FLEXERA™ 2023

Annual Software Vulnerability and Threat Intelligence Report

Jeroen Braak

Based on data from Secunia Research

Reuse

Contents

Introduction

This *Flexera 2023 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 69,000 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.

Example why it's not a good idea to rely on NVD only

Vulnerability: **CVE-2023-46589**

(Information per 1/9/2024)

NIST / NVD Data:

NIST (CVE.ORG) record created: 10/23/2023
NVD Published date: 11/28/2023
Affected products (NVD): Apache Tomcat 8.5—11.0.0
Last Modified: 01/05/2024 (Modified)

Secunia Research:

Vulnerability	Released date	Modified date	Advisory	CVSS	Threat Score
CVE-2023-46589	2023-10-31	2024-01-09	SA121703, SA121453, SA122496	7.5 v3	16

Advisory	Release date	Modified date	Title	Criticality	Zero Day	Solution status	Where	CVSS Score	Threat Score	Type
SA121703	2023-11-28	2023-11-28	Apache Tomcat HTTP Request Smuggling Vulnerability		No	Vendor Patched	From remote	7.2 v3	16	Secunia Advisory
SA121453	2023-12-18	2023-12-18	IBM Security QRadar SIEM Multiple Vulnerabilities		No	Vendor Patched	From local network	8.8 v3	70	Secunia Advisory
SA122496	2024-01-03	2024-01-03	IBM Integration Bus Apache Tomcat Multiple Vulnerabilities		No	Vendor Patched	From local network	6.5 v3	17	Secunia Advisory

Conclusion(s):

1. NVD largely relies on the vendors or third parties updating the CVE entries on MITRE (like more vendor advisory links), so, e.g., in this example there was no information added to the MITRE Tomcat CVE entry and thus NVD doesn't have anything to show beyond the basics. NVD is frequently not complete when it comes to libraries / components that are used in a lot of "downstreams". *(downstreams: Vendors using libraries / components for other software products. Best recent example is the cascading "downstream" effect of the Log4J and Log4shell vulnerabilities)*

2. Secunia Research on the other hand, don't have to rely on the MITRE information, so Secunia Research frequently reacts earlier, many times even before a CVE was assigned (if one gets assigned at all). Secunia Research Team started the CVE research on October 31. 2023, even when there was no publication in NVD. (only registration in NIST CVE.ORG)

3. When The Apache Software Foundation **officially** published the Security Advisory on November 28. 2023, Flexera did the same with SA121703 including all relevant information for remediation as well as additional information for optimizing the prioritization process. (Threat Intelligence, Consequence (Impact), and Secunia Criticality Score)

4. NVD only mentions the base software product (Apache Tomcat), however since the initial publication 2 other products released a notification regarding the vulnerability affecting their product:
    - IBM Security QRadar Siem, on Dec. 18, 2023
    - IBM Integration Bus Apache Tomcat, on Jan. 3, 2024

2023 summary

Total advisories: **9,402** ↑ **(2022: 7,097)**

2023 broke the record for highest number of advisories issued by the Secunia Research team. This was for sure 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:

- **2023** is the year with the **most** recorded Secunia Advisories since 2002
- **NVD** published **28,834 CVEs** in 2023, an increase of 15% compared to 2022 (25,050 CVEs)
- Average **threat score** went up: ↑ **15.68** (2022: 13.66) (click here to learn how we calculate this)
- Average **CVSS3 score** just slightly lower: ↓ **7.28** (2022: 7.35)
- **More extreme critical** advisories have been reported in 2023: **74 (**2022: 44)
- **130** advisories reported a **zero-day** vulnerability (2022: 85)
- More than **50 percent** of all **advisories** are Unix**/Linux** operating systems vulnerabilities.
- More than **50 percent** of all **rejected advisories** are also **Unix/Linux** operating systems related. •

Little over **72 percent** of all **networking-**related advisories are for **Cisco, F5** and **Juniper**

- About Microsoft:
- **2.56%** of all **advisories** were for **Microsoft**, which put them (again) in **eighth place** in vendor ranking.
- **57.6%** ↑ (2022: **56 percent)** of all **zero-days** were related to **Microsoft** products (**first place**).
- **None** of the top four vendors with the most advisories (**SUSE, Red Hat, Ubuntu, Ubuntu**) had any **zero-day** reported in 2023

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

2023 total advisory count: 9,402 ↑ (2022: 7,097)

As expected, 2023 had the highest number of advisories since Secunia started reporting them.

#	Year	# of advisories
1	2023	9402
2	2022	7097
3	2020	7065
4	2016	6348
5	2017	6262
6	2021	6153
7	2018	6101
8	2014	6004
9	2015	5934
10	2019	5837

Figure 1: Top ten years with most advisories

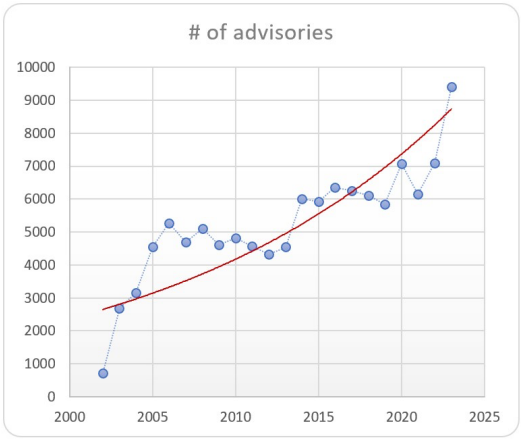


Figure 2: Chart with advisory trendline over the years

This year:	#	Change (last year)
Total # of advisories	9,402	↑ (7,097)
Unique vendors	291	↑ (279)
Unique versions	1,437	↓ (1,801)
Unique versions	1,794	↓ (1,801)
Rejected advisories *	1,500	↑ (1,108)
		↑ increased ↓lower ↔ same

** **1,500 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

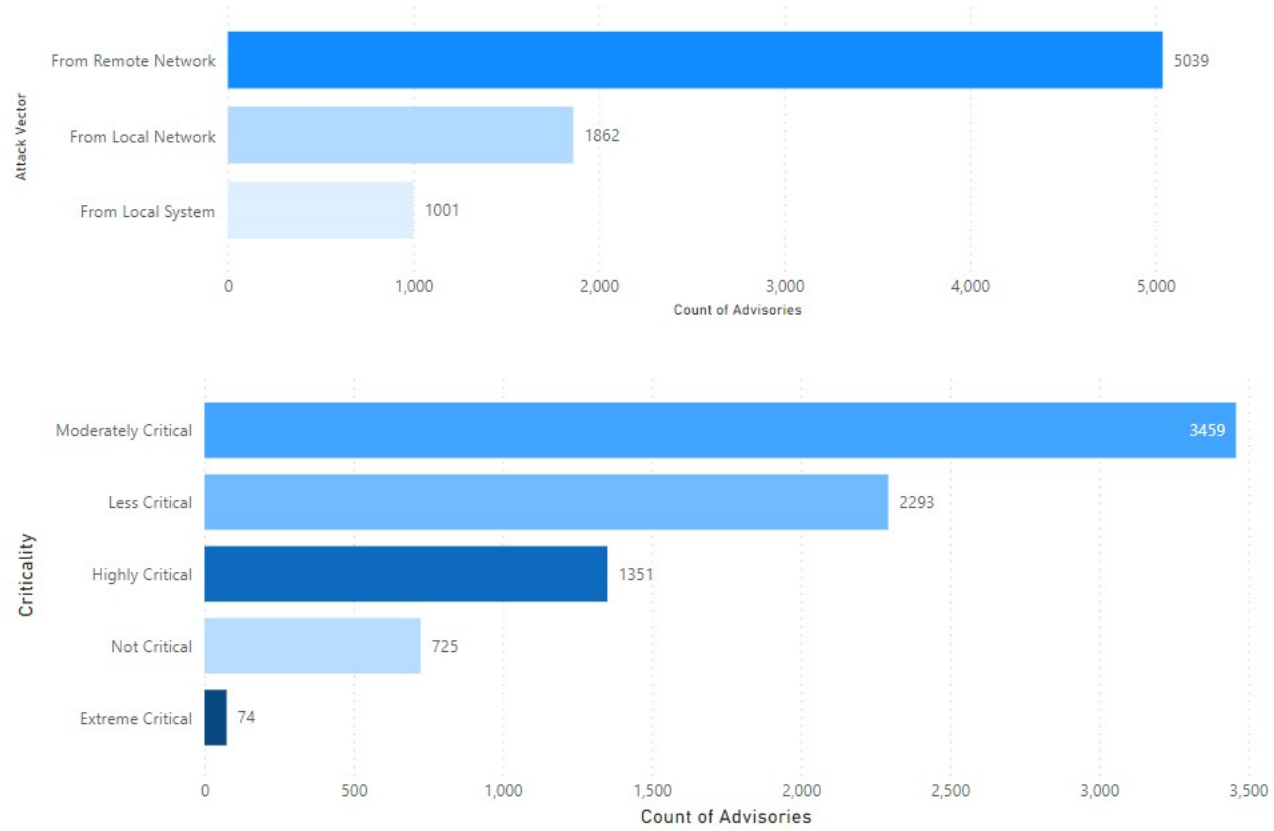


Figure 3: Overview Criticality and Attack Vector

More information about the variables used in the above charts:

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

Though not 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 Impact (Consequence of exploited)

impact Name	Count of Advisories
System access	2222
DoS	1707
Exposure of sensitive information	1149
Security Bypass	1110
Privilege escalation	935
Manipulation of data	280
Cross Site Scripting	200
Unknown	180
Spoofing	114
Hijacking	4
Brute force	1
Total	**7902**

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 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 is able to 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.

Unknown

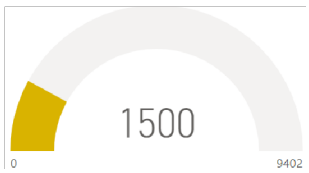
Rejection advisories.

There are large number of vulnerabilities posted in the National Vulnerability Database (NVD), by many vendors and CNA's. They are not always valid, they are not always assigned proper criticality ratings, and in some cases, a vulnerability may be legitimate but does not provide the attacker any benefit.

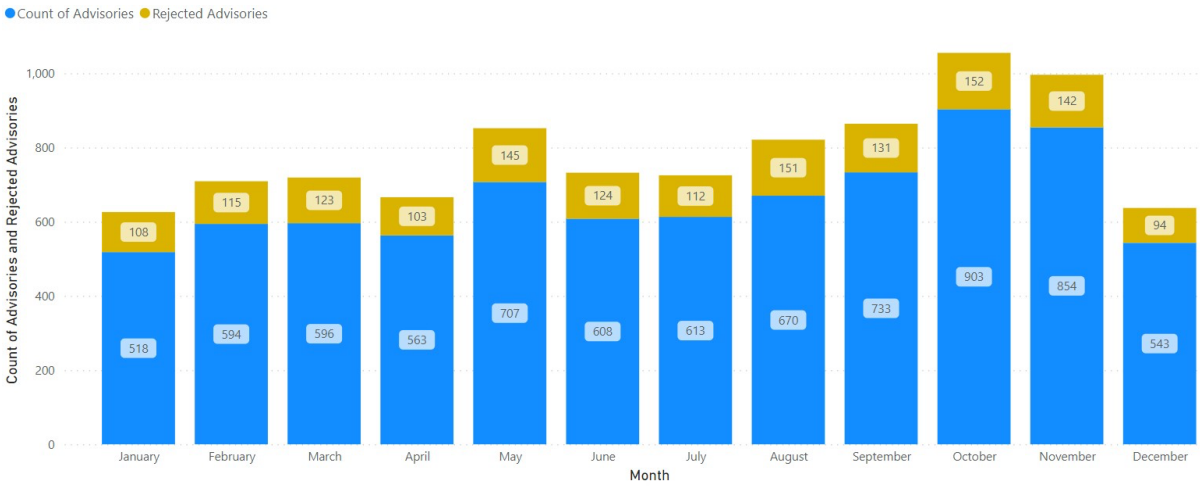
The Flexera Secunia Research team evaluates vulnerabilities from hundreds of sources, rescores them when necessary and even rejects vulnerabilities not worth your attention. **Rejection advisories** help you reduce the volume of vulnerabilities to be mitigated by helping you focus only on those that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

For compliance reasons, for example NERC (North American Electric Reliability Corporation), you may be required to report 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% of the total number of advisories are rejection advisories. 2023 result was 15.95% (1,500 rejection advisories)

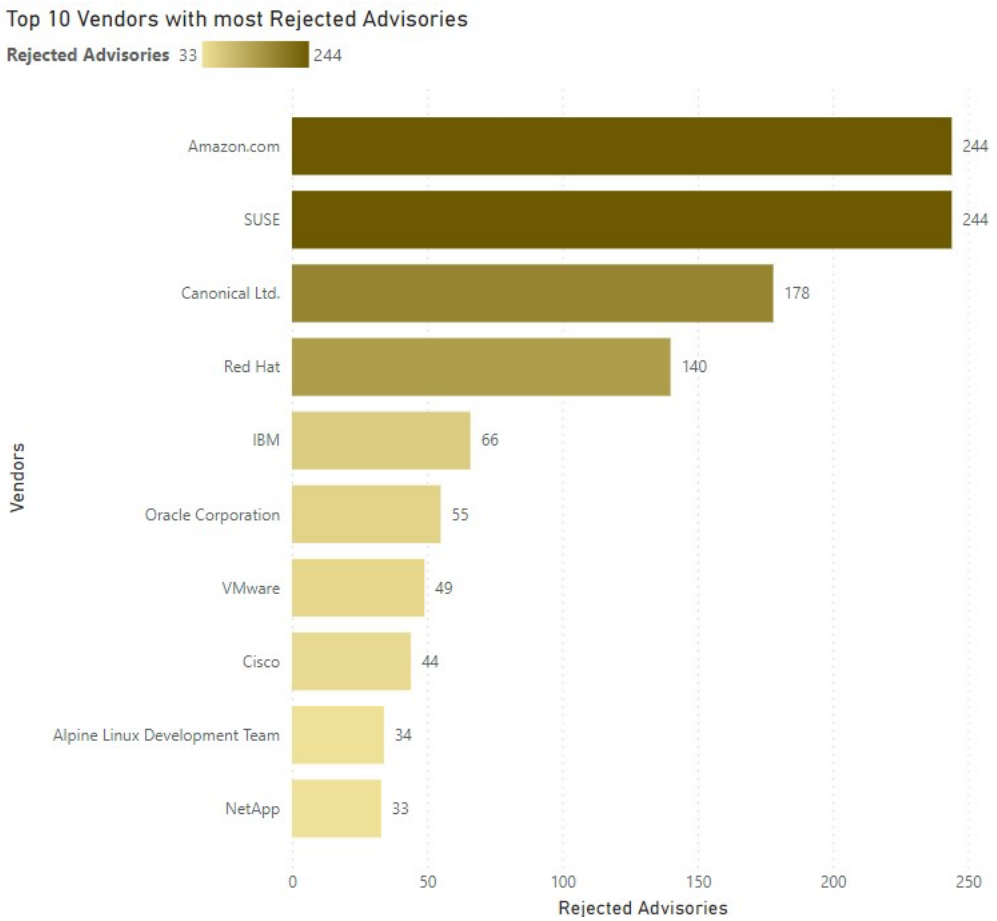


Overview rejection advisories



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

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:

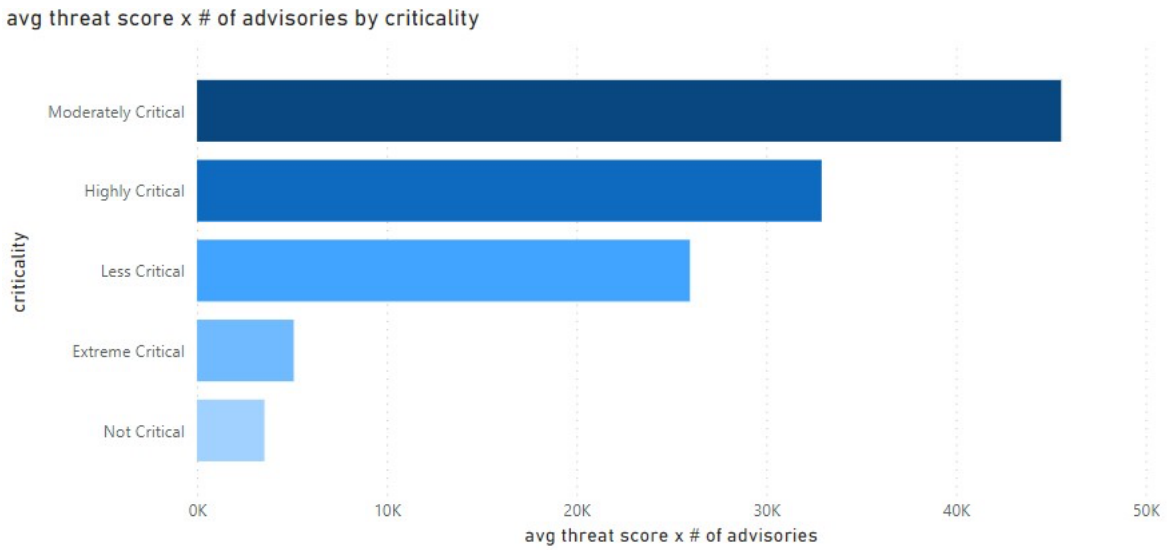
- The most popular method of thoughtful prioritization.
- If exploited, how bad could it affect your security? Is it designated to be of a high criticality? Patch

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 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.

criticality	Count of Advisories	avg. cvss score	avg. criticality score	# of recent exploits	# of ransomware links	#of malware links	# of Zero-day
Moderately critical	3458	7.29	14.37	67	71	700	10
Less critical	2293	6.79	12.73	35	22	384	
Highly critical	1352	9.22	25.09	89	88	412	47
Not critical	725	4.95	5.75	6	4	56	
Extremely critical	74	9.08	69.72	30	21	53	73
Total	**7902**	**7.28**	**15.68**	**177**	**160**	**1449**	**130**

rejection advisories not included.

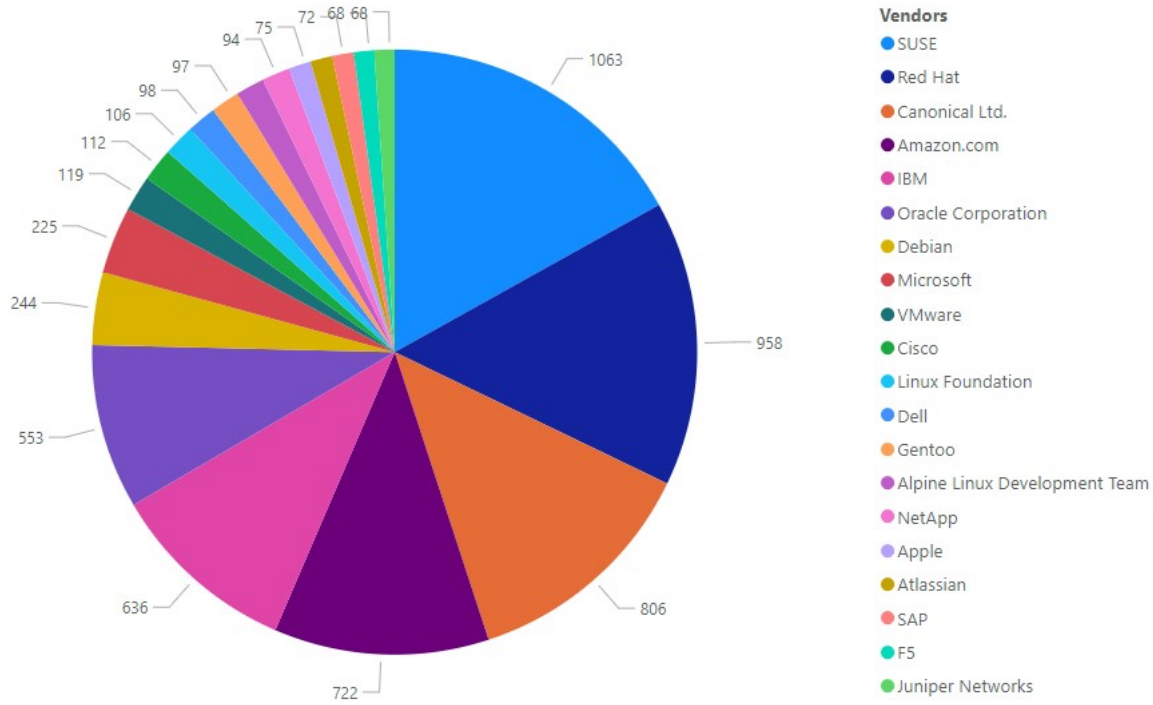
[More about Secunia Criticality (severity) scoring]

Take away 2:

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

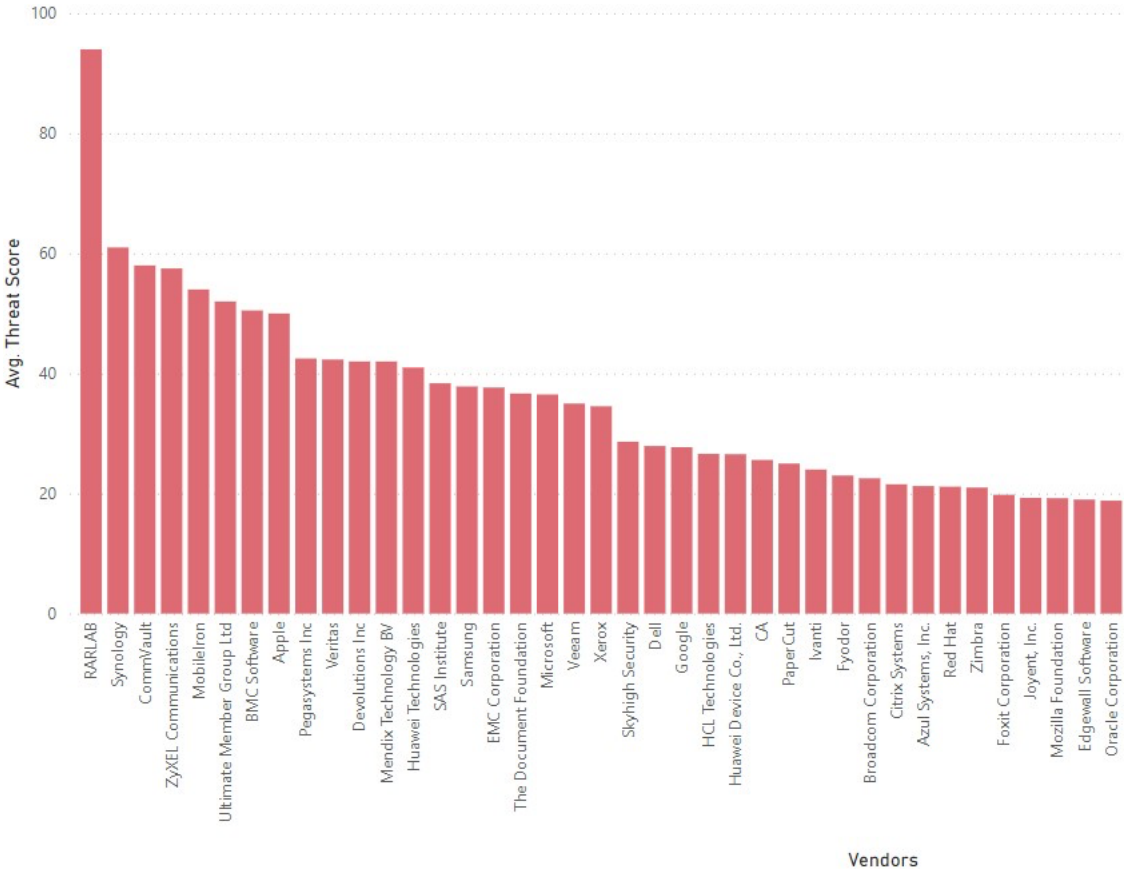
Vendor view

Top vendors with most advisories

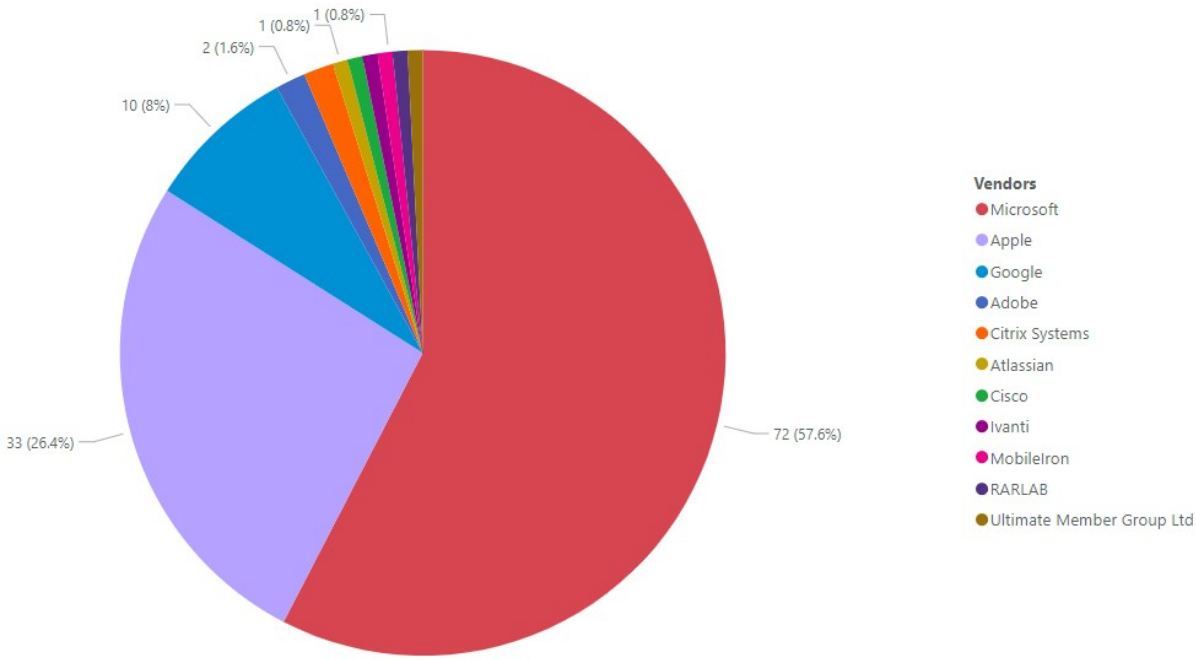


Note: Canonical Ltd. = Ubuntu

Top vendors with highest average threat score



Top vendors with zero-days



Product view

Products with the most zero-days advisories reported*

Products	# of zero day advisories
Apple iOS	16
Apple macOS	11
Microsoft Windows 10	9
Microsoft Windows 11	9
Microsoft Windows Server 2019	9
Microsoft Windows Server 2022	9
Google Chrome	7
Microsoft Edge (Chromium-Based)	7
Apple Safari	6
Microsoft Windows Server 2008	6
Microsoft Windows Server 2012	5
WebKitGTK	5
Microsoft 365 Apps for Enterprise (formerly Office 365 ProPlus)	4
Android	3
Citrix ADC	2
Microsoft .NET	2
Microsoft Excel 2013	2
Microsoft Windows 8.1	2
Adobe Acrobat DC	1
Adobe ColdFusion	1
Atlassian Confluence	1
Cisco 1000 Series Integrated Services Routers	1
Ivanti Endpoint Manager Mobile	1
Microsoft ASP.NET Core	1
Total	**130**

* Covered by Secunia Research

Top 20 of Operating Systems with most advisories

# of advisories	operating system
721	Amazon Linux 2,
537	SUSE Linux Enterprise Server (SLES) 15,
454	Ubuntu Linux,
366	Oracle Linux,
338	SUSE Linux Enterprise Server (SLES) 12,
260	Debian,
251	Red Hat Enterprise Linux (RHEL),
231	Amazon Linux AMI,
146	Red Hat Enterprise Linux,
123	Gentoo Linux,
96	Alpine Linux,
96	SUSE Linux Enterprise Server (SLES) 15 SP1 LTSS,
90	Red Hat Enterprise Linux (RHEL) Extended Update Support,
41	CentOS,
33	Apple macOS,
15	NetApp Data ONTAP,
13	Linux Kernel,
13	Microsoft Windows Server 2022,
12	Microsoft Windows 11,
12	Microsoft Windows Server 2019,

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	# of advisories	avg. threat score	avg. cvss score
Apple Safari	13	44.46	8.88
Google Chrome	35	21.06	8.62
Microsoft Edge (Chromium-Based)	39	21.05	8.68
Mozilla Firefox	32	19.39	8.86
Mozilla SeaMonkey	5	32.60	8.80
Total	**124**	**23.60**	**8.73**

note: filtered on avg. threat score.

Zero-day vulnerabilities

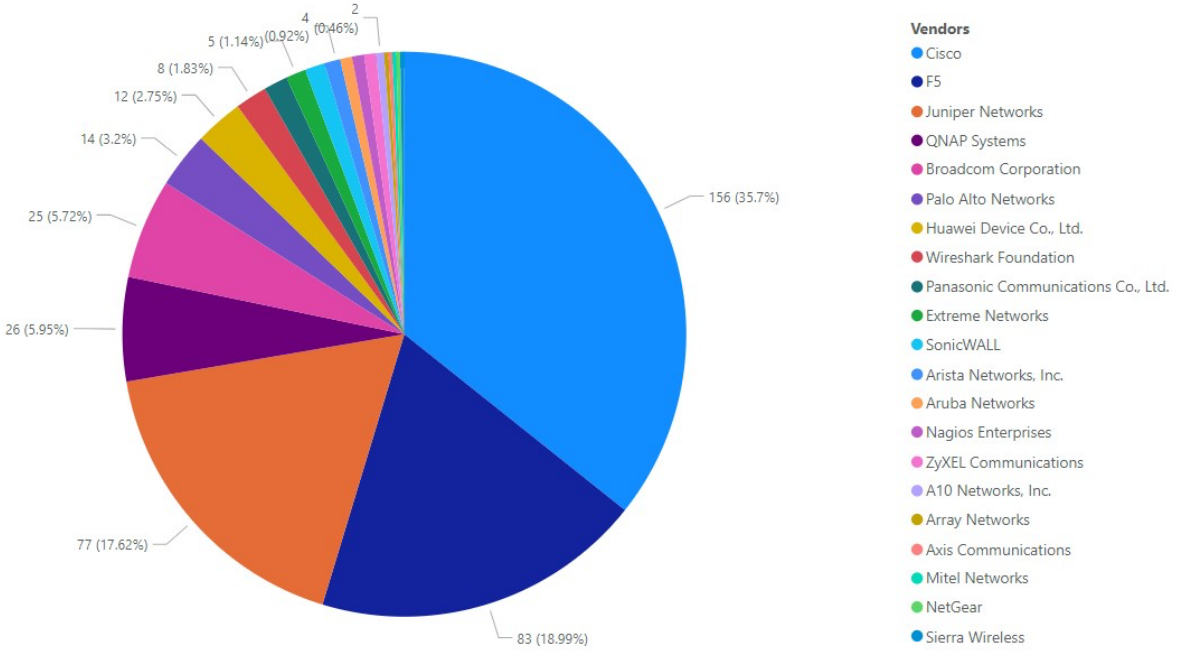
Products	Count of Advisories
Apple Safari	6
Google Chrome	7
Microsoft Edge (Chromium-Based)	7
Total	**20**

Browser Attack Vector

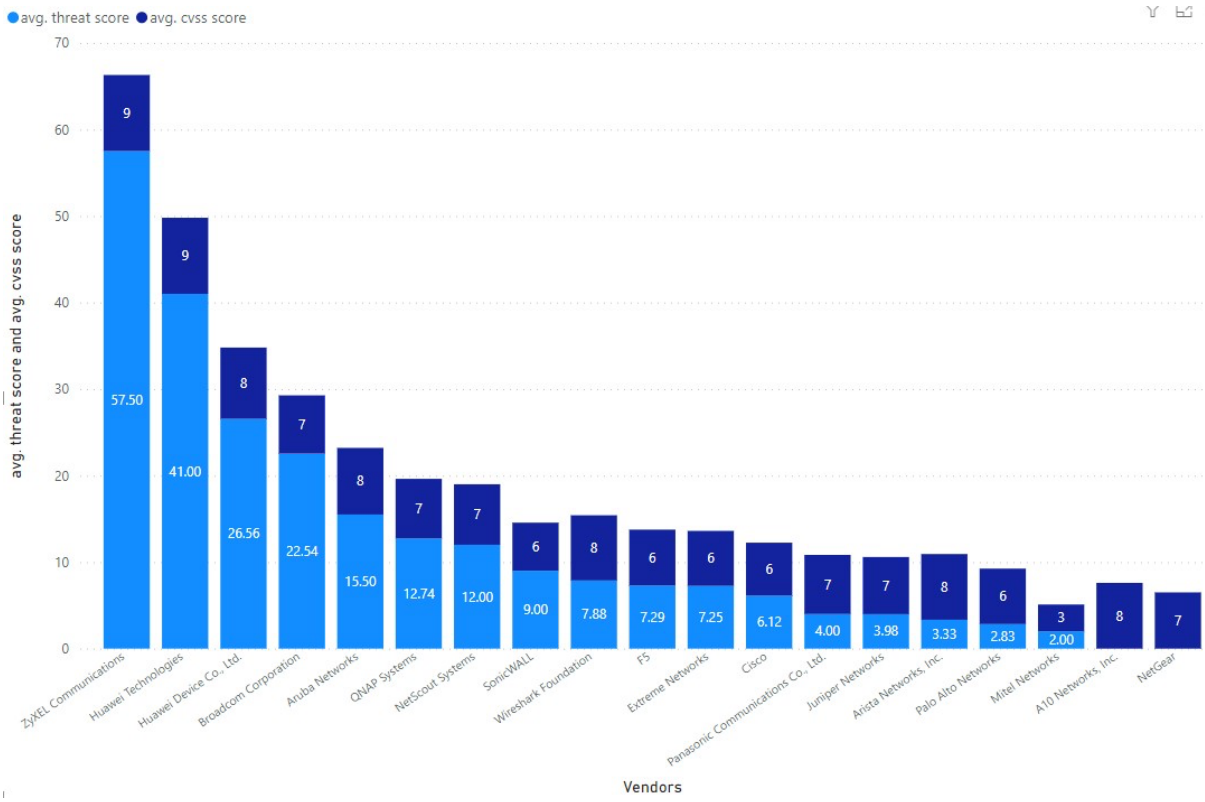
Products	From Remote
Apple Safari	100.00%
Google Chrome	100.00%
Microsoft Edge (Chromium-Based)	100.00%
Mozilla Firefox	100.00%
Mozilla SeaMonkey	100.00%
Total	**100.00%**

Networking-related advisories

Number of advisories per networking-related vendor



Average threat and CVSS score per networking-related vendor.



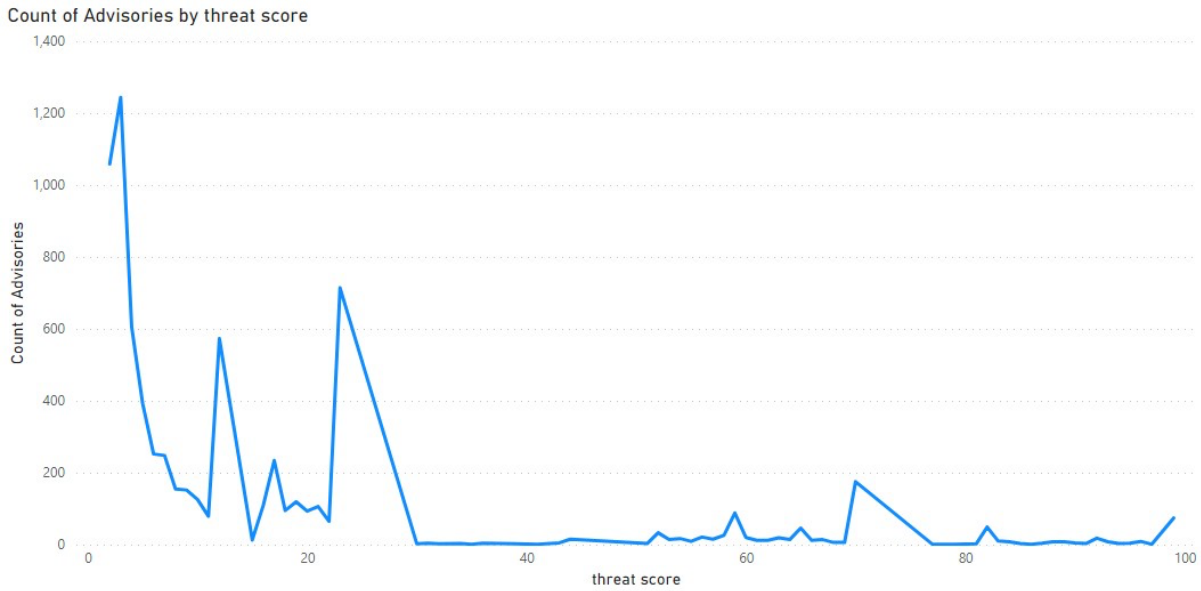
Threat intelligence

In a world where there are more than 23,000 new vulnerabilities (CVE's) every year, being smart about prioritizing remediation efforts is essential. Leveraging Threat Intelligence, another valuable layer of insight is provided to help you understand which of the vulnerabilities affecting your environment are actually 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.

SAIDs containing at least one CVE linked to:

#	Description
848	Historically Linked to Ransomware
3,275	Historically Linked to Malware
801	Recent Cyber Exploit
6,940	Linked to a Historical Cyber Exploits
7,814	Linked Penetration Testing Tools



criticality	Count of Advisories	avg. cvss score	avg. criticality score	# of recent exploits	# of ransomware links	#of malware links	# of Zero-day
Moderately critical	3458	7.29	14.37	67	71	700	10
Less critical	2293	6.79	12.73	35	22	384	
Highly critical	1352	9.22	25.09	89	88	412	47
Not critical	725	4.95	5.75	6	4	56	
Extremely critical	74	9.08	69.72	30	21	53	73
Total	**7902**	**7.28**	**15.68**	**177**	**160**	**1449**	**130**

CVE related statistics

Top 10 CVEs most referred to in Secunia Advisories

NVD largely relies on the vendors or third parties (CNAs) updating the CVE entries on MITRE (like more vendor advisory links). CVEs are reported for a component or library initially but could affect **tens or hundreds** of products "downstream", but that kind of detailed information is not always available in a timely manner.

Relying on NVD data is therefore not advised since not all products and version branches are covered. Other challenges with NVD are invalid or superseded vulnerabilities (with superseded fixes).
The table below shows the top 10 of most referred CVEs in Secunia Advisories.

CVE	# of Secunia Advisories	CVSS3 Score	Threat Score
CVE-2023-44487	225	7.50	59
CVE-2022-4304	134	5.90	4
CVE-2023-0286	132	7.40	19
CVE-2023-0215	123	7.50	4
CVE-2023-24998	100	7.50	3
CVE-2023-21967	98	5.90	3
CVE-2023-21930	96	7.40	4
CVE-2023-39325	96	7.50	19
CVE-2022-4450	94	7.50	4
CVE-2023-21937	91	3.70	3
Total	**1189**	**67.80**	**122**

.

Some interesting take-away from the CVE list:

CVE-2023-44487:

In August and September, threat actors unleashed the biggest distributed denial-of-service attacks in Internet history by exploiting a previously unknown vulnerability in a key technical protocol. (HTTP/2)

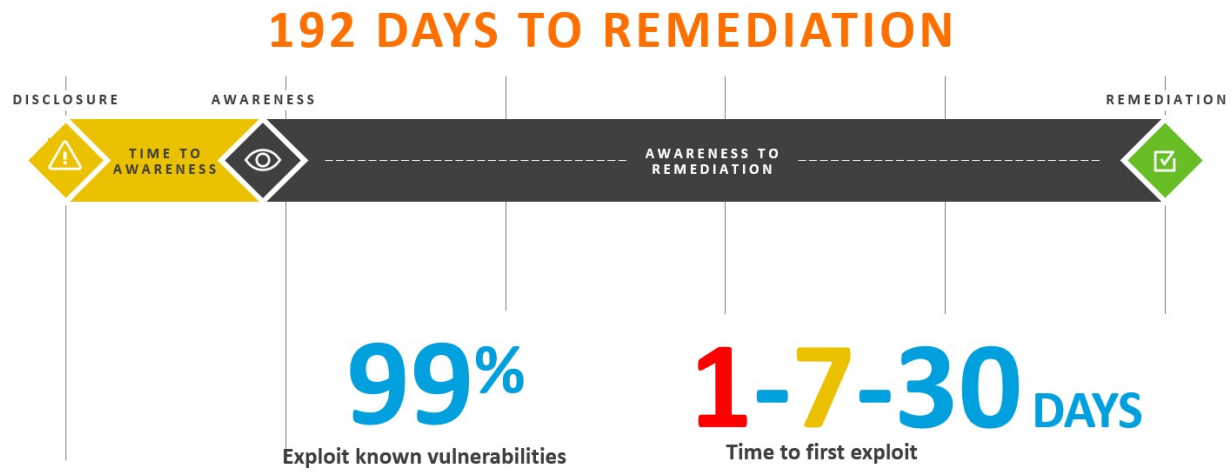
There were 225 Secunia Advisories mentioning this CVE.
This means that approx. 225 (downstream) products or product versions were affected by this Vulnerability.

MITRE registration date:	Sept.29,2023	
NVD/NIST registration date:	Oct.10,2023 – Last modified: Dec.20, 2023	
First Secunia Advisory:	Oct.10,2023 – Last modified: Jan. 9,2024	*(as of Jan .10, 2024)*

This is proving once again that Software Vulnerability Research is crucial for not only identifying, verifying and testing vulnerabilities, but also detecting all downstream software depending on these libraries and components (OSS) in the supply chain.

Patching

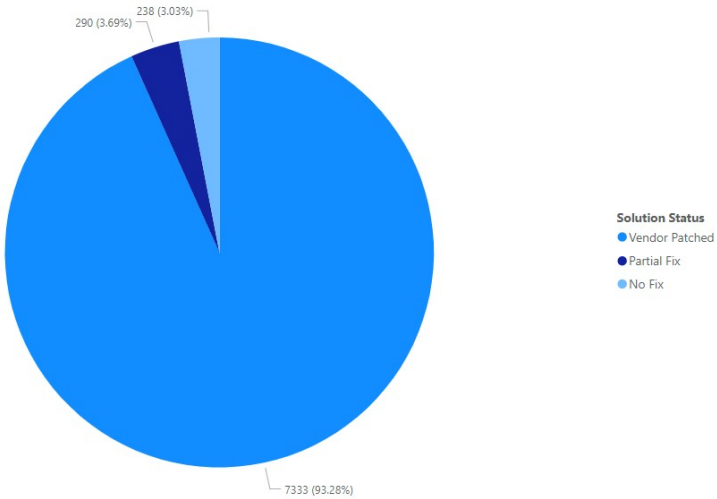
Most of 2023's vulnerabilities were vendor patched. In fact, most vulnerabilities are patched within 24 hours after disclosure.



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

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



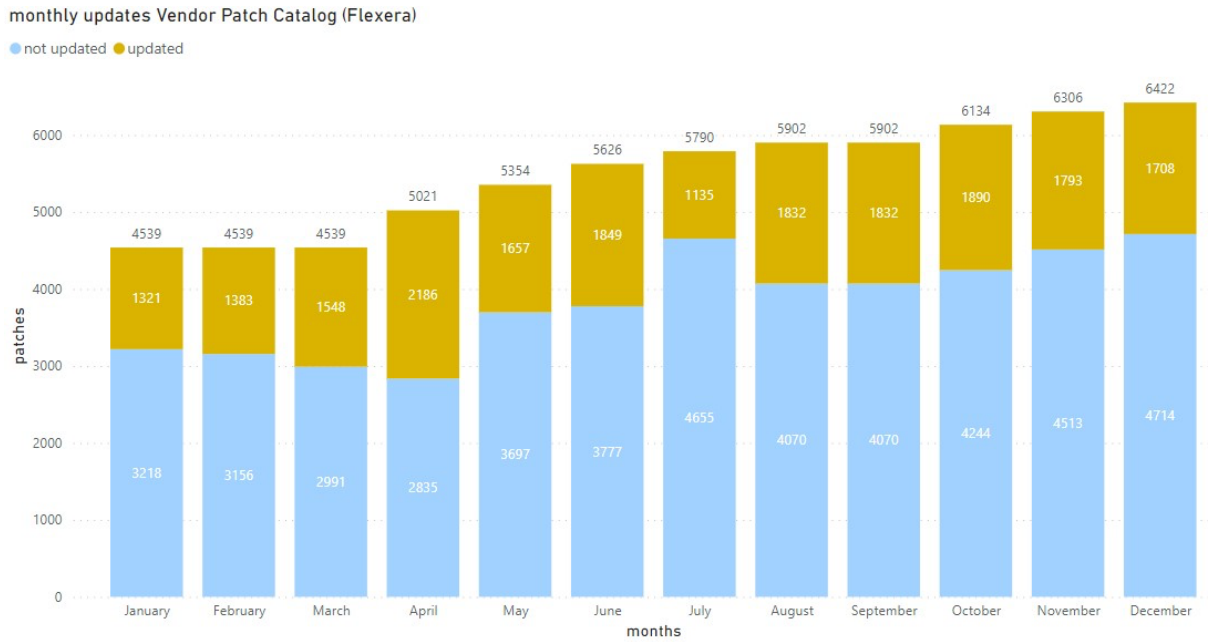
SVM patch statistics

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 about the Vendor Patch Catalog (VPM) including list of products covered.

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.)



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 saves customers billions of dollars in wasted technology spend. A pioneer in Hybrid ITAM and FinOps, Flexera provides award-winning, data-oriented SaaS solutions for technology value optimization (TVO), enabling IT, finance, procurement and cloud teams to gain deep insights into cost optimization, compliance and risks for each business service. Flexera One solutions are built on a set of definitive customer, supplier and industry data, powered by Technopedia, that enables organizations to visualize their Enterprise Technology Blueprint™ in hybrid environments—from on-premises to SaaS to containers to cloud.

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**