flexera™

MONTHLY VULNERABILITY INSIGHTS

Based on Data from Secunia Research

MARCH 2025

Author: Jeroen Braak

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 Monthly Vulnerability Insights Report* as stipulated in the terms of the license.

Content

Introduction

Welcome to our Monthly Vulnerability Insights by Flexera. This comprehensive, monthly review is based upon data from the Secunia Research team at Flexera who produces valuable advisories leveraged by users of Flexera's Software Vulnerability Research and Software Vulnerability Manager solutions.

The Secunia Research team is comprised of several security specialists who methodically test, verify and validate disclosed vulnerabilities from hundreds of sources. Since the founding of the Secunia Research team in 2002, it has been our goal to provide the most accurate and reliable source of vulnerability intelligence.

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 which 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.

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 issues 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 and 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

Secunia
Stay Secure

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.

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

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

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

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

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.

Monthly Summary

Total advisories: **946 (**last month: **967**)

Important conclusions from this month report are:

- Secunia reported **16** (last month : 21) Advisories without CVE that have a CVSS range from 8.8 to 5.0 :
  - **8.8** for python json-logger.3.x
  - **8.8** for Dotclear 2.x
- **10 Zero-day** Advisories reported for **Microsoft**, **Google**, **Broadcom** and **VMWare**.
- There was an unusual spike of **139** advisories being published on **March 18**, mainly for **Rocky Linux (93)** , **SUSE Liberty Linux (14)** and **SLES (4)** with high Threat scores.
- Microsoft released **extreme critical** advisories for Win11(see below) , Windows Server 2012, 2016/W10 , 2019,2022/2025 all with active exploits in the wild.
- The trend continues with the **Linux Foundation** producing a high volume of "vulnerabilities" with low threat or risk yet requiring significant validation effort , however this month lower than average. **(36 , last month 73)**
  Out of **48** Linux Foundation Advisories (last month :132), there were **36** (73) **Rejected** by Secunia, **12** (51) identified as **Not Critical** (learn more about Secunia criticality Rating)

Notable Vulnerability – and Threat Intelligence news:

Microsoft – Windows 11

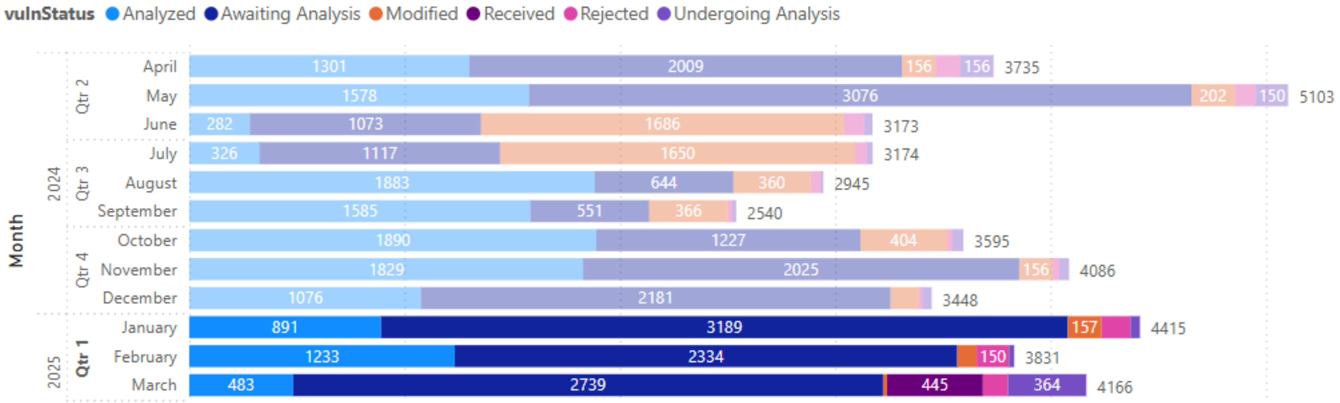
Secunia Advisory CVSS3: **9.8** |Threat Score : **99** | Zero-Day: **Yes** | Secunia Criticality Rating: **Extreme Critical** | Impact: **System access, DoS, Privilege escalation, Exposure of sensitive information, Spoofing, Security Bypass** | CVE references : CVE-2025-24984 CVE-2025-24993 CVE-2025-24044 CVE-2025-24988 CVE-2025-24084 CVE-2025-24054 CVE-2025-24985 CVE-2025-24992 CVE-2025-24035 CVE-2025-24995 CVE-2025-24059 CVE-2025-24051 CVE-2025-24997 CVE-2025-24061 CVE-2025-24071 CVE-2025-24076 CVE-2025-24987 CVE-2025-24996 CVE-2025-26645 CVE-2025-21247 CVE-2025-24067 CVE-2025-24991 CVE-2025-24048 CVE-2025-21180 CVE-2024-9157 CVE-2025-24994 CVE-2025-24066 CVE-2025-26633 CVE-2025-24055 CVE-2025-24056 CVE-2025-24046 CVE-2025-24050 CVE-2025-24072

Multiple vulnerabilities have been reported in Microsoft Windows 11, which can be exploited by malicious people with physical access to disclose sensitive information, by malicious, local users with physical access to bypass certain security restrictions, by malicious, local users to cause a DoS (Denial of Service) and gain escalated privileges, and by malicious people to conduct spoofing attacks, disclose sensitive information, bypass certain security restrictions, and compromise a vulnerable system.

NVD update

Flexera's Secunia Research team does not rely on NVD Vulnerability Data, and for good reason. As of now, the National Vulnerability Database (NVD) is experiencing a significant analysis backlog—with 15,547 of 40,704 CVEs from 2024 and 8,262 of 12,522 CVEs from 2025 still awaiting analysis. That's nearly half of all recent vulnerabilities left unprocessed.

In an environment where every day counts, relying on delayed and incomplete data poses a serious risk. Flexera's Secunia Research provides a verified, continuously updated vulnerability intelligence feed—empowering organizations to act fast, shrink their risk window, and stay ahead of potential exploits.



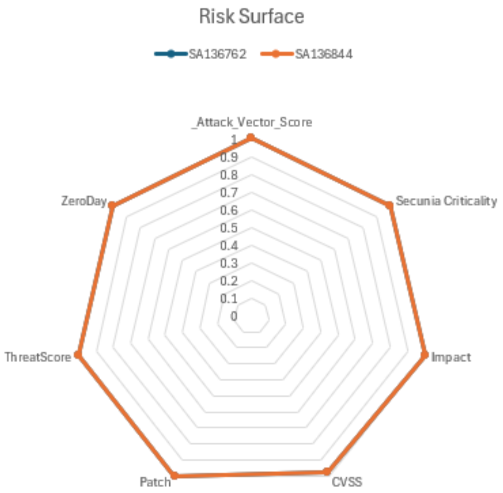
Risk Scoring Model:

There are many ways to prioritize Software Vulnerabilities ,
a previous article I wrote on LinkedIn : Key Elements of a Balanced Risk Scoring Model I shared some key components that can build a balanced risk scoring model. There is no standard in prioritizing vulnerability remediation , but the goal is to spark some discussion about what's important, and for obvious reasons , I've used the Secunia Research Data to perform the calculation.

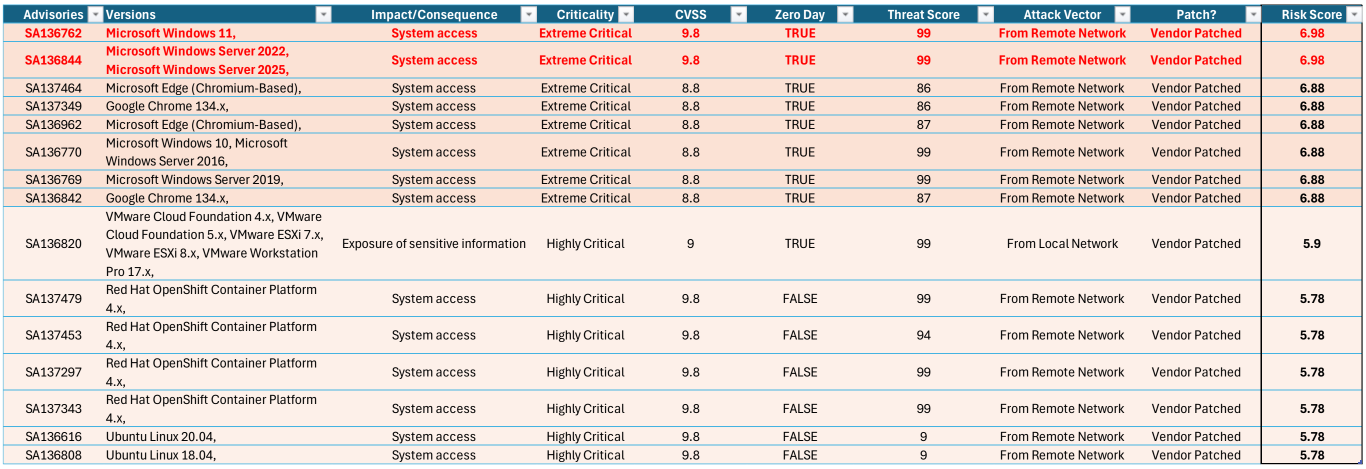
My current model is based on 7 variables that have been normalized to a score between 0 and 1 based on custom scaling or just using the score as is (CVSS)

- Attack Vector
- Secunia Criticality Score
- Impact / Consequence
- CVSS Score
- Patch Availability
- Threat Intelligence
- Zero Day

With that the Risk Score will be between 0 – 7
(0 = rejected)



Top Advisories released in March based on the calculated Risk Score:



Advisories	Versions	Impact/Consequence	Criticality	CVSS	Zero Day	Threat Score	Attack Vector	Patch?	Risk Score
SA136762	**Microsoft Windows 11,**	**System access**	**Extreme Critical**	**9.8**	**TRUE**	**99**	**From Remote Network**	**Vendor Patched**	**6.98**
SA136844	**Microsoft Windows Server 2022, Microsoft Windows Server 2025,**	**System access**	**Extreme Critical**	**9.8**	**TRUE**	**99**	**From Remote Network**	**Vendor Patched**	**6.98**
SA137464	Microsoft Edge (Chromium-Based),	System access	Extreme Critical	8.8	TRUE	86	From Remote Network	Vendor Patched	**6.88**
SA137349	Google Chrome 134.x,	System access	Extreme Critical	8.8	TRUE	86	From Remote Network	Vendor Patched	**6.88**
SA136962	Microsoft Edge (Chromium-Based),	System access	Extreme Critical	8.8	TRUE	87	From Remote Network	Vendor Patched	**6.88**
SA136770	Microsoft Windows 10, Microsoft Windows Server 2016,	System access	Extreme Critical	8.8	TRUE	99	From Remote Network	Vendor Patched	**6.88**
SA136769	Microsoft Windows Server 2019,	System access	Extreme Critical	8.8	TRUE	99	From Remote Network	Vendor Patched	**6.88**
SA136842	Google Chrome 134.x,	System access	Extreme Critical	8.8	TRUE	87	From Remote Network	Vendor Patched	**6.88**
SA136820	VMware Cloud Foundation 4.x, VMware Cloud Foundation 5.x, VMware ESXi 7.x, VMware ESXi 8.x, VMware Workstation Pro 17.x,	Exposure of sensitive information	Highly Critical	9	TRUE	99	From Local Network	Vendor Patched	**5.9**
SA137479	Red Hat OpenShift Container Platform 4.x,	System access	Highly Critical	9.8	FALSE	99	From Remote Network	Vendor Patched	**5.78**
SA137453	Red Hat OpenShift Container Platform 4.x,	System access	Highly Critical	9.8	FALSE	94	From Remote Network	Vendor Patched	**5.78**
SA137297	Red Hat OpenShift Container Platform 4.x,	System access	Highly Critical	9.8	FALSE	99	From Remote Network	Vendor Patched	**5.78**
SA137343	Red Hat OpenShift Container Platform 4.x,	System access	Highly Critical	9.8	FALSE	99	From Remote Network	Vendor Patched	**5.78**
SA136616	Ubuntu Linux 20.04,	System access	Highly Critical	9.8	FALSE	9	From Remote Network	Vendor Patched	**5.78**
SA136808	Ubuntu Linux 18.04,	System access	Highly Critical	9.8	FALSE	9	From Remote Network	Vendor Patched	**5.78**

Risk Score Thresholds

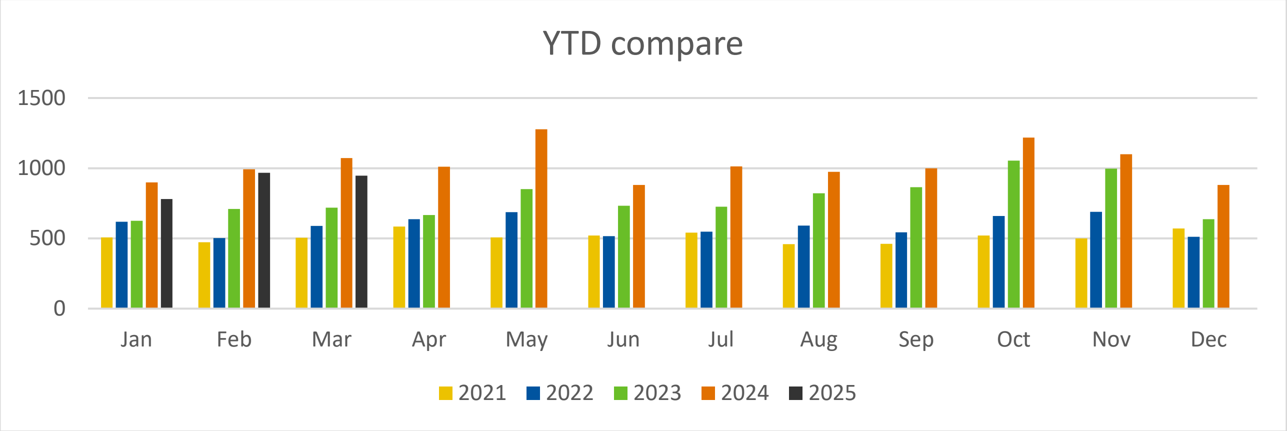
Attack Vector	Secunia Criticality	Impact Severity
Remote Network → 1.0	Extreme Critical → 1.0	System Access → 1.0
Local Network → 0.5	Highly Critical → 0.8	Privilege Escalation, Spoofing → 0.9
Local System → 0.2	Moderately Critical → 0.6	XSS, Hijacking → 0.8
Unknown → 0.0	Less Critical → 0.4	Info Exposure, Data Manipulation → 0.7
	Not Critical → 0.2	DoS, Security Bypass → 0.6
	Rejected → 0.0	System Info Exposure, Unknown → 0.5

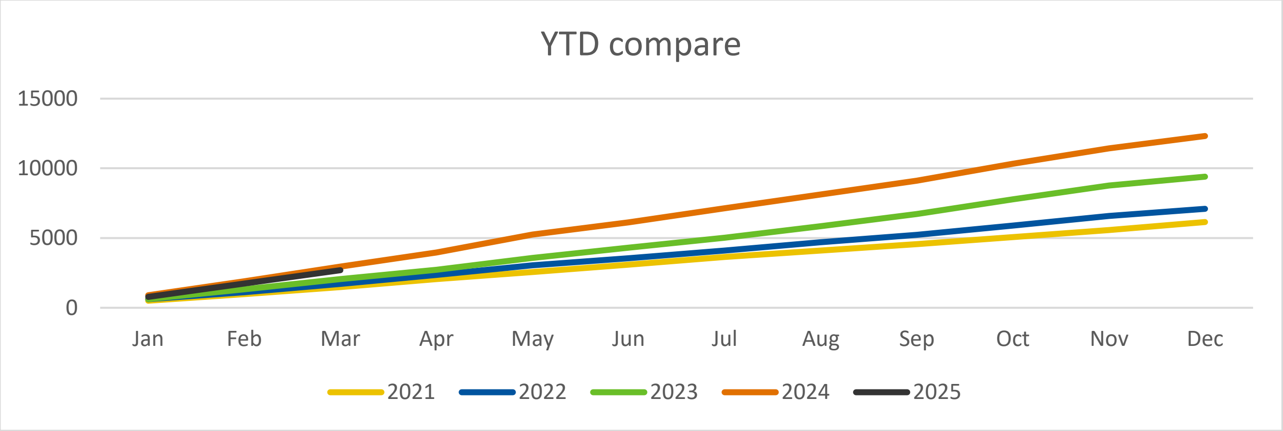
CVSS Score	Patch Availability	Threat Score
CVSS v3 ÷ 10 → 0.0 - 1.0	Vendor Patched → 1.0	71+ → 1.0
	Partial Fix, Workaround → 0.5	45 - 70 → 0.8
	No Fix / Unknown → 0.0	24 - 44 → 0.6
		13 - 23 → 0.4
		1 - 12 → 0.2
		0 or unranked → 0.0

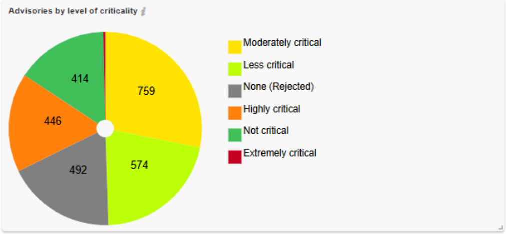
Zero-Day	Risk Score Formula	
True → 1.0	Risk Score =	Sum of all scores
False → 0.0	Higher Score = Higher Risk	Used for prioritization & patching

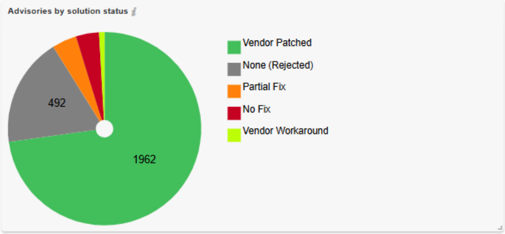
Year-to-date overview

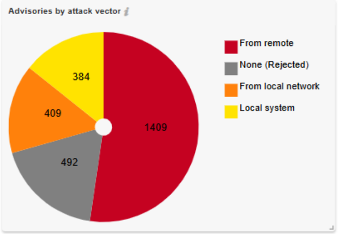
As of **March 31,2025**, the year-to-date total is **2,694** Advisories ↓ which is lower than 2023: **2,964** YTD Advisories)

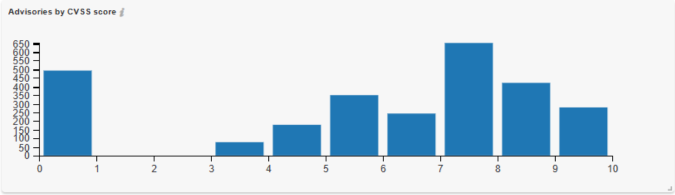


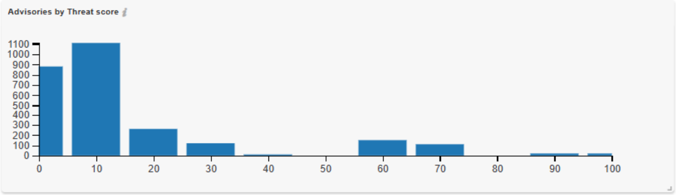












Monthly data

This month, a total of **946** ↓ (last month: **967**) advisories were reported by the Secunia Research Team.

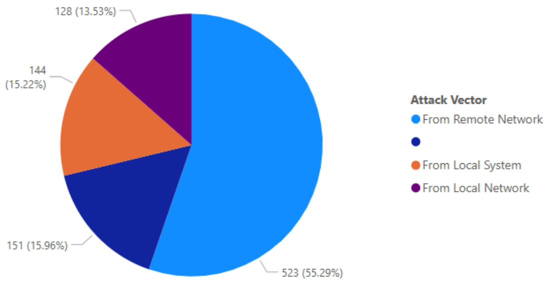
This month:	**#**	**Change** *(last month):*
Total # of advisories	**946**	↓ ***(967)***
Unique Vendors	**94**	↑ ***(87)***
Unique Products	**303**	↓ **(351*)***
Unique Versions	**373**	↓ ***(419)***
Rejected Advisories *	**151**	↓ ***(185)***
NEW Advisories without CVE ID	**16**	↓ ***(21)***
Advisories with Threat Score (>0)	**656**	↑ **(551)**
Total Unique CVE ID's reported	**2,895**	↑ **(2,699)**

↑ increased ↓lower ↔ same

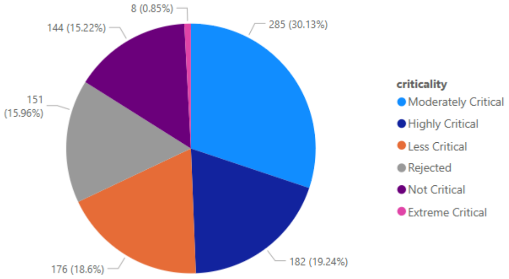
** **151** advisories have received the "rejected" status which means in general that leveraging it would require one or more violations of security best practices (e.g., product not securely configured or not used securely) or that it was "too weak of a gain" (e.g., administrative, local users already being too privileged so that additional gain becomes neglectable). More information about rejections can be found in the rejection section.*

Vulnerability information

Advisories by attack vector

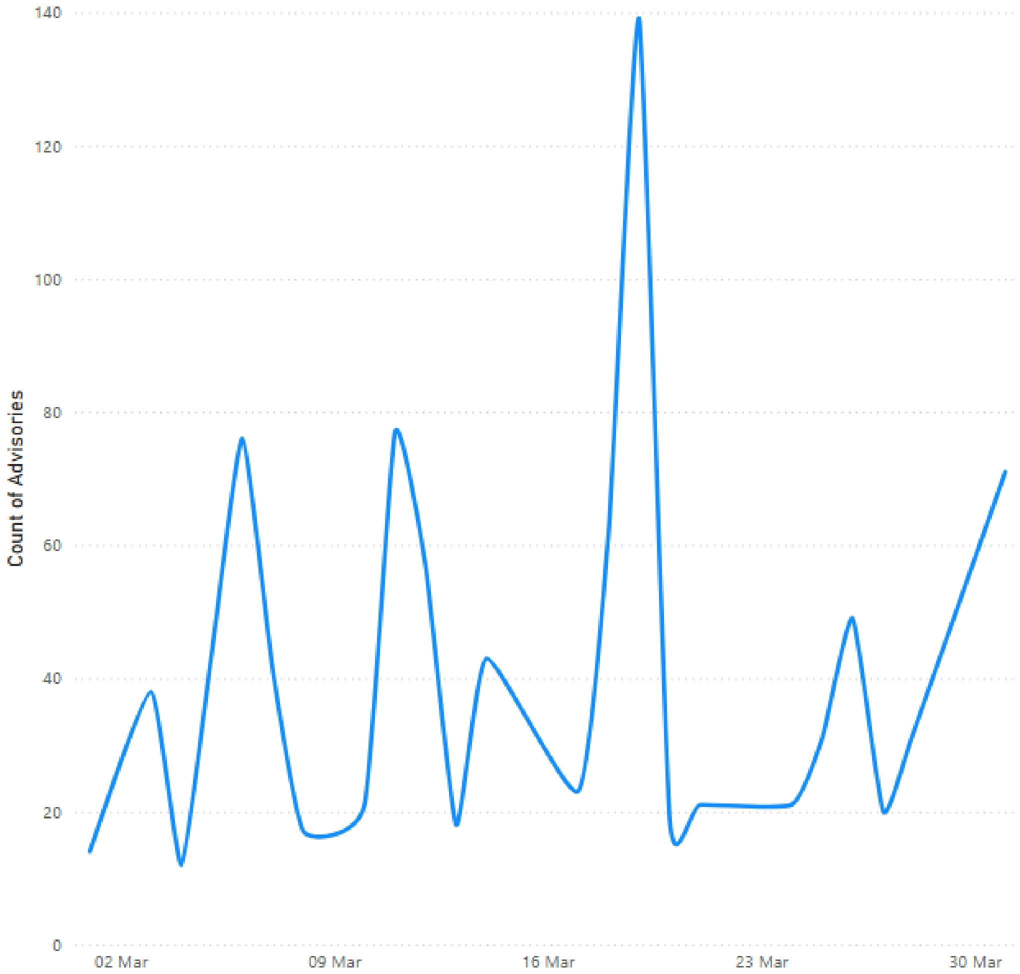


Advisories by criticality



Advisories per day

Below an overview of the daily advisory count.

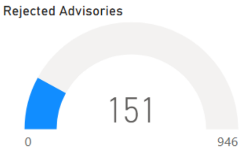


Year	Month	Day	Count of Advisories
2025	March	1	14
2025	March	3	38
2025	March	4	12
2025	March	5	44
2025	March	6	76
2025	March	7	41
2025	March	8	17
2025	March	10	21
2025	March	11	77
2025	March	12	57
2025	March	13	18
2025	March	14	43
2025	March	17	23
2025	March	18	62
2025	March	19	139
2025	March	20	19
2025	March	21	21
2025	March	24	21
2025	March	25	31
2025	March	26	49
2025	March	27	20
2025	March	28	32
2025	March	31	71
Total			**946**

Advisories without CVE

Advisories	Versions	Cvss3_score	criticality	Description	solution_status
SA136900	python-json-logger 3.x,	8.8	Highly Critical	python-json-logger Arbitrary Code Execution Vulnerability	Vendor Patched
SA137296	Dotclear 2.x,	8.8	Moderately Critical	Dotclear Multiple Vulnerabilities	Vendor Patched
SA136768	MOVITOOLS MotionStudio 6.x,	7.8	Moderately Critical	MOVITOOLS MotionStudio Arbitrary Code Execution Vulnerability	Vendor Patched
SA134925	Vertica 23.x,	6.1	Less Critical	Vertica Management Console Cross-Site Scripting Vulnerability	Vendor Patched
SA136704	CA Gen 8.x,	5.6	Moderately Critical	CA Gen z/OS Common Modules Unspecified Vulnerability	Vendor Patched
SA136763	Mattermost 10.x, Mattermost 9.x,	5.6	Moderately Critical	Mattermost Server Multiple Unspecified Vulnerabilities	Vendor Patched
SA137132	Dell BSAFE Crypto-J 6.2.x,	5.6	Moderately Critical	Dell BSAFE Crypto-J Unspecified Vulnerability	No Fix
SA137200	COMMON COMPONENTS AND SERVICES FOR Z/OS 15.x,	5.6	Moderately Critical	Common Components and Services for z/OS Apache Tomcat Unspecified Vulnerability	Vendor Patched
SA137215	Magnolia 6.x,	5.6	Moderately Critical	Magnolia Multiple Unspecified Vulnerabilities	Vendor Patched
SA137475	GNU MPFR 4.x,	5.6	Moderately Critical	GNU MPFR Unspecified Memory Corruption Vulnerability	Vendor Patched
SA137500	Cygwin 3.x,	5.6	Moderately Critical	Cygwin update for mpfr and mingw64-mpfr	Vendor Patched
SA137510	SUSE Linux Enterprise Server (SLES) 15 SP5, SUSE Linux Enterprise Server for SAP Applications 15 SP5,	5.5	Not Critical	SUSE update for apparmor	Vendor Patched
SA136427	CA Database Management for Db2 for z/OS 20.x,	5	Less Critical	CA Database Management for Db2 for z/OS Multiple Unspecified Vulnerabilities	Vendor Patched
SA136956	Deep Security Manager 20.x,	5	Less Critical	Trend Micro Deep Security Manager Multiple Unspecified Vulnerabilities	Vendor Patched
SA136958	Keras 3.x,	0	Rejected	Keras Rejection Notice	Unknown
SA137507	SUSE Linux Enterprise Server (SLES) 15 SP6,	0	Rejected	SUSE govulncheck-vulndb Rejection Notice	likely Fixed

Rejected advisories.

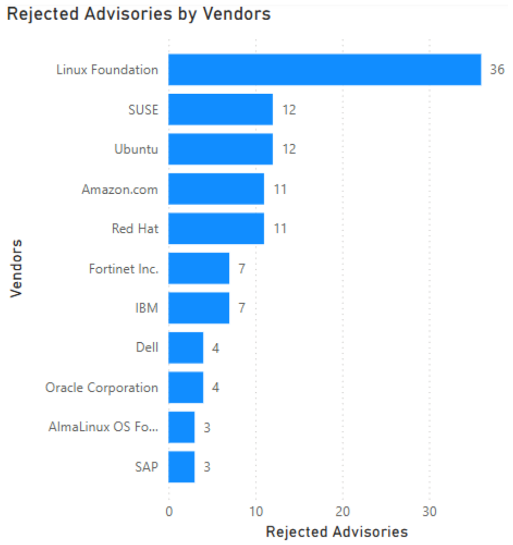


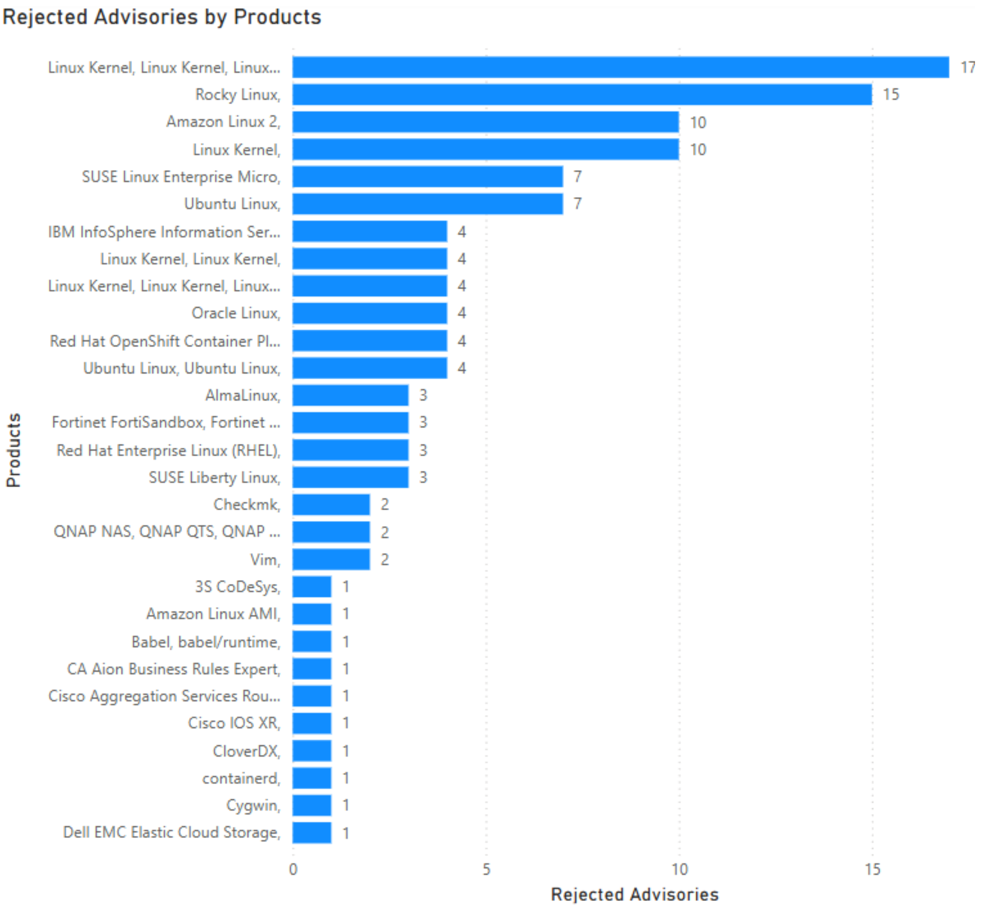
There are many vulnerabilities posted to the National Vulnerability Database (NVD) by a lot of people and companies. They are not always valid, assigned a proper criticality, and in some cases, a vulnerability may be legitimate but not afford the attacker any benefit.

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

An advisory may be rejected 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? It’s on all systems? **Patch**.

Asset Sensitivity:

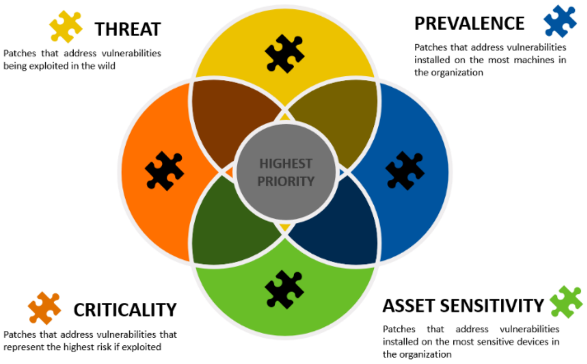
- What systems would result in the most risk if compromised?
- Is it a high-risk device? **Patch**.

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**.


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

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

Focusing on vulnerabilities with CVSS 7 or higher would address about 50 percent of exploits. Most exploits are CVSS scored between 4 and 7. Focusing

on vulnerabilities for the top 20 vendors would address only about 20 percent.

Take away 1:

Critical vulnerabilities do not necessarily present the most risk.

Leverage threat intelligence to better prioritize what demands your most urgent attention.

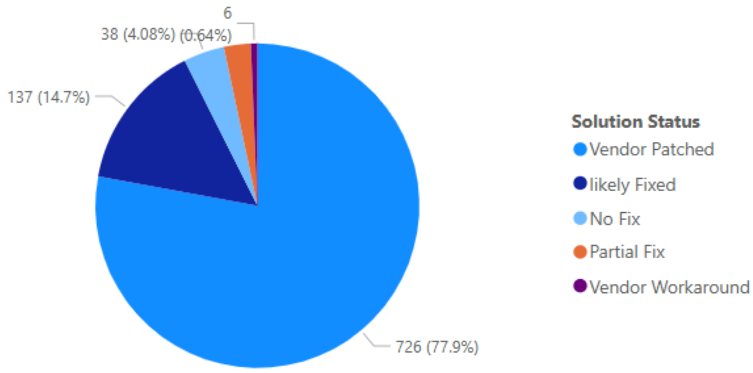
Organizations who do not have Threat Intelligence data should consider implementing this to ensure they have the complete picture.

Take away 2:

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

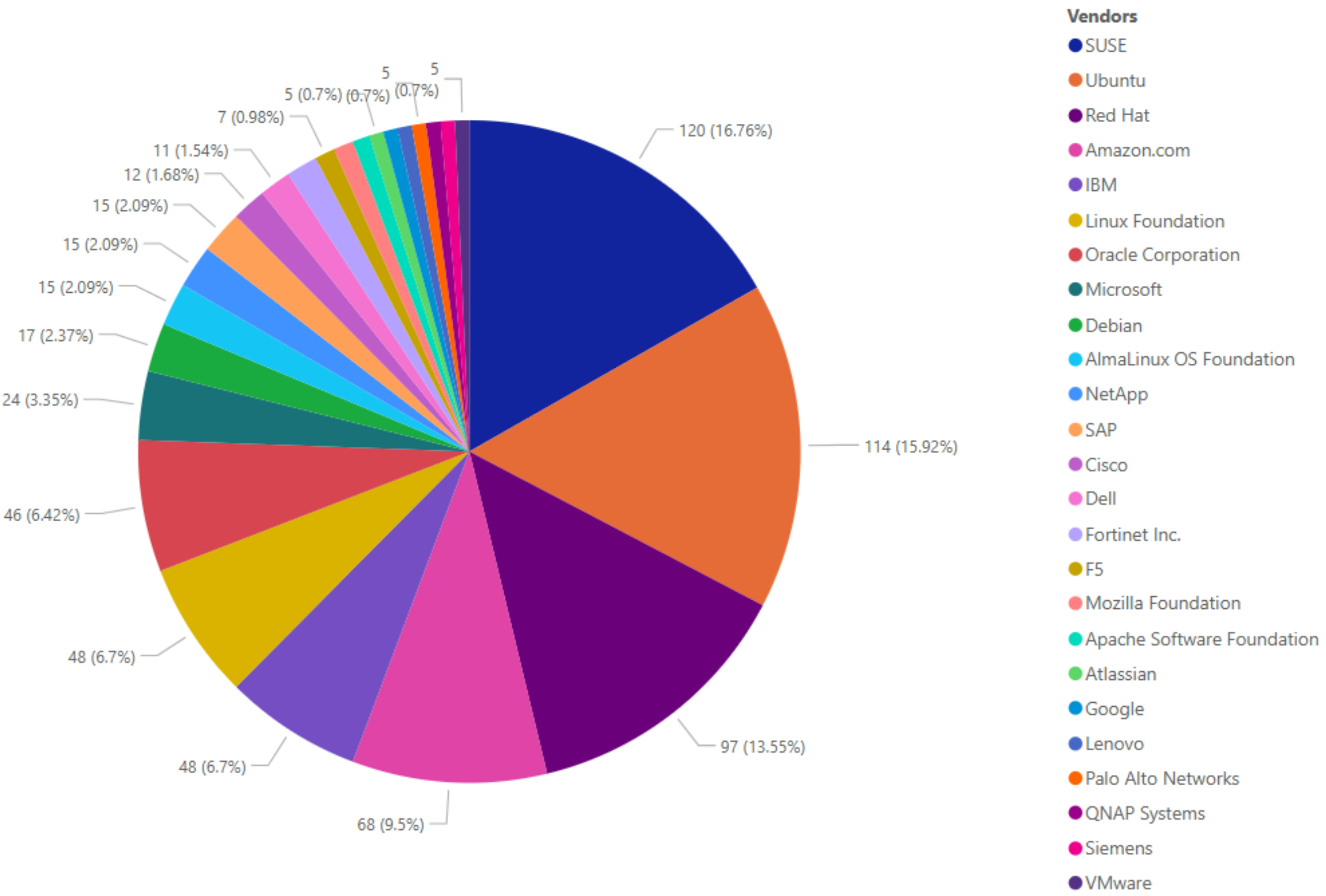
No fix: no patch available for this insecure version, therefore need to upgrade

likely (Possibly) fixed: related to a rejection advisory



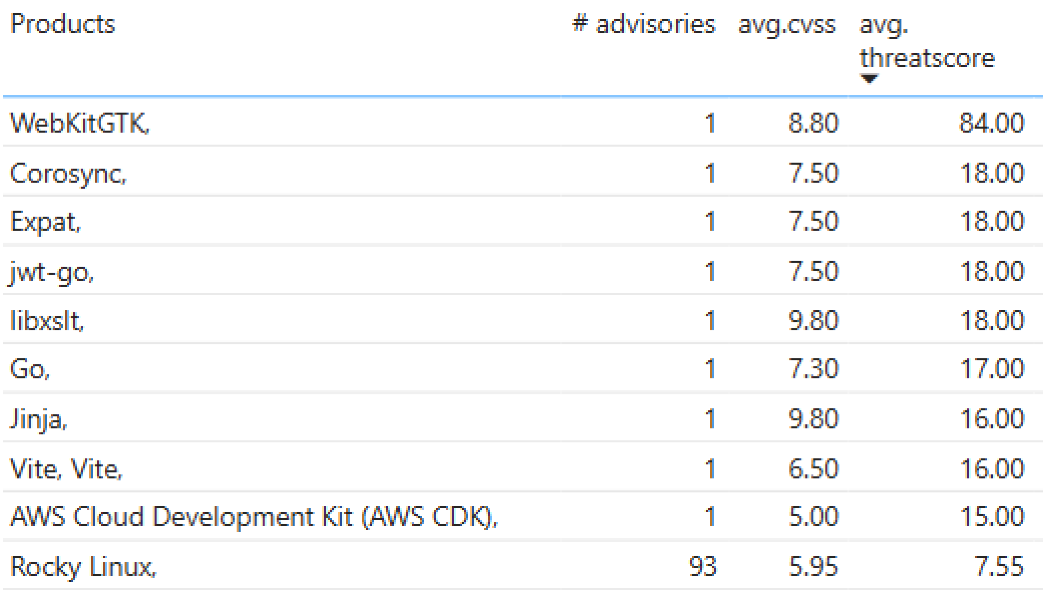
Vendor view

Top vendors with the most advisories



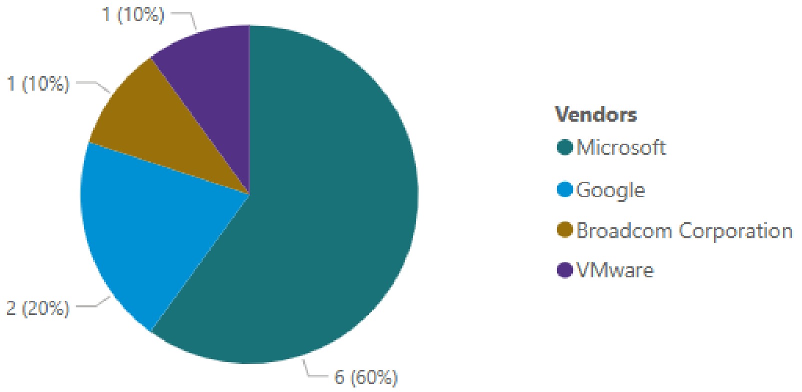
142 Advisories this month were open-source products or plugin, **93 from Rocky Linux**

top 10 Open Source based on Average Threat Score



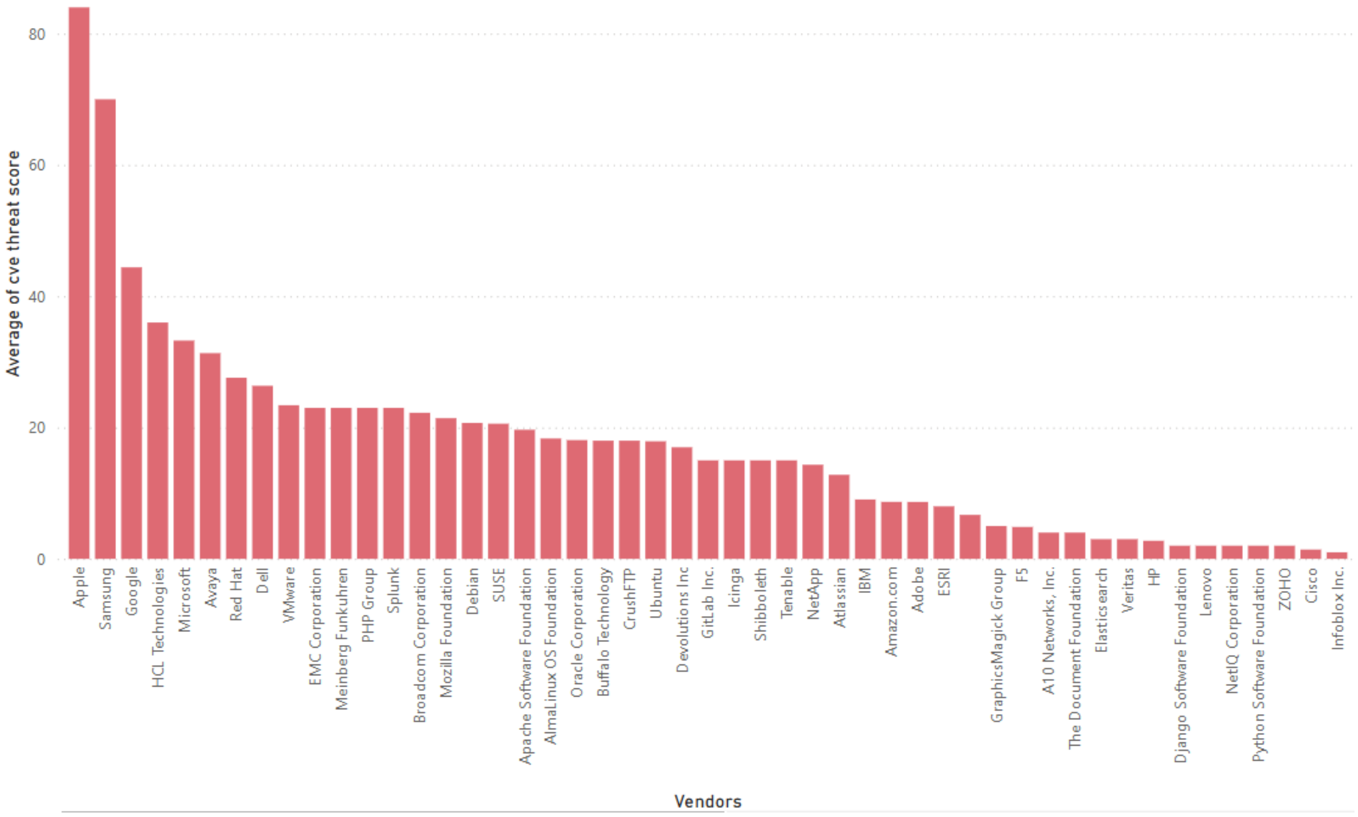
Products	# advisories	avg.cvss	avg. threatscore
WebKitGTK,	1	8.80	84.00
Corosync,	1	7.50	18.00
Expat,	1	7.50	18.00
jwt-go,	1	7.50	18.00
libxslt,	1	9.80	18.00
Go,	1	7.30	17.00
Jinja,	1	9.80	16.00
Vite, Vite,	1	6.50	16.00
AWS Cloud Development Kit (AWS CDK),	1	5.00	15.00
Rocky Linux,	93	5.95	7.55

Top vendors with zero-day



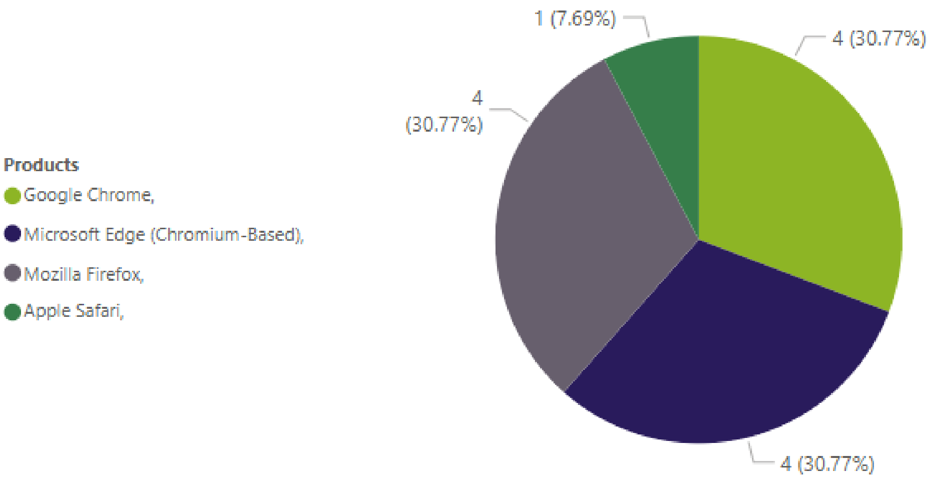
Advisories	Versions
SA136842	Google Chrome 134.x,
SA137349	Google Chrome 134.x,
SA136962	Microsoft Edge (Chromium-Based),
SA137464	Microsoft Edge (Chromium-Based),
SA136770	Microsoft Windows 10, Microsoft Windows Server 2016,
SA136762	Microsoft Windows 11,
SA136769	Microsoft Windows Server 2019,
SA136844	Microsoft Windows Server 2022, Microsoft Windows Server 2025,
SA136820	VMware Cloud Foundation 4.x, VMware Cloud Foundation 5.x, VMware ESXi 7.x, VMware ESXi 8.x, VMware Workstation Pro 17.x,
SA136697	VMware Fusion 13.x,

Top Vendors with highest average threat score



Browser-related advisories

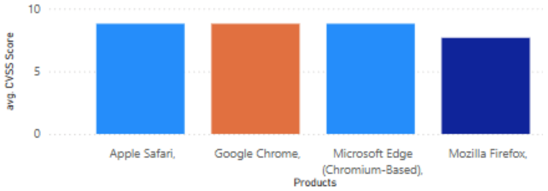
Advisories per browser



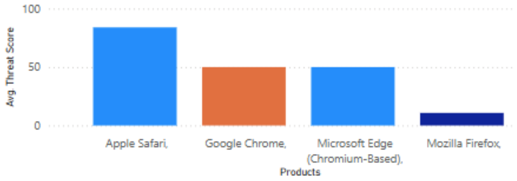
Browser zero-day vulnerabilities

Description	Advisories	Cvss3	ThreatScore	Consequence	solution_status
Google Chrome Multiple Vulnerabilities	SA136842	8.80	87.00	System access	Vendor Patched
Microsoft Edge (Chromium-Based) Multiple Vulnerabilities	SA136962	8.80	87.00	System access	Vendor Patched
Google Chrome Arbitrary Code Execution Vulnerability	SA137349	8.80	86.00	System access	Vendor Patched
Microsoft Edge (Chromium-Based) Arbitrary Code Execution Vulnerability	SA137464	8.80	86.00	System access	Vendor Patched

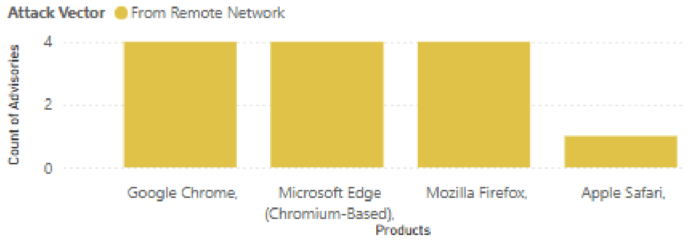
Average CVSS (criticality) score per browser



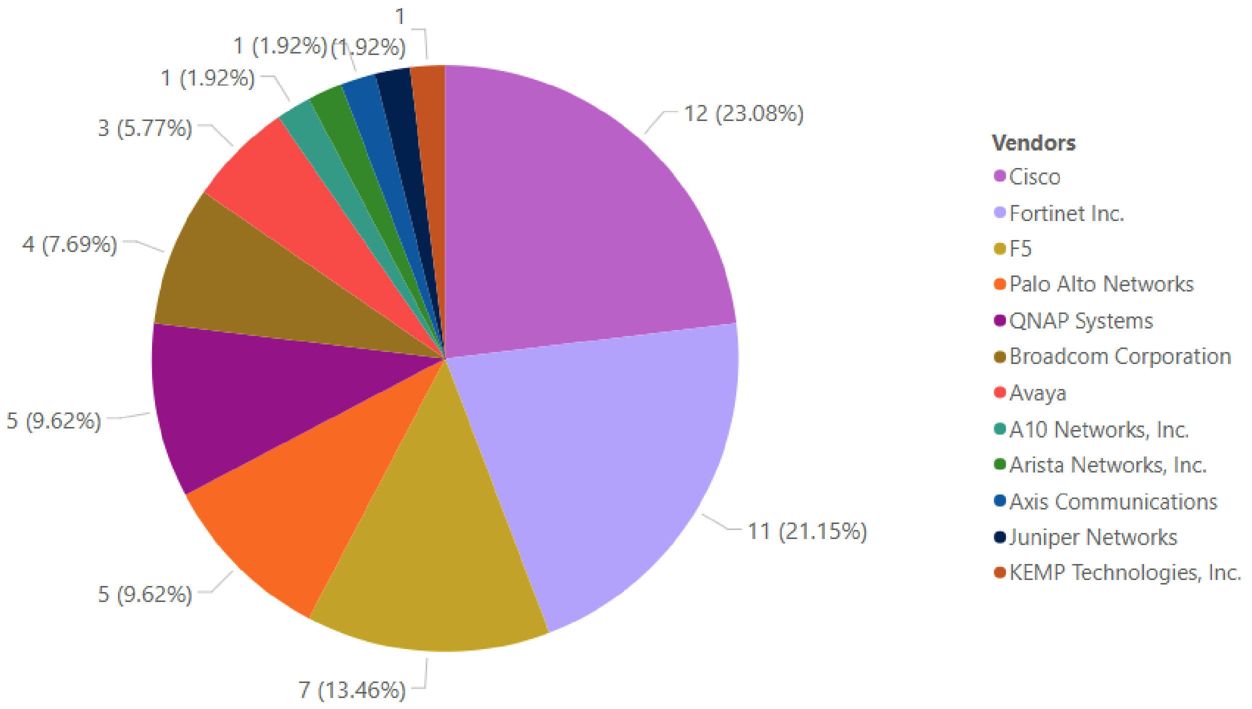
Average threat score per browser



What's the Attack Vector?



Networking related advisories

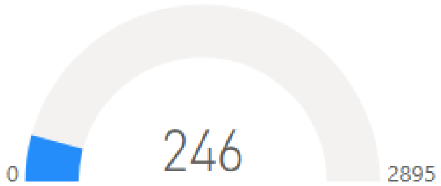


Threat intelligence

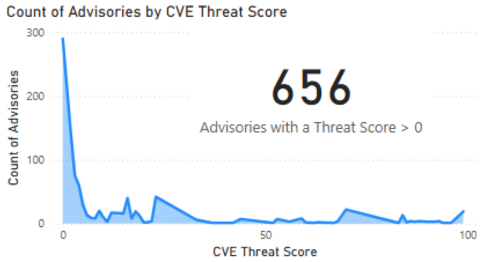
In a world where there are more than 25,000 new vulnerabilities every year, being smart about prioritizing remediation efforts is essential. Leveraging Threat Intelligence, another valuable layer of insight is provided to help you understand which of the vulnerabilities affecting your environment are 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 Software Vulnerability Research's vulnerability intelligence with a Threat Score that provides the ultimate prioritization tool for your busy desktop operations teams.

Count of malware-exploited CVEs



Count of advisories by CVE threat score



Threat intelligence advisory statistics

SAIDs with a threat score (1+)	**656** ↑ (551*)*	69.34%
SAIDs with no threat score (=0)	**290** ↓ *(416)*	30.66%

SAID: Secunia Advisory Identifier

Range	**# SAIDS**	***Last month***
Low-range threat score SAIDs (1-12)	385 ↑	*(307)*
Medium-range threat score SAIDs (13-23)	145 ↑	*(105)*
Very critical threat score SAIDs (71-99)	**59** ↓	*(83)*
Critical-range threat score SAIDs (45-70)	**51** ↓	*(53)*
High-range threat score SAIDs (24-44)	16 ↑	*(3)*

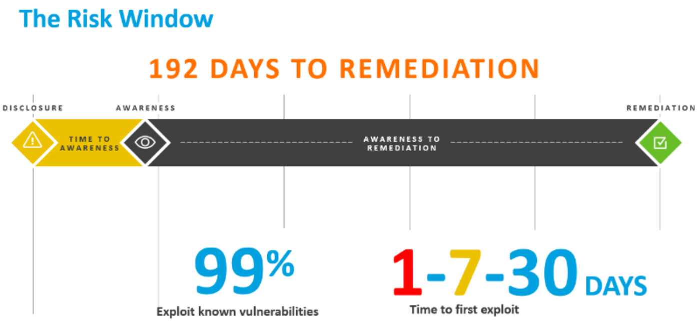
More information about how the Secunia team calculates the threat score:

- Evidence of exploitation
- Criteria for the threat Score Calculation
- Threat Score Calculation - Examples

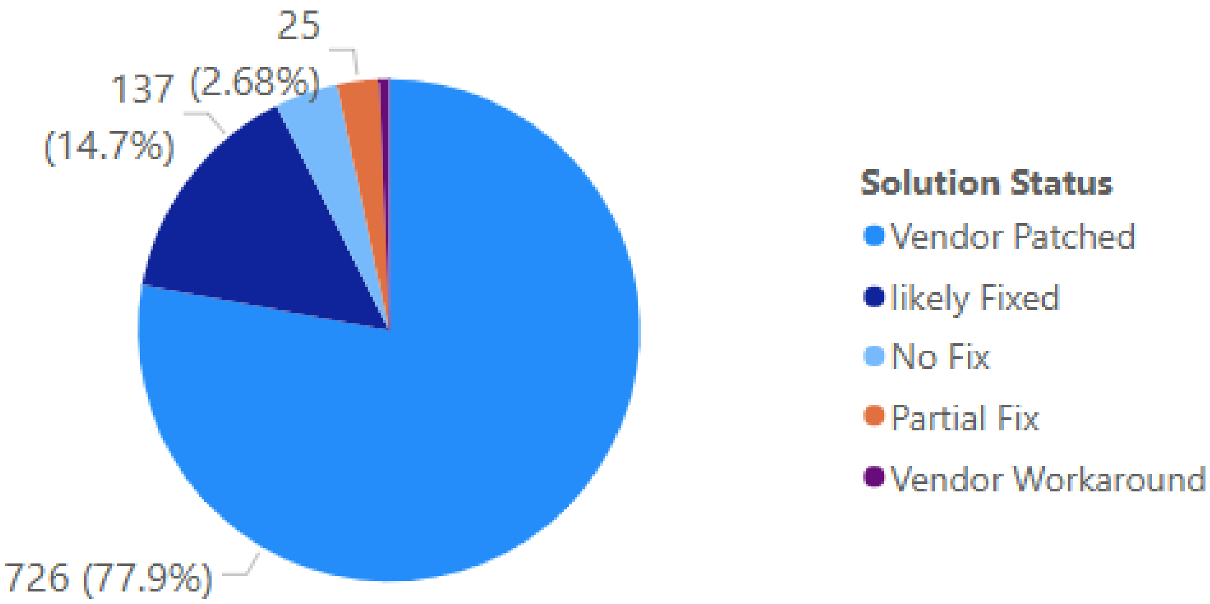
Patching

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

The challenge remains that organizations do not have full visibility or awareness when a vulnerability is disclosed (time to awareness). Another big challenge is the 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).

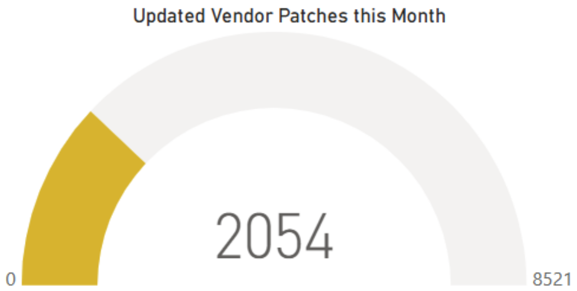


Vulnerabilities that are vendor patched



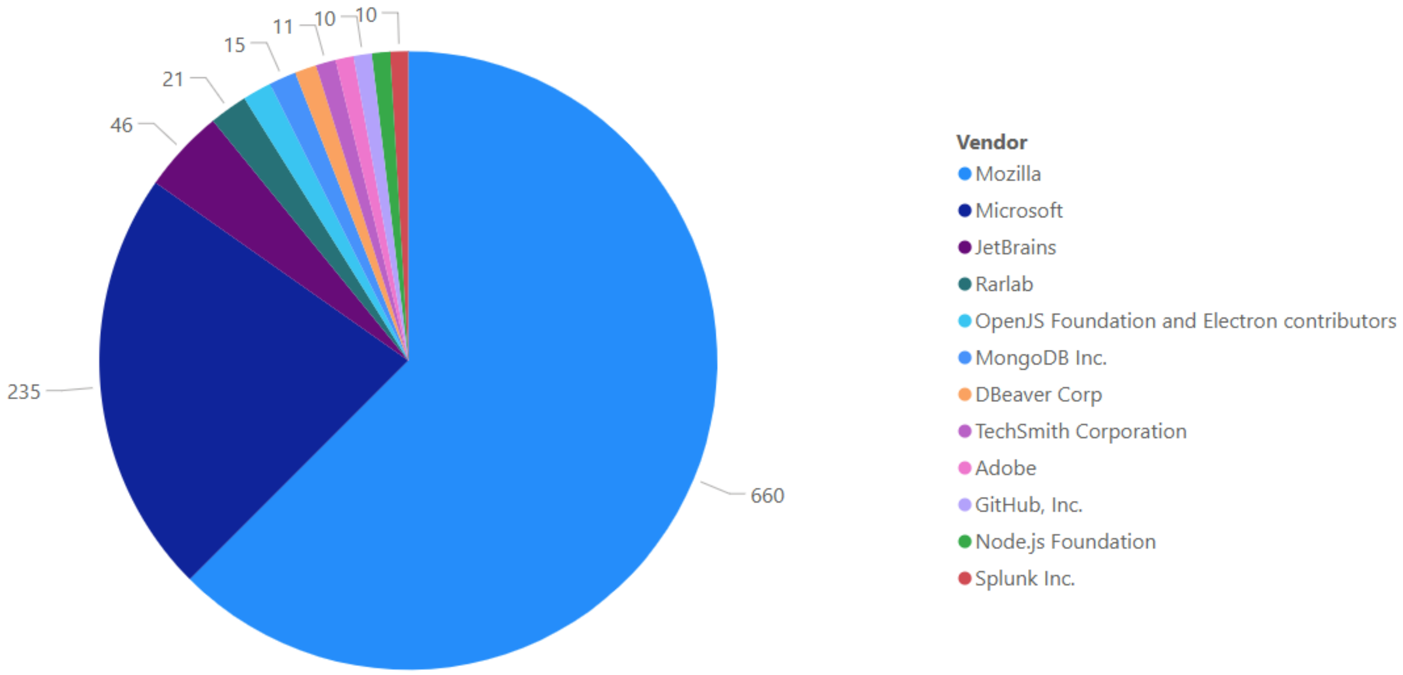
Flexera's Vendor Patch Module (VPM) statistics

Flexera has the largest third-party patch catalog **(8000+)** in the world. This helps customers act quicker and save time by offering an integrated approach to effectively locate, prioritize threats and remediate them quickly to lower the risk to your organization.



This month's top 10 vendor patches

(Updated Patches per vendor, NOT including MS Patch Tuesday patches)

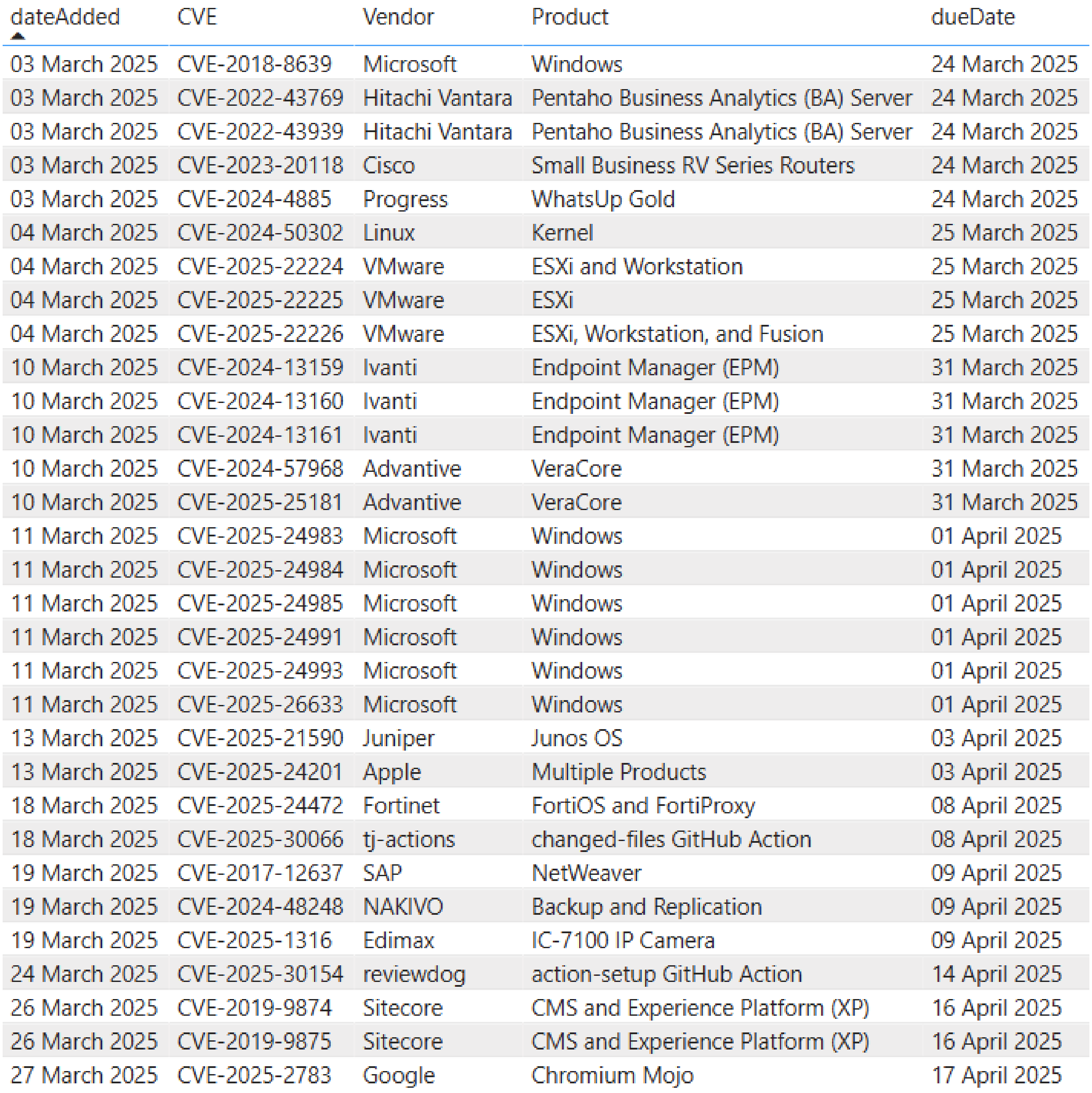


Other sources

CISA

For the benefit of the cybersecurity community and network defenders—and to help every organization better manage vulnerabilities and keep pace with threat activity—CISA maintains the authoritative source of vulnerabilities that have been exploited in the wild: the Known Exploited Vulnerability (KEV) catalog. CISA strongly recommends all organizations review and monitor the KEV catalog and prioritize remediation of the listed vulnerabilities to reduce the likelihood of compromise by known threat actors.

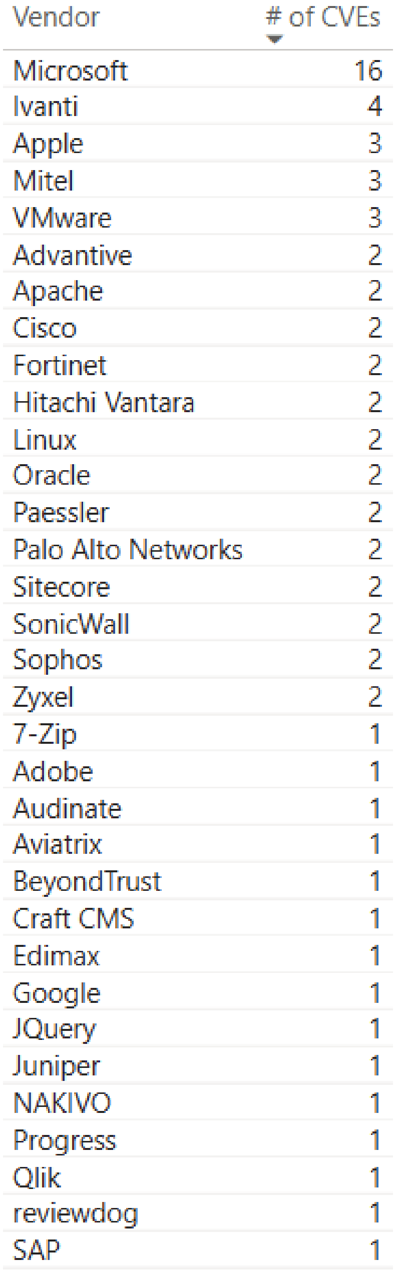
This months' the additions to the KEV catalog



dateAdded ▲	CVE	Vendor	Product	dueDate
03 March 2025	CVE-2018-8639	Microsoft	Windows	24 March 2025
03 March 2025	CVE-2022-43769	Hitachi Vantara	Pentaho Business Analytics (BA) Server	24 March 2025
03 March 2025	CVE-2022-43939	Hitachi Vantara	Pentaho Business Analytics (BA) Server	24 March 2025
03 March 2025	CVE-2023-20118	Cisco	Small Business RV Series Routers	24 March 2025
03 March 2025	CVE-2024-4885	Progress	WhatsUp Gold	24 March 2025
04 March 2025	CVE-2024-50302	Linux	Kernel	25 March 2025
04 March 2025	CVE-2025-22224	VMware	ESXi and Workstation	25 March 2025
04 March 2025	CVE-2025-22225	VMware	ESXi	25 March 2025
04 March 2025	CVE-2025-22226	VMware	ESXi, Workstation, and Fusion	25 March 2025
10 March 2025	CVE-2024-13159	Ivanti	Endpoint Manager (EPM)	31 March 2025
10 March 2025	CVE-2024-13160	Ivanti	Endpoint Manager (EPM)	31 March 2025
10 March 2025	CVE-2024-13161	Ivanti	Endpoint Manager (EPM)	31 March 2025
10 March 2025	CVE-2024-57968	Advantive	VeraCore	31 March 2025
10 March 2025	CVE-2025-25181	Advantive	VeraCore	31 March 2025
11 March 2025	CVE-2025-24983	Microsoft	Windows	01 April 2025
11 March 2025	CVE-2025-24984	Microsoft	Windows	01 April 2025
11 March 2025	CVE-2025-24985	Microsoft	Windows	01 April 2025
11 March 2025	CVE-2025-24991	Microsoft	Windows	01 April 2025
11 March 2025	CVE-2025-24993	Microsoft	Windows	01 April 2025
11 March 2025	CVE-2025-26633	Microsoft	Windows	01 April 2025
13 March 2025	CVE-2025-21590	Juniper	Junos OS	03 April 2025
13 March 2025	CVE-2025-24201	Apple	Multiple Products	03 April 2025
18 March 2025	CVE-2025-24472	Fortinet	FortiOS and FortiProxy	08 April 2025
18 March 2025	CVE-2025-30066	tj-actions	changed-files GitHub Action	08 April 2025
19 March 2025	CVE-2017-12637	SAP	NetWeaver	09 April 2025
19 March 2025	CVE-2024-48248	NAKIVO	Backup and Replication	09 April 2025
19 March 2025	CVE-2025-1316	Edimax	IC-7100 IP Camera	09 April 2025
24 March 2025	CVE-2025-30154	reviewdog	action-setup GitHub Action	14 April 2025
26 March 2025	CVE-2019-9874	Sitecore	CMS and Experience Platform (XP)	16 April 2025
26 March 2025	CVE-2019-9875	Sitecore	CMS and Experience Platform (XP)	16 April 2025
27 March 2025	CVE-2025-2783	Google	Chromium Mojo	17 April 2025

Top (YTD) KEV vendors

Vendors added this year with Known Exploited Vulnerabilities according to CISA

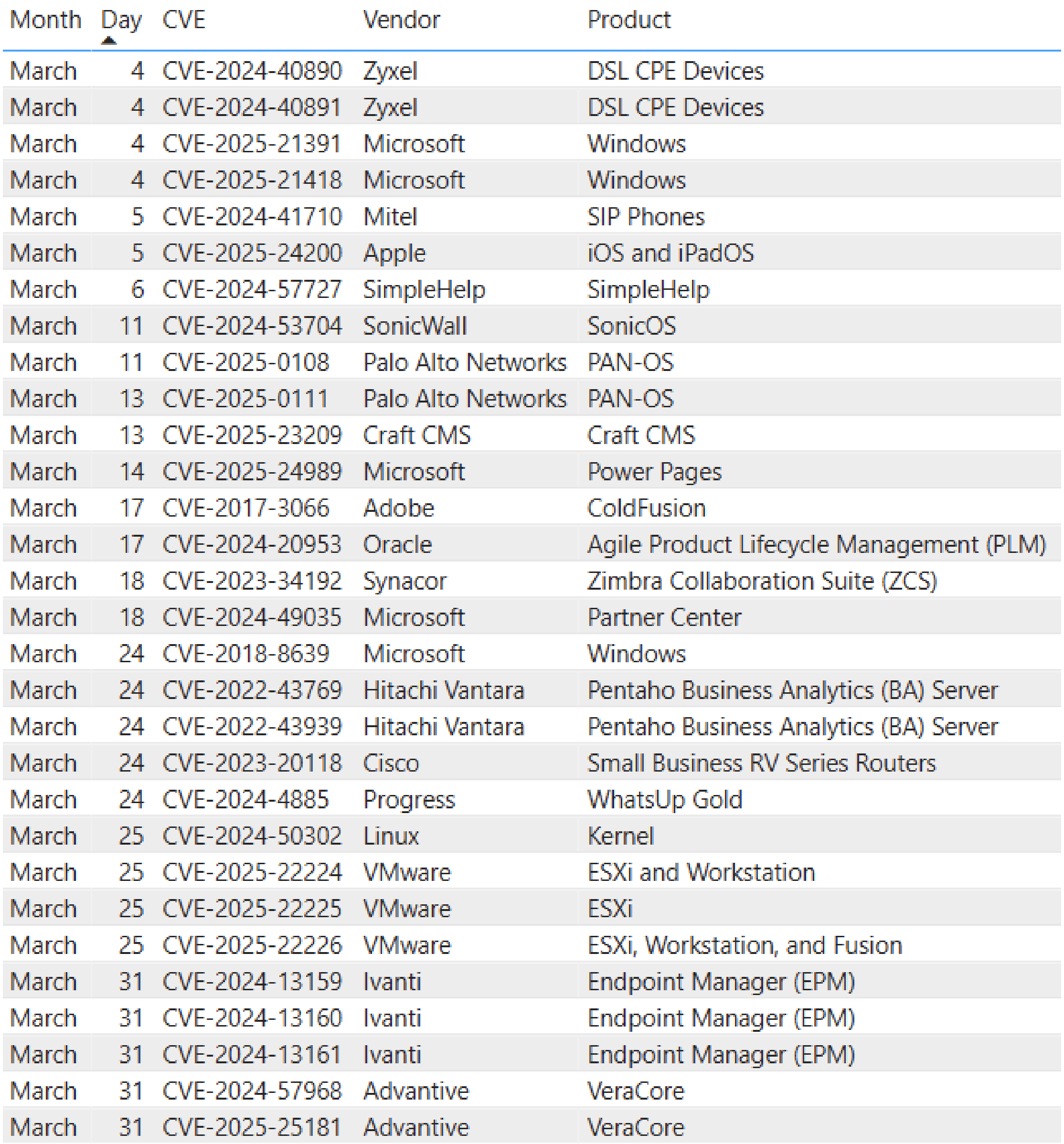


Vendor	# of CVEs
Microsoft	16
Ivanti	4
Apple	3
Mitel	3
VMware	3
Advantive	2
Apache	2
Cisco	2
Fortinet	2
Hitachi Vantara	2
Linux	2
Oracle	2
Paessler	2
Palo Alto Networks	2
Sitecore	2
SonicWall	2
Sophos	2
Zyxel	2
7-Zip	1
Adobe	1
Audinate	1
Aviatrix	1
BeyondTrust	1
Craft CMS	1
Edimax	1
Google	1
JQuery	1
Juniper	1
NAKIVO	1
Progress	1
Qlik	1
reviewdog	1
SAP	1

Due Date this month

CISA adds known exploited vulnerabilities to the catalog when there is a clear action for the affected organization to take. The remediation action referenced in BOD 22-01 requires federal civilian executive branch (FCEB) agencies to take the following actions for all vulnerabilities in the KEV, and

CISA strongly encourages all organizations to do the same:



Month	Day	CVE	Vendor	Product
March	4	CVE-2024-40890	Zyxel	DSL CPE Devices
March	4	CVE-2024-40891	Zyxel	DSL CPE Devices
March	4	CVE-2025-21391	Microsoft	Windows
March	4	CVE-2025-21418	Microsoft	Windows
March	5	CVE-2024-41710	Mitel	SIP Phones
March	5	CVE-2025-24200	Apple	iOS and iPadOS
March	6	CVE-2024-57727	SimpleHelp	SimpleHelp
March	11	CVE-2024-53704	SonicWall	SonicOS
March	11	CVE-2025-0108	Palo Alto Networks	PAN-OS
March	13	CVE-2025-0111	Palo Alto Networks	PAN-OS
March	13	CVE-2025-23209	Craft CMS	Craft CMS
March	14	CVE-2025-24989	Microsoft	Power Pages
March	17	CVE-2017-3066	Adobe	ColdFusion
March	17	CVE-2024-20953	Oracle	Agile Product Lifecycle Management (PLM)
March	18	CVE-2023-34192	Synacor	Zimbra Collaboration Suite (ZCS)
March	18	CVE-2024-49035	Microsoft	Partner Center
March	24	CVE-2018-8639	Microsoft	Windows
March	24	CVE-2022-43769	Hitachi Vantara	Pentaho Business Analytics (BA) Server
March	24	CVE-2022-43939	Hitachi Vantara	Pentaho Business Analytics (BA) Server
March	24	CVE-2023-20118	Cisco	Small Business RV Series Routers
March	24	CVE-2024-4885	Progress	WhatsUp Gold
March	25	CVE-2024-50302	Linux	Kernel
March	25	CVE-2025-22224	VMware	ESXi and Workstation
March	25	CVE-2025-22225	VMware	ESXi
March	25	CVE-2025-22226	VMware	ESXi, Workstation, and Fusion
March	31	CVE-2024-13159	Ivanti	Endpoint Manager (EPM)
March	31	CVE-2024-13160	Ivanti	Endpoint Manager (EPM)
March	31	CVE-2024-13161	Ivanti	Endpoint Manager (EPM)
March	31	CVE-2024-57968	Advantive	VeraCore
March	31	CVE-2025-25181	Advantive	VeraCore

More information

Below 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’s Software Vulnerability Manager landing page
- Request a trial / demo
- Flexera’s Community Pages
  with lots of great resources of information including:
  - Software Vulnerability Management Blog
  - Software Vulnerability Management Knowledge Base
  - Product Documentation
  - Forum
  - 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.

www.flexera.com/svm