team has rejected as not being a valid threat to security.

On average, 15 percent of the total number of advisories are rejection advisories. In 2024, there were 23.35% (2,877 rejection advisories). This is mostly due to the high volume of rejections from **Linux Foundation.**



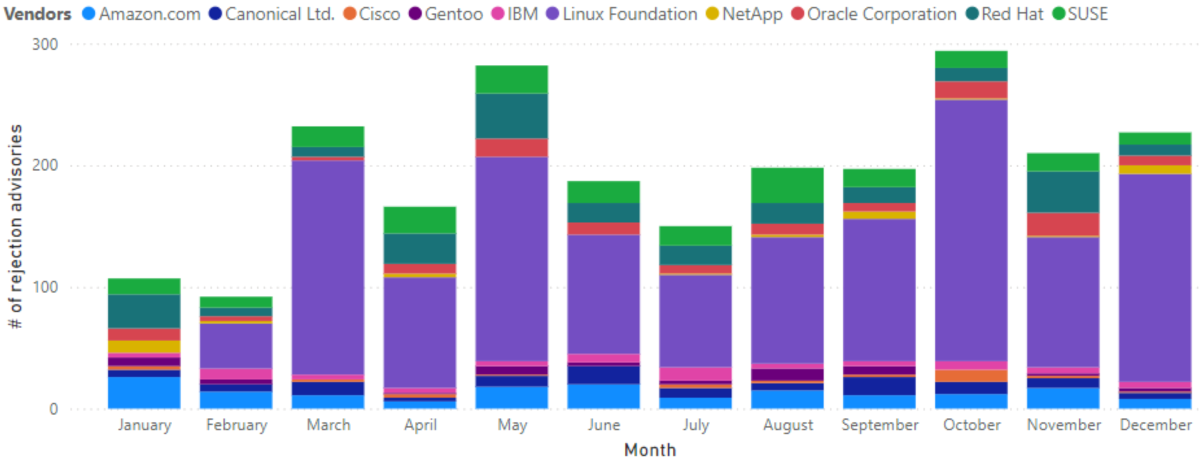
Linux Foundation was responsible for a total of **2,600** advisories in 2024, of which **more than half** (**1,360**) were given the rejection tag by the Secunia Research Team.

Overview rejection advisories



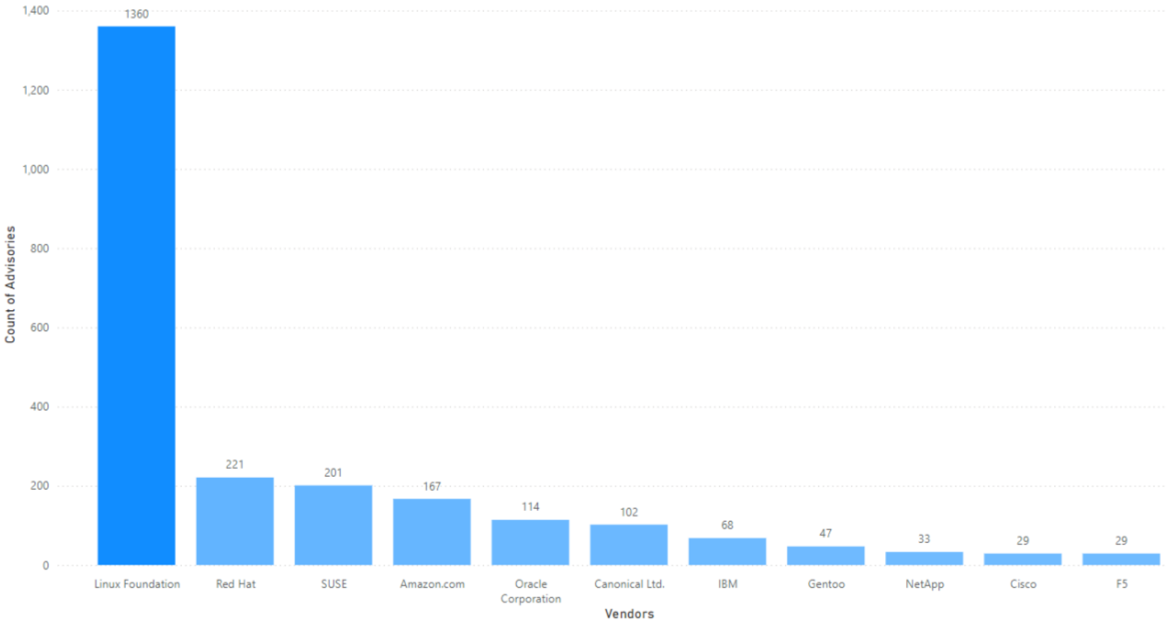
Top Vendors with most rejection advisories

The **Linux Foundation** has not only disclosed the most vulnerabilities this year, but most of these vulnerabilities were given a rejection reason by the Secunia Research Team.

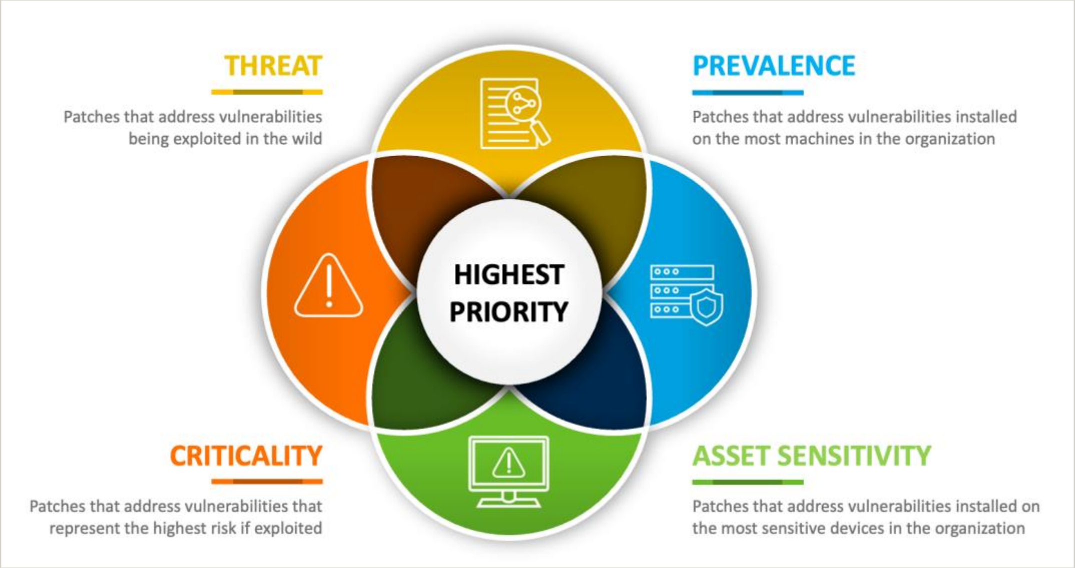


An advisory may be rejected for many reasons; the most common are:

- **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


THREAT
Patches that address vulnerabilities being exploited in the wild
PREVALENCE
Patches that address vulnerabilities installed on the most machines in the organization
HIGHEST PRIORITY
CRITICALITY
Patches that address vulnerabilities that represent the highest risk if exploited
ASSET SENSITIVITY
Patches that address vulnerabilities installed on the most sensitive devices in the organization

Prevalence

- 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

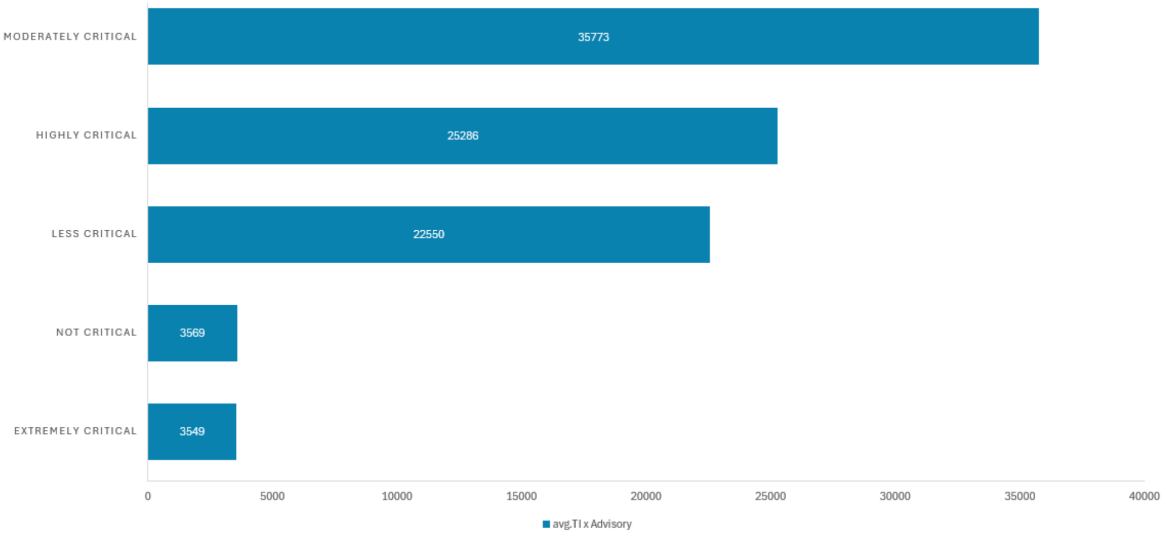
- The most popular method of thoughtful prioritization.
- If exploited, how bad could it affect your security?
- Is it designated to be of a high criticality? Patch.

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 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.

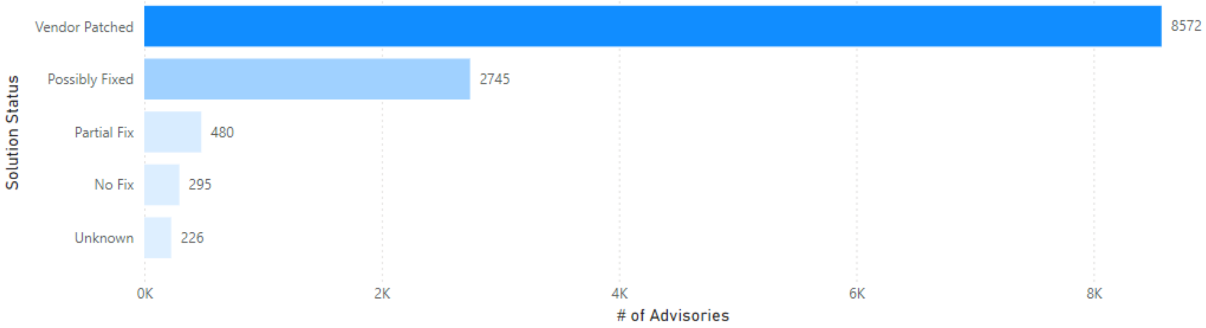
criticality	# of Advisories	# of ZeroDays	Avg.ThreatScore	Avg.CVSS3	# of CyberExploit	# of RecentCyberExploit	# of RansomwareLinks
Extreme Critical	50	50	70.98	9.24	46	17	19
Highly Critical	1340	33	18.87	9.20	635	114	86
Less Critical	2589		8.71	6.71	698	41	39
Moderately Critical	3738		9.57	7.35	1193	96	67
Not Critical	1724		2.07	5.10	166	8	4

rejection advisories not included.

[More about Secunia Criticality (severity) scoring]

Take away 2

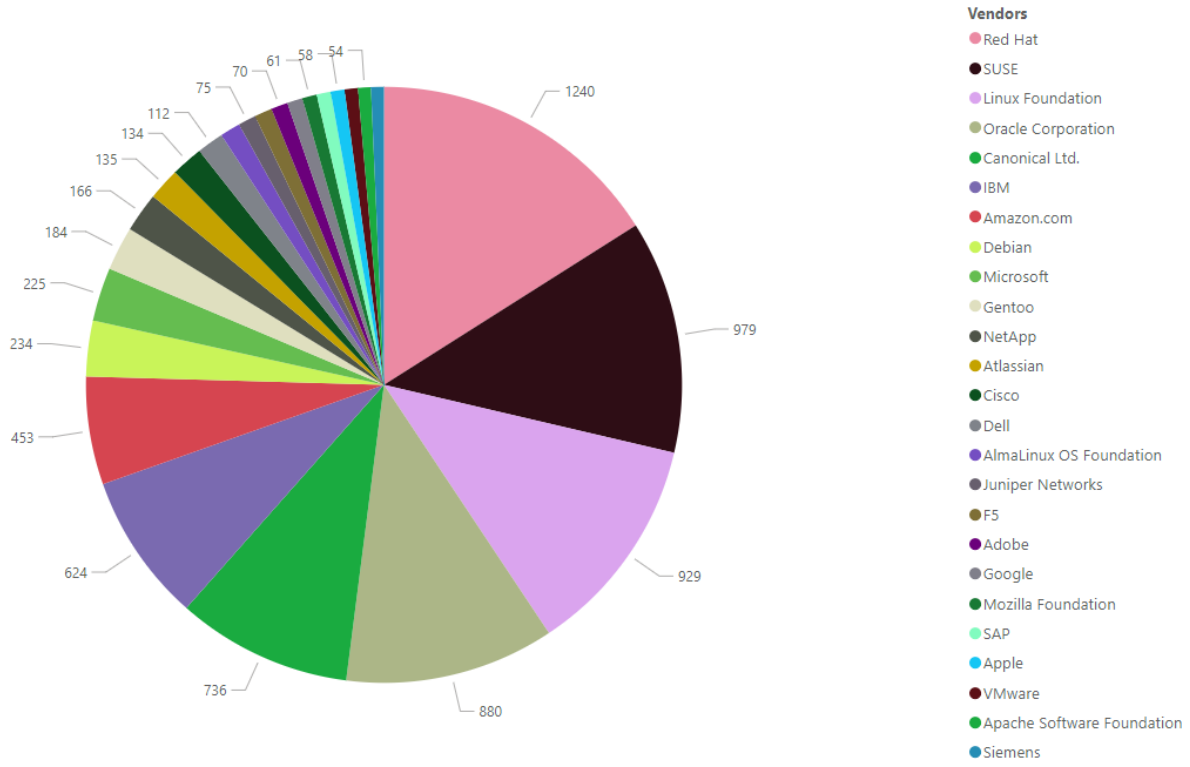
Most vulnerabilities have a patch available typically within 24 hours after disclosure.



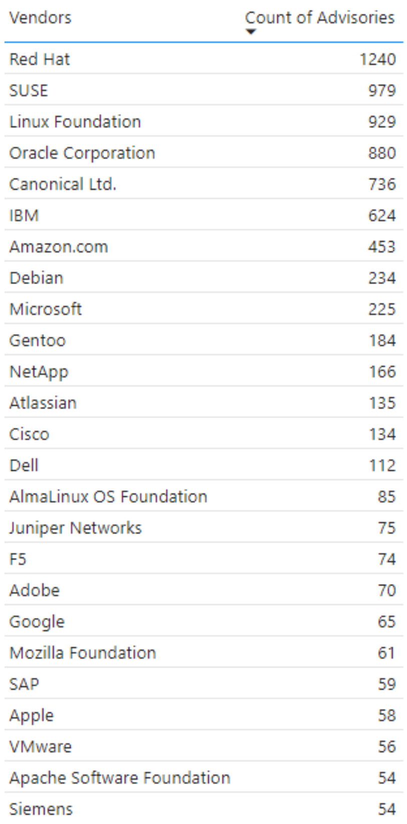
Vendor view

Top 25 vendors with most advisories

no rejection advisories included

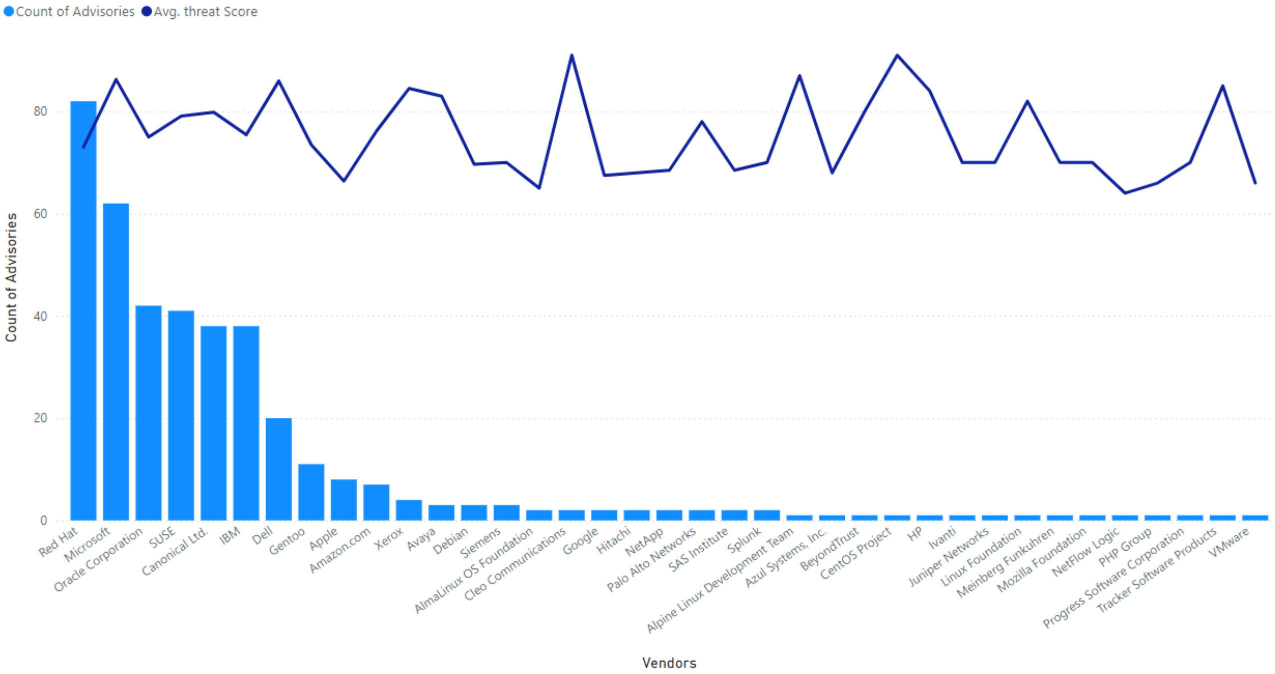


Note: Canonical Ltd. = Ubuntu

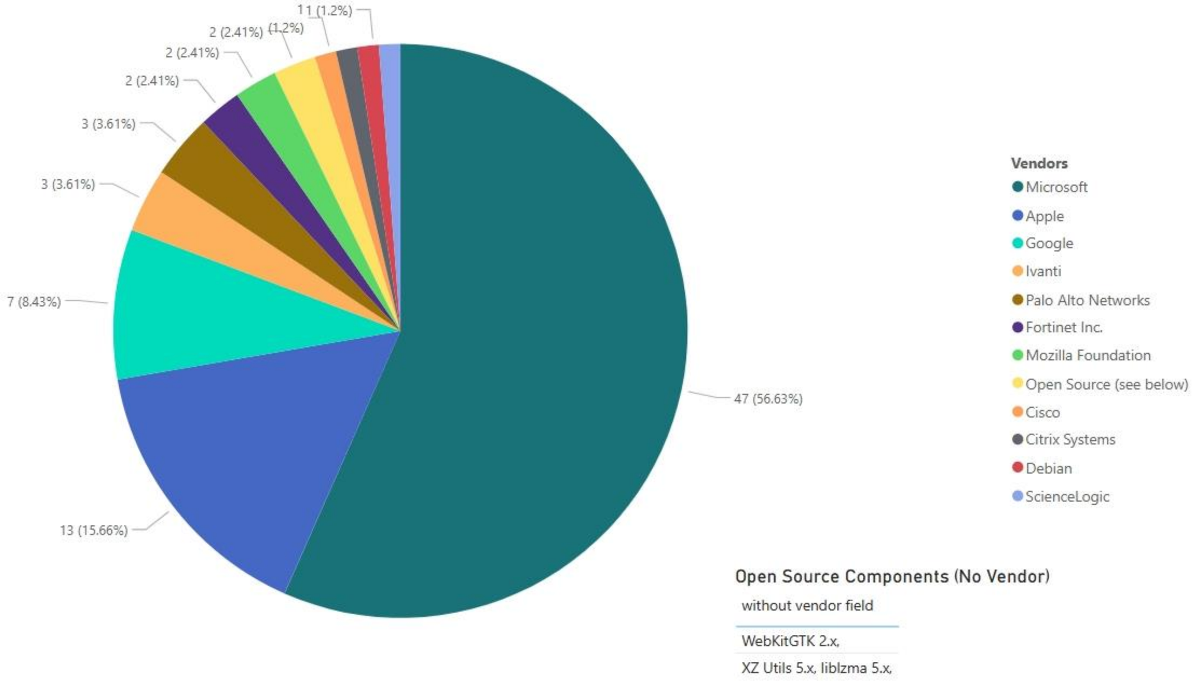


Vendors	Count of Advisories
Red Hat	1240
SUSE	979
Linux Foundation	929
Oracle Corporation	880
Canonical Ltd.	736
IBM	624
Amazon.com	453
Debian	234
Microsoft	225
Gentoo	184
NetApp	166
Atlassian	135
Cisco	134
Dell	112
AlmaLinux OS Foundation	85
Juniper Networks	75
F5	74
Adobe	70
Google	65
Mozilla Foundation	61
SAP	59
Apple	58
VMware	56
Apache Software Foundation	54
Siemens	54

Top vendors with highest average threat score



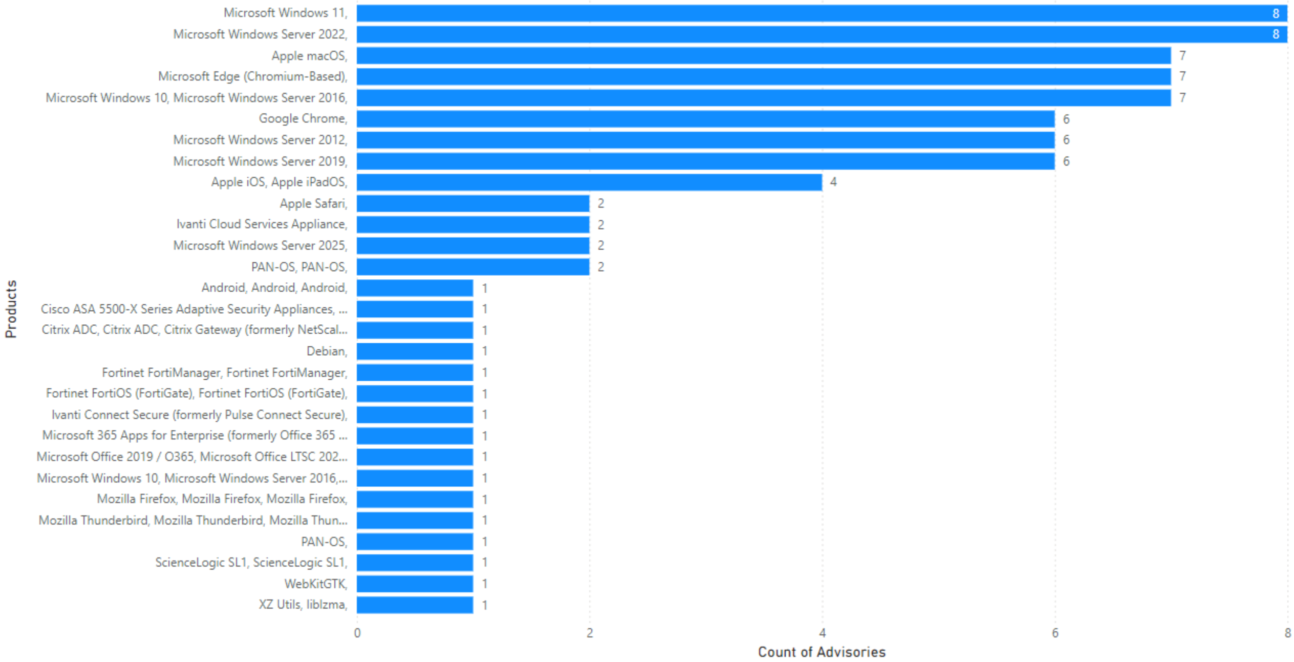
Top vendors with zero-days



Open Source Components (No Vendor)
without vendor field
WebKitGTK 2.x,
XZ Utils 5.x, liblzma 5.x,

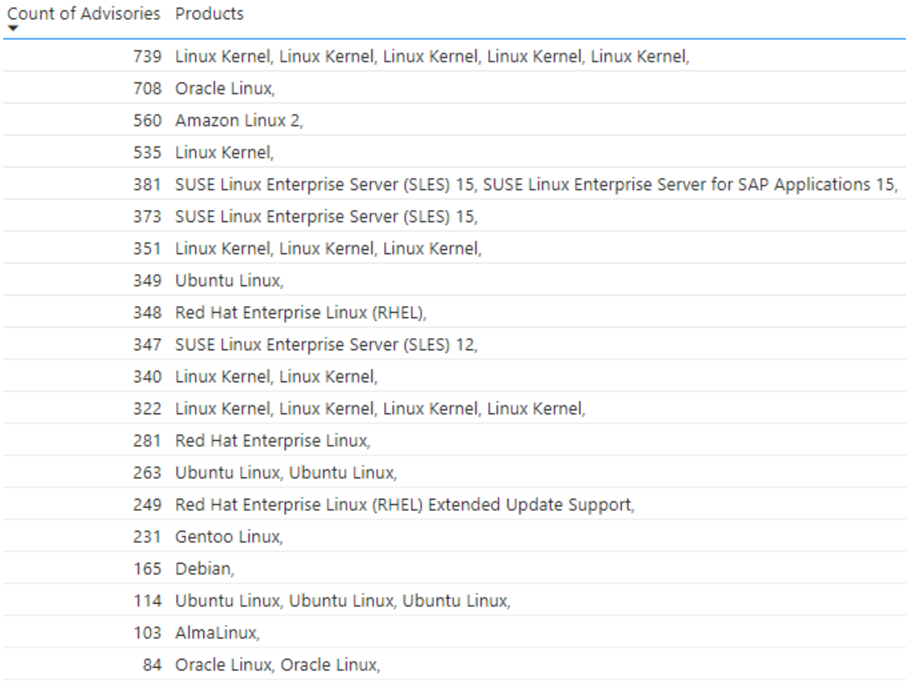
Product view

Products with the most zero-days advisories reported*



* Covered by Secunia Research

Top 20 operating systems with most advisories



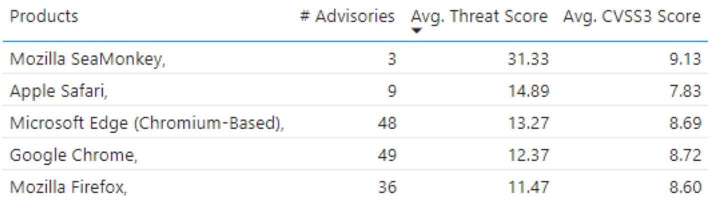
Count of Advisories	Products
739	Linux Kernel, Linux Kernel, Linux Kernel, Linux Kernel, Linux Kernel,
708	Oracle Linux,
560	Amazon Linux 2,
535	Linux Kernel,
381	SUSE Linux Enterprise Server (SLES) 15, SUSE Linux Enterprise Server for SAP Applications 15,
373	SUSE Linux Enterprise Server (SLES) 15,
351	Linux Kernel, Linux Kernel, Linux Kernel,
349	Ubuntu Linux,
348	Red Hat Enterprise Linux (RHEL),
347	SUSE Linux Enterprise Server (SLES) 12,
340	Linux Kernel, Linux Kernel,
322	Linux Kernel, Linux Kernel, Linux Kernel, Linux Kernel,
281	Red Hat Enterprise Linux,
263	Ubuntu Linux, Ubuntu Linux,
249	Red Hat Enterprise Linux (RHEL) Extended Update Support,
231	Gentoo Linux,
165	Debian,
114	Ubuntu Linux, Ubuntu Linux, Ubuntu Linux,
103	AlmaLinux,
84	Oracle Linux, Oracle Linux,

Browser-related advisories

Web browsers serve as our gateway to the internet, providing a seamless interface for accessing information, services and entertainment. However, this very connectivity exposes browsers to an array of vulnerabilities, in most cases exploited through a **remote attack vector**.

The urgency of timely browser patching cannot be overstated. As users traverse the digital landscape, the constant evolution of security mechanisms by browser developers remains a critical line of defense. Failing to patch vulnerabilities in a timely manner increases the likelihood of falling victim to remote exploits, exposing users to a range of potential risks.

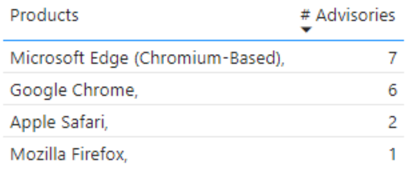
Advisories per browser



Products	# Advisories	Avg. Threat Score	Avg. CVSS3 Score
Mozilla SeaMonkey,	3	31.33	9.13
Apple Safari,	9	14.89	7.83
Microsoft Edge (Chromium-Based),	48	13.27	8.69
Google Chrome,	49	12.37	8.72
Mozilla Firefox,	36	11.47	8.60

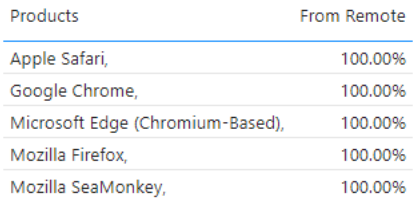
note: filtered on avg. threat score.

Zero-day vulnerabilities



Products	# Advisories
Microsoft Edge (Chromium-Based),	7
Google Chrome,	6
Apple Safari,	2
Mozilla Firefox,	1

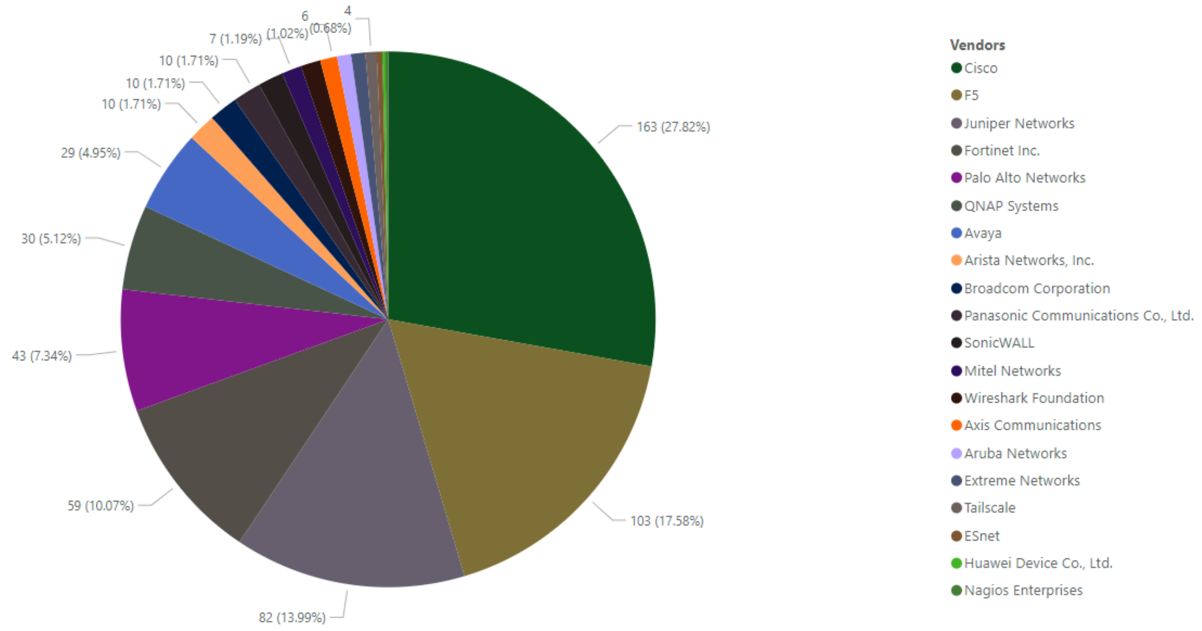
Browser attack vector



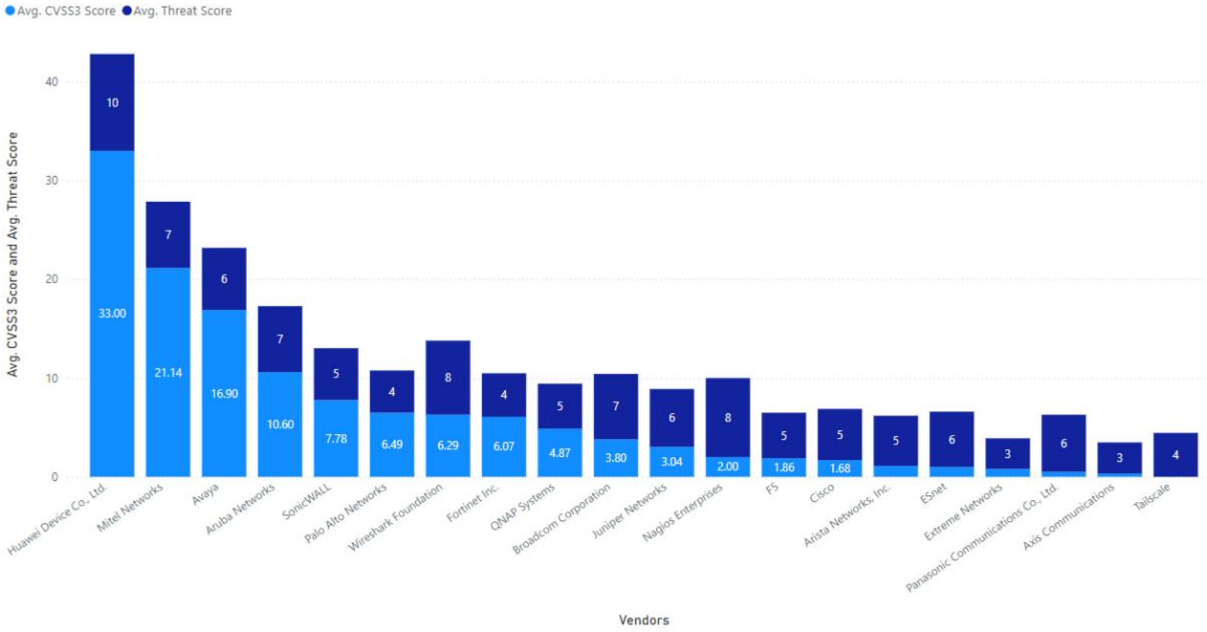
Products	From Remote
Apple Safari,	100.00%
Google Chrome,	100.00%
Microsoft Edge (Chromium-Based),	100.00%
Mozilla Firefox,	100.00%
Mozilla SeaMonkey,	100.00%

Networking-related advisories

Number of advisories per networking-related vendor



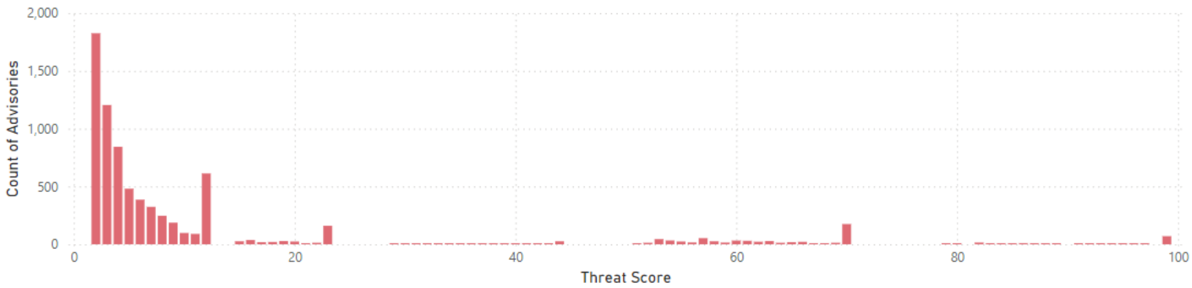
Average threat and CVSS score per networking-related vendor

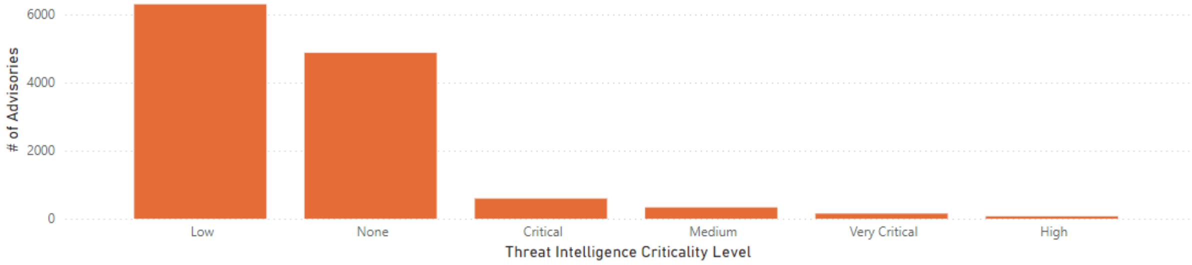


Threat intelligence

In a world where there are now more than 40,000 new vulnerabilities (CVEs) every year, being smart about prioritizing remediation efforts is essential. Leveraging threat intelligence is another valuable layer of insight that helps you understand which of the vulnerabilities affecting your environment are being exploited in the wild.

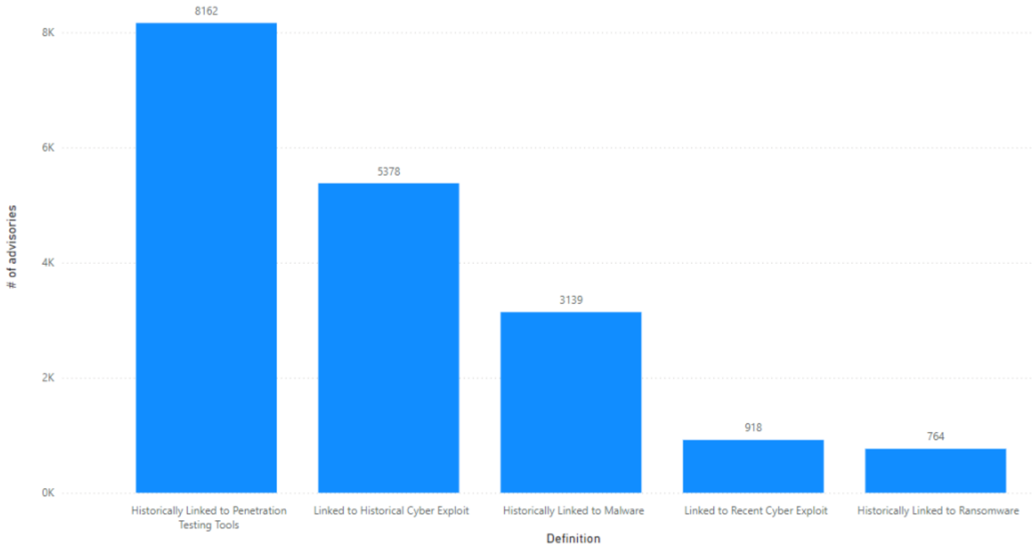
Leveraging machine learning, artificial intelligence, and human curation from thousands of sources in the open, deep and dark web, threat intelligence augments Flexera's Software Vulnerability Research's vulnerability intelligence with a threat score that provides the ultimate prioritization tool for your busy desktop operations teams.





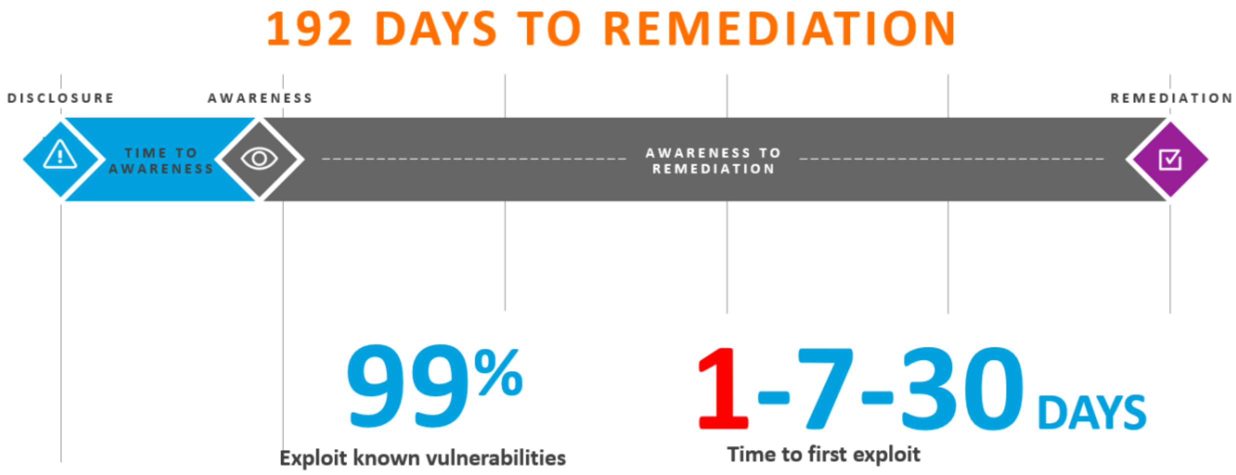
More information on how we add Threat Intelligence Scoring

SAIDs containing at least one CVE



Patching

Most of 2024’s vulnerabilities were vendor patched. In fact, most vulnerabilities are patched within 24 hours after disclosure.



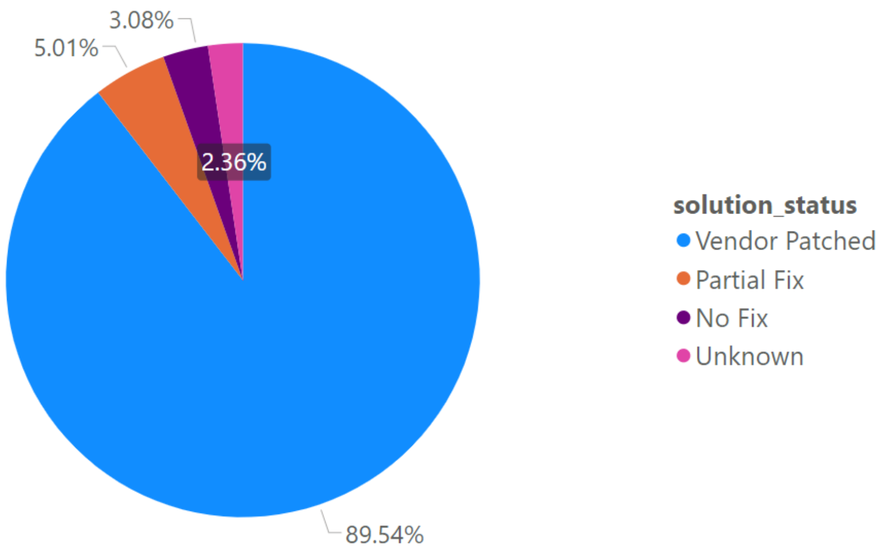
The challenge remains that organizations don’t have full visibility or awareness when a vulnerability is disclosed (time to awareness). Another big challenge is time to remediation (the time from having this information, correlating that with your environment and initiating the process to get the software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

Recent data about MTTR (Mean Time to Remediation)

- **192 Days** is an industry average based on recent studies
- **271 Days** for organizations using standard practices without dedicated vulnerability management solutions
- **135 Days** for organizations with robust processes for critical vulnerabilities
- **Sector specific trends**
    - **Finance/Banking**: Tends to have faster MTTRs (under 100 days for critical vulnerabilities) due to regulatory pressures and proactive security measures
    - **Healthcare**: Slower MTTRs (often exceeding 200 days) due to legacy systems and resource constraints
    - **Technology/IT**: Typically, closer to 100 days due to better integration of automated patching systems
-

Vendor patched vulnerabilities

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



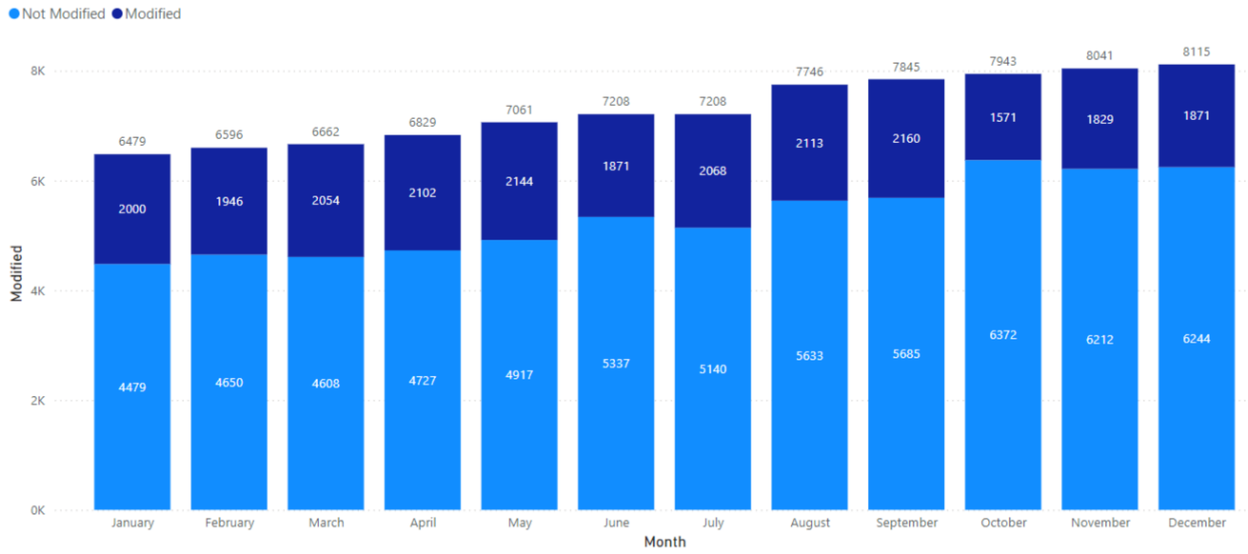
SVM patch statistics

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. [More information](#).

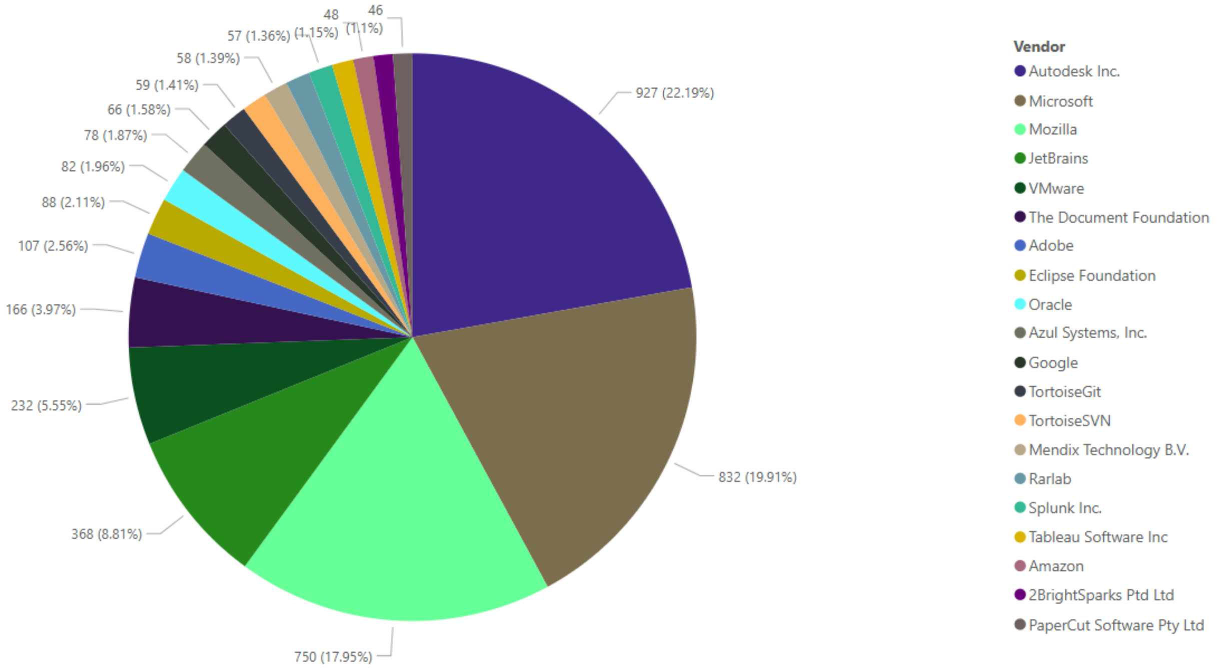
Updated patches per month in SVM

Flexera's Vendor Patch Module application coverage changes regularly as we update existing entries and add new ones daily. (Users can suggest new software to be added to the catalog.)

On average, the refresh rate of updated patches was **27.05%** and the catalog grew **25.25%** in 2024.



This year’s top 25 vendor patches (by vendor)



Learn more

Below are a few links with information about how Flexera can help you with creating an effective software vulnerability and patch management process to reduce security risk.

- Flexera Software Vulnerability Manager
- Flexera Monthly Vulnerability Report
- Request a trial / demo
- Flexera Community with resources that include:
    - Software Vulnerability Management Blog
    - Software Vulnerability Management Knowledge Base
    - Product Documentation
    - Forums
    - Learning Center

About Flexera

Flexera helps organizations understand and maximize the value of their technology, saving billions of dollars in wasted spend. Powered by the Flexera Technology Intelligence Platform, our award-winning IT asset management, FinOps and SaaS management solutions provide comprehensive visibility and actionable insights on an organization's entire IT ecosystem. This intelligence enables IT, finance, procurement and cloud teams to address skyrocketing costs, optimize spend, mitigate risk, and identify opportunities to create positive business outcomes.

More than 50,000 global organizations rely on Flexera and its Technopedia reference library, the largest repository of technology asset data. Learn more at **flexera.com**.

Secunia Research from Flexera is comprised of world-class security specialists dedicated to discovering, testing, verifying, and validating vulnerabilities in a wide range of software products. Since 2002, Secunia Research has provided the most accurate and reliable vulnerability intelligence available. The team's expertise ensures that organizations receive the best vulnerability intelligence for mitigating risks effectively.

This industry-leading vulnerability research forms the foundation for two of Flexera's key products: **Software Vulnerability Management (SVM)** and **Software Vulnerability Research (SVR)**.

SVM leverages Secunia Research to help organizations proactively manage software vulnerabilities. Automating the identification, reporting, prioritization, and patching of vulnerabilities, shrinking the risk window and increasing security.

With **SVR**, organizations gain access to real-time, verified vulnerability—and threat intelligence. Covering ~71,000 products, SVR provides detailed advisories that many valuable datapoints to help security teams prioritize remediation efforts, reduce risk, and stay ahead of potential threats.