MONTHLY VULNERABILITY INSIGHTS

Based on Data from Secunia Research

JANUARY 2025

flexera™

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.

Monthly Summary

Total advisories: **781 (**last month: **881**)

Important conclusions from this month report are:

- After a record-breaking year , the first month started with the lowest advisory count in 12 months.
- January also is third month in a row that the advisory count was lower than the month before and this is breaking a trend that on average January reports normally more advisories than in December.
- Secunia reported 16 Advisories without CVE , mostly for Trend Micro Deep Security, Suse Linux (SLES), PDF-Xchange Editor, Mattermost, Django, Opsview, RedHat and CA.
- 1 Extreme Critical Product has been reported: **Ivanti Connect Secure 22.**
- The trend continues with the **Linux Foundation** producing a high volume of "vulnerabilities," many with low threat or risk, yet requiring significant validation effort.
  Out of 114 Advisories : 77 **Rejected** by Secunia, 37 identified as **Not Critical.**

Notable Vulnerability – and Threat Intelligence news:

Fortinet – FortiOS

Secunia Advisory CVSS3: **8.8** |Threat Score : **91** | Zero-Day: **Yes** | Impact: **Security Bypass**

On January 14, 2025, **Fortinet** disclosed a critical zero-day vulnerability, **CVE-2024-55591**, affecting FortiOS and FortiProxy. This authentication bypass flaw allows remote attackers to gain super-admin privileges through crafted requests to the Node.js websocket module. The vulnerability has been actively exploited in the wild since mid-November 2024 (source)
The vulnerability is reported in versions 7.0.0 through 7.0.16
Solution: Update to version 7.0.17

Ivanti – Connect Secure

Secunia Advisory CVSS3: **9.8** |Threat Score : **95** | Zero-Day: **Yes** | Impact: **System access, Privilege escalation**

Ivanti has released an update that addresses one critical and one high vulnerability in Ivanti Connect Secure, Policy Secure and ZTA Gateways. Successful exploitation of CVE-2025-0282 could lead to unauthenticated remote code execution. CVE-2025-0283 could allow a local authenticated attacker to escalate privileges.
Ivanti is aware of a limited number of customers' Ivanti Connect Secure appliances being exploited by CVE-2025-0282 at the time of disclosure.
Solution: Update to version 22.7R2.5

Microsoft Patch Tuesday

Microsoft's January 2025 Patch Tuesday includes security updates for 159 flaws, including eight zero-day vulnerabilities, with three actively exploited in attacks including fixes for twelve "Critical" vulnerabilities, including information disclosure, privileges elevation, and remote code execution flaws.
https://msrc.microsoft.com/update-guide/releaseNote/2025-Jan

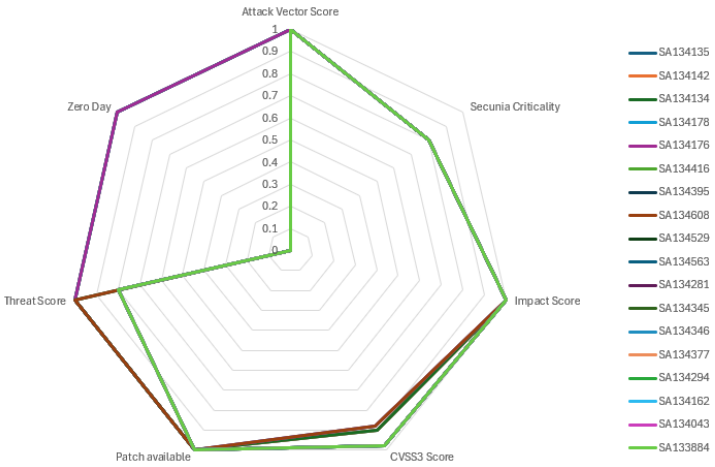
Risk Scoring Model:

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 January based on the calculated Risk Score:

Advisories	Product Versions	Impact or Consequence	OS	Description	criticality	CVSS3 Score	Zero Day	Threat Score	Attack Vector	Vendor Patched	Risk Score
SA134851	Ivanti Connect Secure 22.x,	System access	FALSE	Ivanti Connect Secure Multiple Vulnerabilities	Extreme Critical	9.8	TRUE	95	From Remote Network	Vendor Patched	6.98
SA135194	Microsoft Windows 11,	System access	TRUE	Microsoft Windows 11 Multiple Vulnerabilities	Highly Critical	9.8	TRUE	99	From Remote Network	Vendor Patched	6.78
SA135197	Microsoft Windows 10, Microsoft Windows Server 2016,	System access	TRUE	Microsoft Windows Server 2016 / Windows 10 Multiple Vulnerabilities	Highly Critical	9.8	TRUE	99	From Remote Network	Vendor Patched	6.78
SA135195	Microsoft Windows Server 2022,	System access	TRUE	Microsoft Windows Server 2022 Multiple Vulnerabilities	Highly Critical	9.8	TRUE	99	From Remote Network	Vendor Patched	6.78
SA135193	Microsoft Windows Server 2025,	System access	TRUE	Microsoft Windows Server 2025 Multiple Vulnerabilities	Highly Critical	9.8	TRUE	99	From Remote Network	Vendor Patched	6.78
SA135198	Microsoft Windows Server 2012,	System access	TRUE	Microsoft Windows Server 2012 Multiple Vulnerabilities	Highly Critical	9.8	TRUE	23	From Remote Network	Vendor Patched	6.18
SA135196	Microsoft Windows Server 2019,	System access	TRUE	Microsoft Windows Server 2019 Multiple Vulnerabilities	Highly Critical	9.8	TRUE	23	From Remote Network	Vendor Patched	6.18
SA134939	Aviatrix Controller 7.x,	System access	FALSE	Aviatrix Controller Command Injection Vulnerability	Highly Critical	10	FALSE	88	From Remote Network	Vendor Patched	5.8
SA135463	Apple iOS 18.x, Apple iPadOS 18.x,	System access	TRUE	Apple iOS and iPadOS Multiple Vulnerabilities	Highly Critical	9.8	FALSE	92	From Remote Network	Vendor Patched	5.78
SA135350	Apple macOS 15.x,	System access	TRUE	Apple macOS Sequoia Multiple Vulnerabilities	Highly Critical	9.8	FALSE	96	From Remote Network	Vendor Patched	5.78

Advisory of the month: SA134851 (Ivanti Connect Secure 22.x)

Secunia Advisory ID	SA134851
Creation Date	2025-01-08
Criticality	- Extremely critical
Zero Day	Yes
Impact	System access, Privilege escalation
Where	From remote
Solution Status	Vendor Patched
Secunia CVSS Scores	CVSS3 Base: 9.8, Overall: 9.4 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C
CVE references	CVE-2025-0282 CVE-2025-0283
Threat Score	95 (Last Updated 2025-01-24)

Advisory Details:

Description:

Multiple vulnerabilities have been reported in Ivanti Connect Secure, which can be exploited by malicious, local users to gain escalated privileges and by malicious people to compromise a vulnerable system. 1) An unspecified error can be exploited to cause a stack-based buffer overflow and subsequently execute arbitrary code. Note: The vulnerability #1 is currently actively exploited in limited, targeted attacks. 2) An unspecified error can be exploited to cause a stack-based buffer overflow and subsequently execute arbitrary code with elevated privileges. The vulnerabilities are reported in versions 22.7R2.4 and prior.

Solution:

Update to version 22.7R2.5.

Provided and/or discovered by:

1) Reported as a 0-day. 2) Reported by the vendor.

Original advisory

Ivanti Connect Secure Multiple Vulnerabilities - CVE

CVE	CVSS*	Threat Score	Threat Reason
CVE-2025-0282	CVSS v3: 9 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H	87	Linked to Historical Cyber Exploit Historically Linked to Penetration Testing Tools Historically Linked to Malware Recently Verified Intelligence Recently exploited in the wild Recently Linked to Malware Recent possible POC Linked to Recent Cyber Exploit

Description*
A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a remote unauthenticated attacker to achieve remote code execution.

Threat Intel Module
The CVE threat score of 87 was based on the following triggers:

- Linked to Historical Cyber Exploit
- Historically Linked to Penetration Testing Tools
- Historically Linked to Malware
- Recently Verified Intelligence
- Recently exploited in the wild
- Recently Linked to Malware
- Recent possible POC
- Linked to Recent Cyber Exploit

The threat score was last updated on 2025-01-24. These threats have been associated with the following exploits:

- J-magic
- PhishWP
- Gayfemboy (Botnet)
- PySoxy (Offensive Security Tools (OST))
- THINSPOOL (Trojan)

Learn More about Threat Scoring

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.

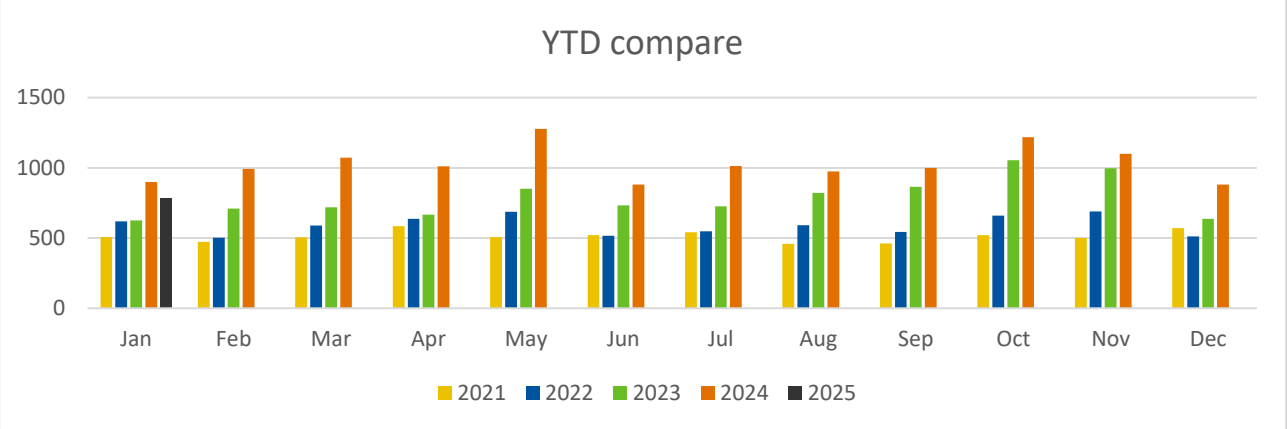
In this case, the CVE is related to a dangling pointer and requiring a difficult to exploit race condition involving the garbage collection (GC), which makes it less likely to be able to exploit this vulnerability for a full-fledged privilege escalation. Thus, in the base Linux Kernel itself we rated 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).

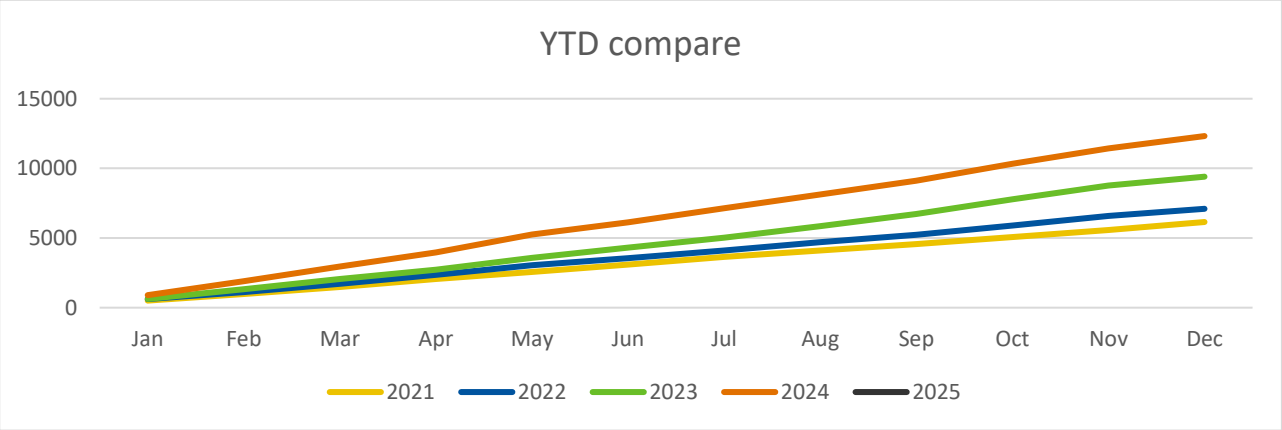
Nevertheless, the situation for SUSE, Red Hat, etc. may differ e.g., due to how their own kernel is configured and compiled and which parts of the original Linux Kernel code base is used.

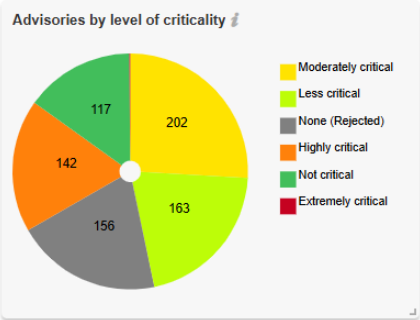
Therefore, Secunia Research has the capabilities to rate the very same vulnerability differently depending on the actual product exposing the vulnerability. The product context matters! The CVSS scores provided by each vendor are considered as a data point for the respective Secunia Advisories related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

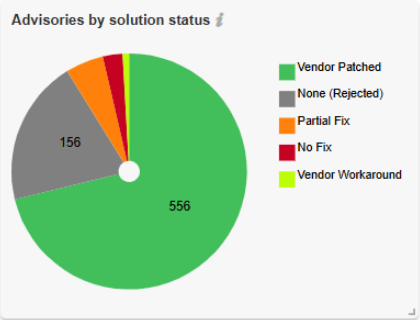
Year-to-date overview

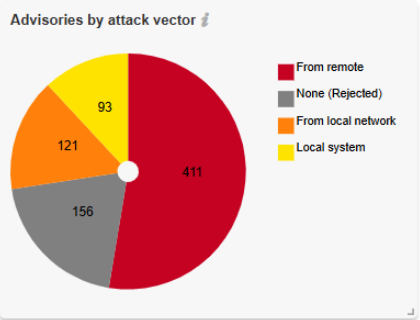
As of **January 31,2025**, the year-to-date total is **12,318** Advisories ↑ which is **31%** higher than 2023: **9,402** YTD Advisories)

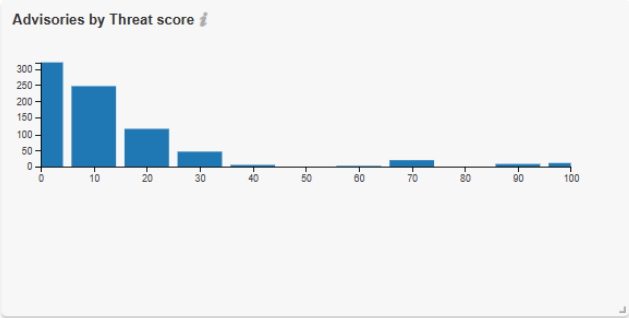


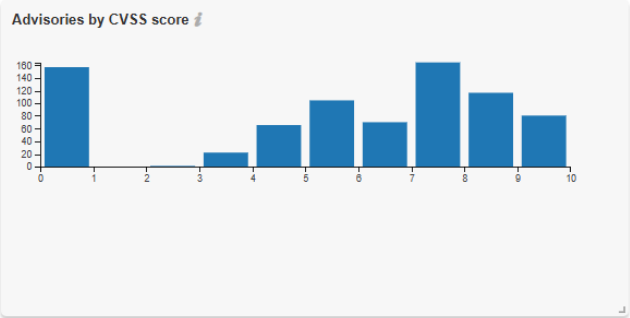












Monthly data

This month, a total of **1,100** ↓ (last month: **881**) advisories were reported by the Secunia Research Team.

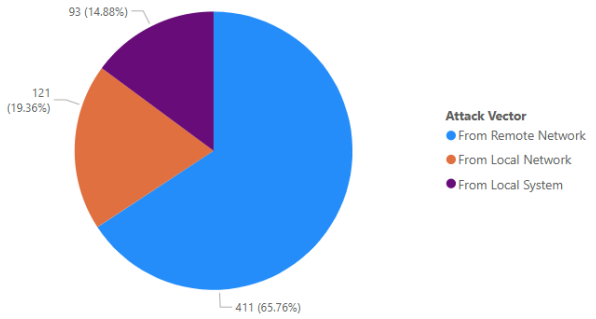
This month:	#	Change *(last month):*
Total # of advisories	**781**	↓ *(**1,100**)*
Unique Vendors	**79**	↓ *(**83**)*
Unique Products	**320**	↓ **(259***)*
Unique Versions	**404**	↑ ***(320)***
Rejected Advisories *	**156**	↓ ***(256)***
NEW Advisories without CVE ID	**16**	↑ *(**10**)*
Advisories with Threat Score (>0)	**460**	↑ **(438)**
Total Unique CVE ID's reported	**2,393**	↓ **(2,654)**

↑ increased ↓lower ↔ same

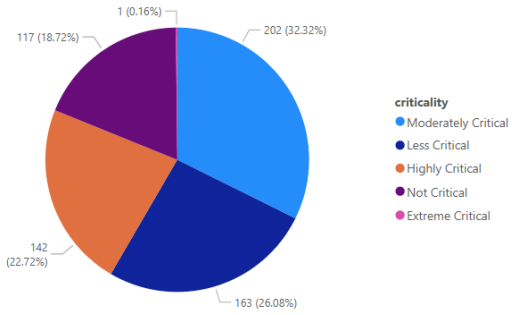
** **156** advisories have received the "rejected" status which means in general that leveraging it would require one or more violations of security best practices (e.g., product not securely configured or not used securely) or that it was "too weak of a gain" (e.g., administrative, local users already 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

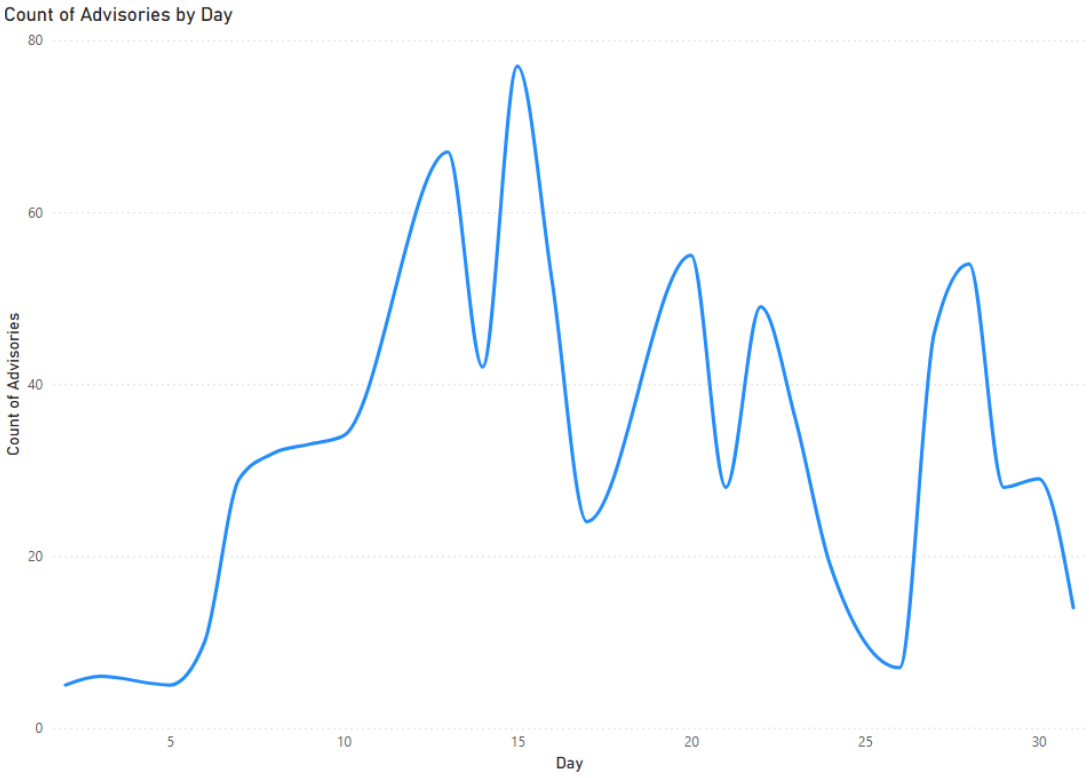


Advisories by criticality



Advisories per day

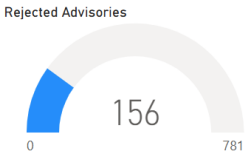
Below an overview of the daily advisory count.



Year	Month	Day	# of Advisories
2025	January	2	5
2025	January	3	6
2025	January	5	5
2025	January	6	10
2025	January	7	29
2025	January	8	32
2025	January	9	33
2025	January	10	34
2025	January	13	67
2025	January	14	42
2025	January	15	77
2025	January	16	52
2025	January	17	24
2025	January	20	55
2025	January	21	28
2025	January	22	49
2025	January	23	36
2025	January	24	19
2025	January	26	7
2025	January	27	46
2025	January	28	54
2025	January	29	28
2025	January	30	29
2025	January	31	14
Total			**781**

Rejected advisories.

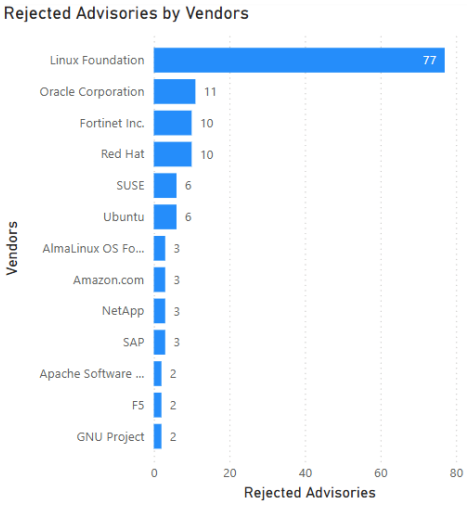
There are many vulnerabilities posted to the National Vulnerability Database (NVD) by a lot of people and companies. They are not always valid, assigned a proper criticality, and in some cases, a vulnerability may be legitimate but not afford the attacker any benefit.

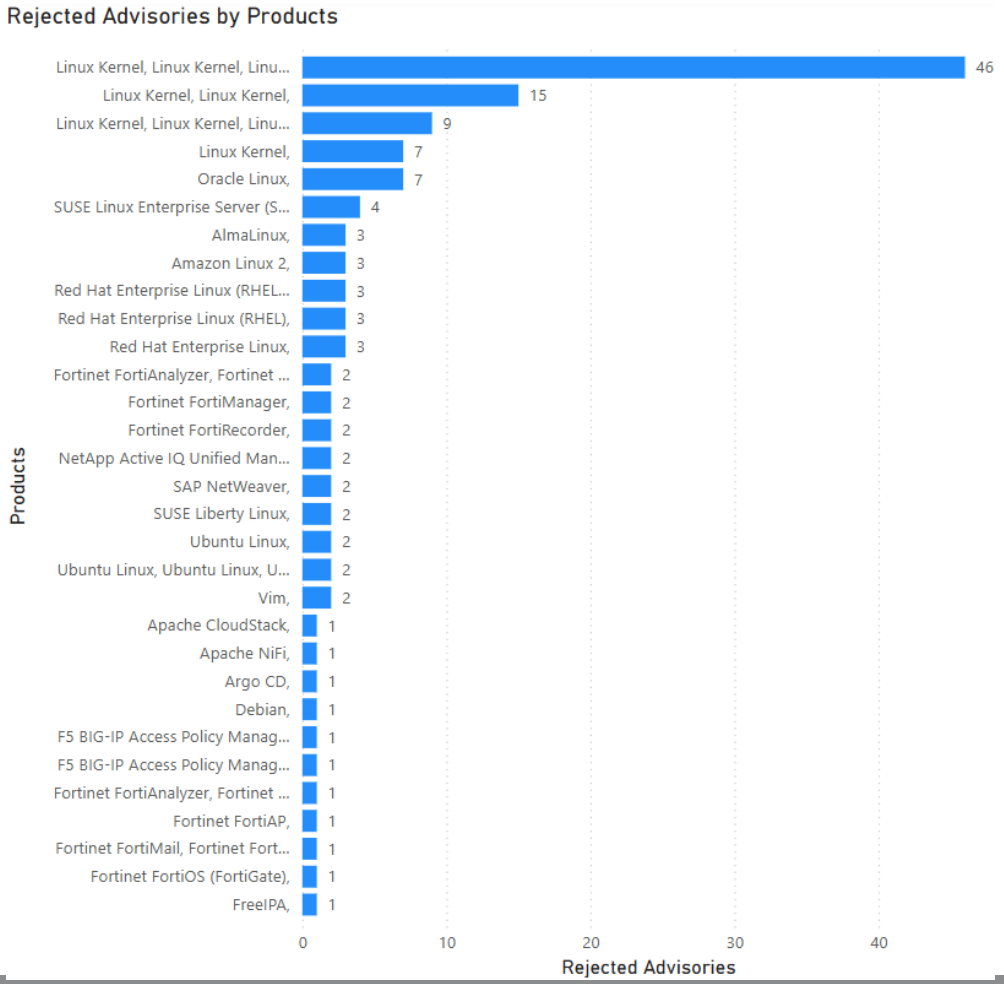


The Secunia Research team at Flexera evaluates vulnerabilities from hundreds of sources, rescores them when necessary and even rejects vulnerabilities not worth your attention. Rejection Advisories help you to reduce the volume of vulnerabilities to be mitigated by helping you focus only on those that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

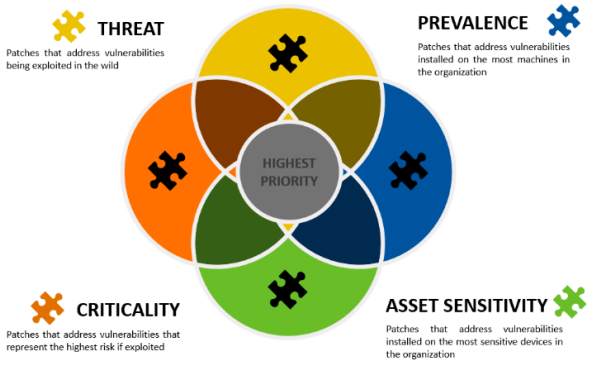
- What systems would result in the most risk if compromised?
- Is it a high-risk device? **Patch**.

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**.



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

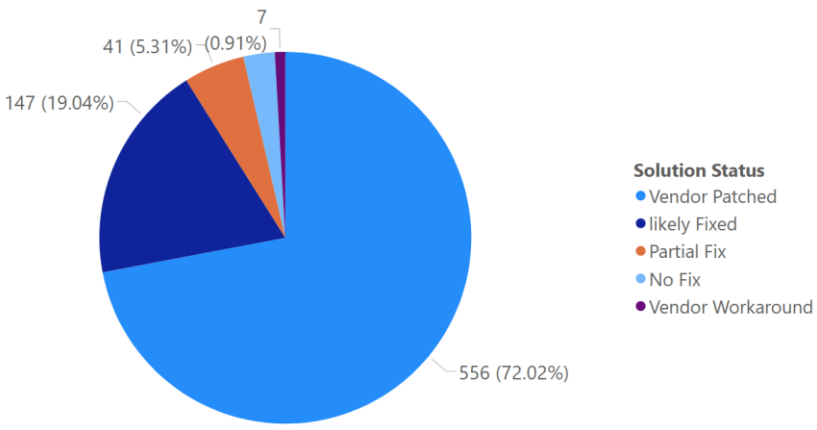
Focusing on vulnerabilities with CVSS 7 or higher would address about 50 percent of exploits. Most exploits are CVSS scored between 4 and 7. Focusing
on vulnerabilities for the top 20 vendors would address only about 20 percent.

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.

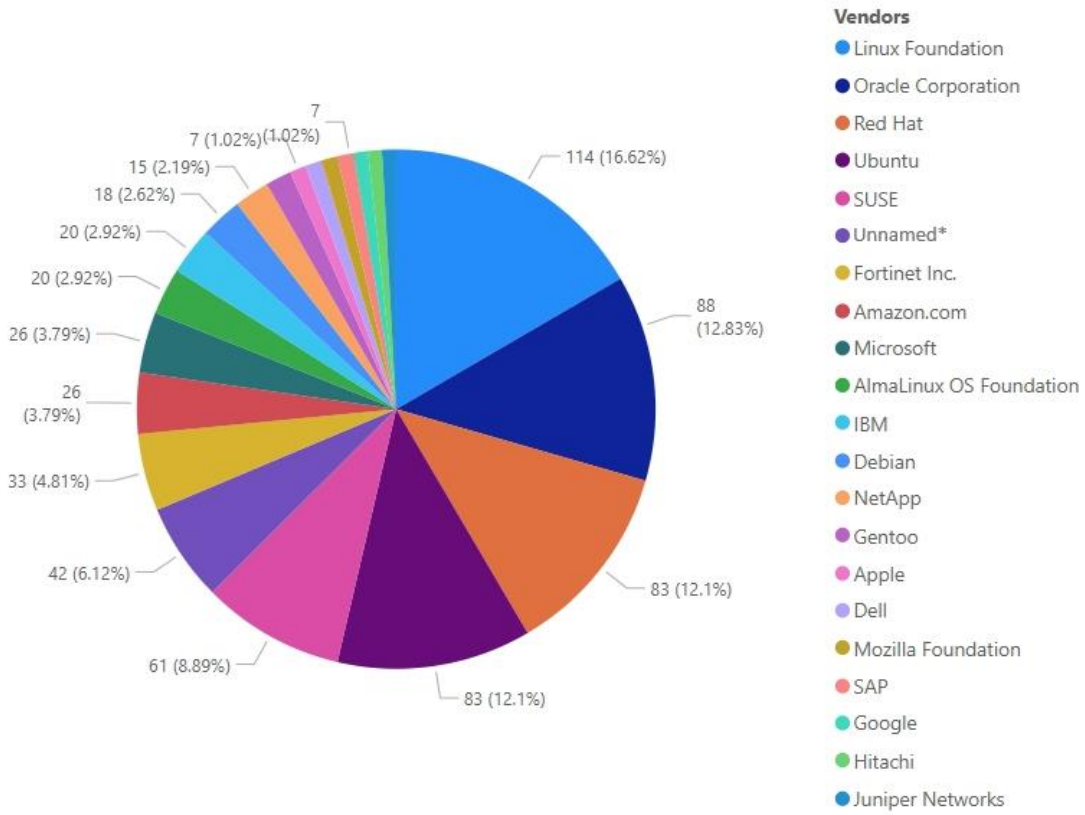
Take away 2:

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

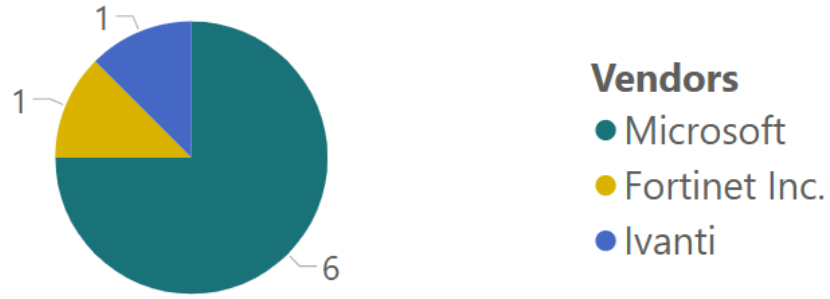
Top vendors with the most advisories



*Unnamed are open source products or plugins:

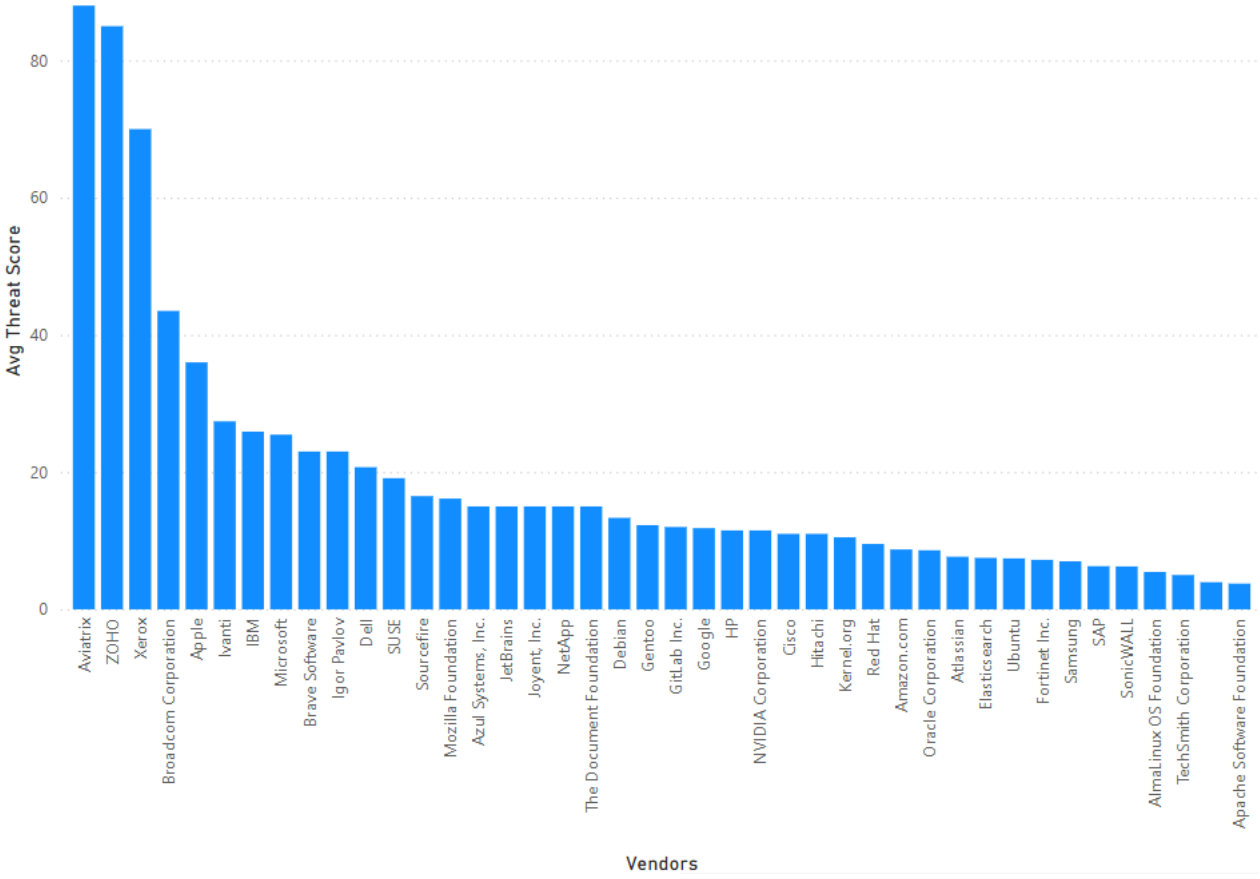
Versions
Argo CD 2.x,
Carbon 2.x,
FreeIPA 4.x,
Git LFS 3.x,
Go 1.x,
Go Ethereum 1.x,
gSOAP Toolkit 2.x,
iTerm2 3.x,
Joomla! 3.x,
JsonCpp 1.x,
Kubernetes 1.29.x,
MediaWiki 1.x,
Narayana 7.x,
Node.js 20.x, Node.js 22.x,
OpenSSL 1.x, OpenSSL 3.x,
PhpSpreadsheet 1.x,
Qt 5.x,
Redis 6.x, Redis 7.x,
Redis 7.x,
Rocky Linux 8.x,
rsync 3.x,
Vim 9.x,
Vite 4.x, Vite 5.x,
vLLM 0.x,
WordPress Crelly Slider Plugin 1.x,
WordPress List category posts Plugin 0.x,
WordPress Page Builder by SiteOrigin Plugin 2.x,
WordPress UpdraftPlus Plugin 1.x,
WordPress WP GPX Maps Plugin 1.x,
WordPress WP-Polls Plugin 2.x,

Top vendors with zero-day



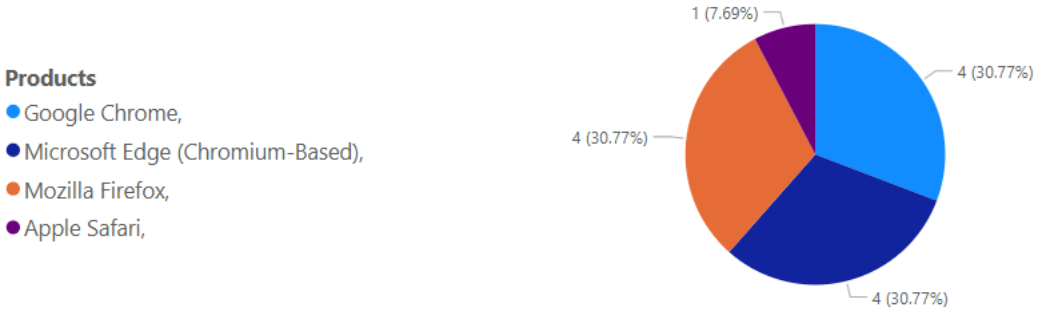
Advisories	Versions
SA135111	Fortinet FortiOS (FortiGate) 6.x, Fortinet FortiOS (FortiGate) 7.x,
SA134851	Ivanti Connect Secure 22.x,
SA135197	Microsoft Windows 10, Microsoft Windows Server 2016,
SA135194	Microsoft Windows 11,
SA135198	Microsoft Windows Server 2012,
SA135196	Microsoft Windows Server 2019,
SA135195	Microsoft Windows Server 2022,
SA135193	Microsoft Windows Server 2025,

Top Vendors with highest average threat score



Browser-related advisories

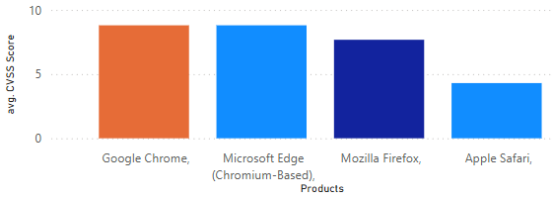
Advisories per browser



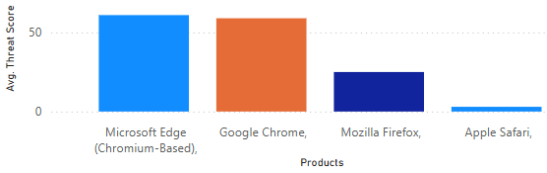
Browser zero-day vulnerabilities

Description	Advisories	Cvss3	ThreatScore	Consequence
Google Chrome Multiple Vulnerabilities	SA134884	8.80	23.00	System access
Microsoft Edge (Chromium-Based) Multiple Vulnerabilities	SA135340	8.80	23.00	System access
Microsoft Edge (Chromium-Based) Multiple Vulnerabilities	SA135313	8.80	19.00	System access
Google Chrome Multiple Vulnerabilities	SA133339	8.80	17.00	System access
Google Chrome Multiple Vulnerabilities	SA135593	8.80	15.00	System access
Microsoft Edge (Chromium-Based) Multiple Vulnerabilities	SA135607	8.80	15.00	System access
Mozilla Firefox Multiple Vulnerabilities	SA134407	8.80	12.00	System access
Mozilla Firefox ESR Multiple Vulnerabilities	SA134446	8.80	9.00	System access
Mozilla Firefox ESR Multiple Arbitrary Code Execution Vulnerabilities	SA128777	8.80	4.00	System access
Google Chrome Multiple Vulnerabilities	SA132863	8.80	4.00	System access
Microsoft Edge (Chromium-Based) Multiple Vulnerabilities	SA135076	8.80	4.00	System access
Apple Safari Multiple Vulnerabilities	SA135438	4.30	3.00	Spoofing
Mozilla Firefox for iOS Multiple Spoofing Vulnerabilities	SA135084	4.30	0.00	Spoofing

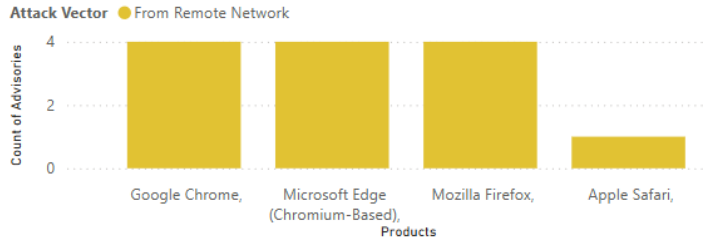
Average CVSS (criticality) score per browser



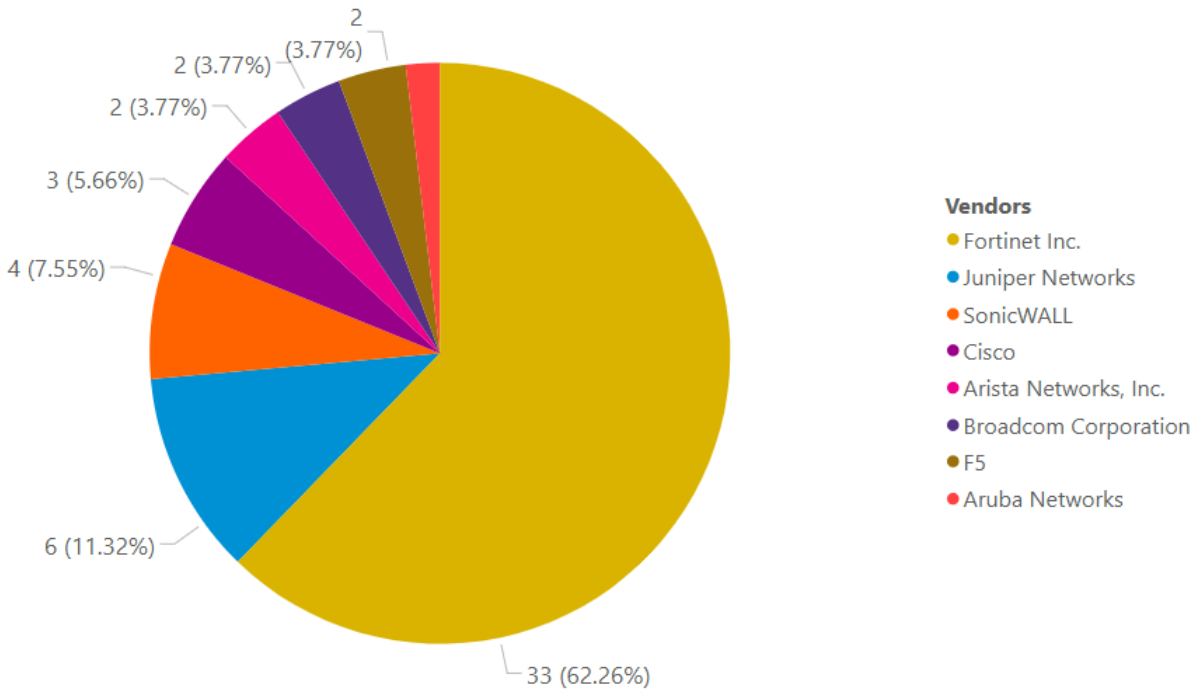
Average threat score per browser



What's the Attack Vector?



Networking related advisories

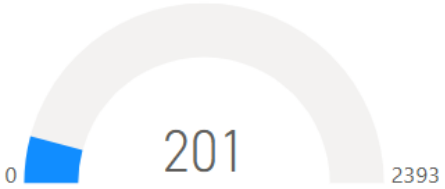


Threat intelligence

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+)	**460** ↑ (438)	58.90%
SAIDs with no threat score (=0)	**321** ↓ *(443)*	41.10%

SAID: Secunia Advisory Identifier

Range	# SAIDS	*Last month*
Low-range threat score SAIDs (1-12)	275 ↓	*(350)*
Medium-range threat score SAIDs (13-23)	133 ↑	*(53)*
Critical-range threat score SAIDs (45-70)	**23** ↑	*(20)*
Very critical threat score SAIDs (71-99)	**21** ↑	*(9)*
High-range threat score SAIDs (24-44)	8 ↑	*(6)*

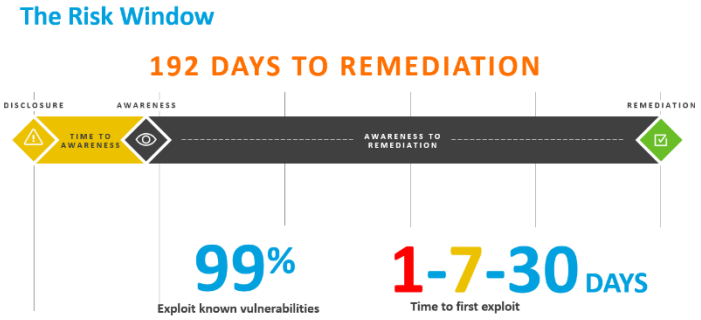
More information about how the Secunia team calculates the threat score:

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

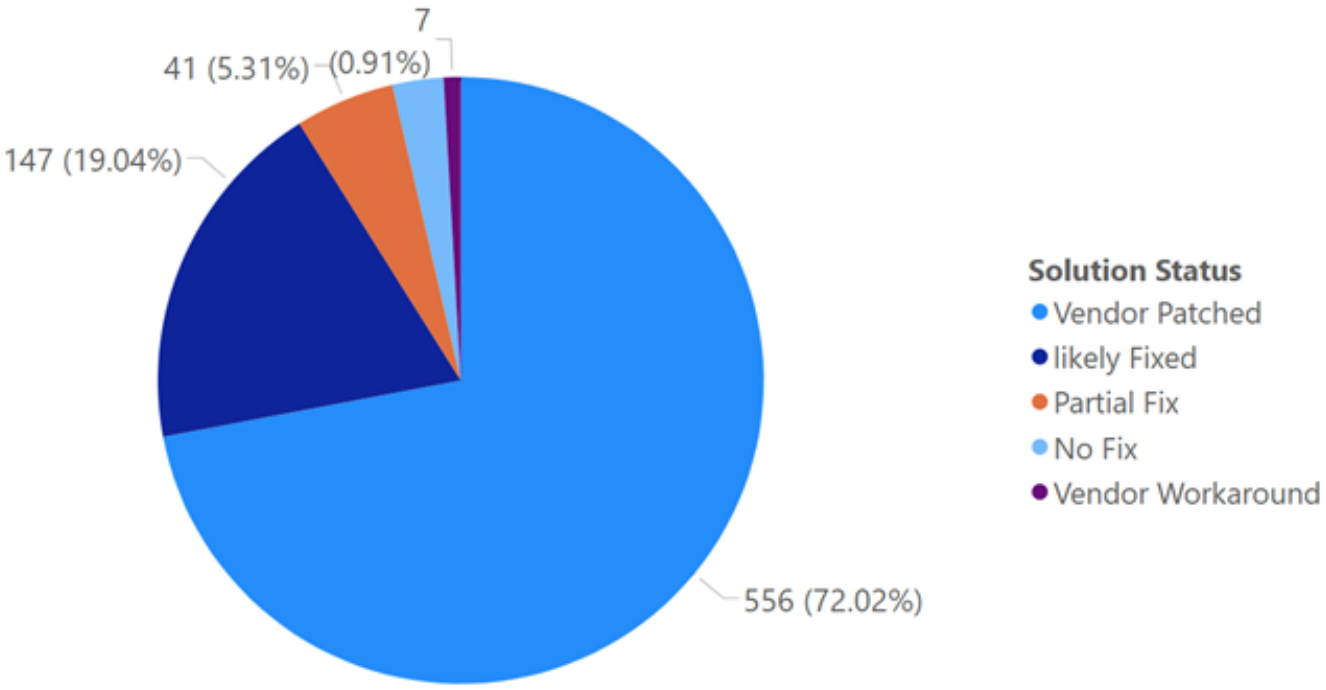
Patching

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

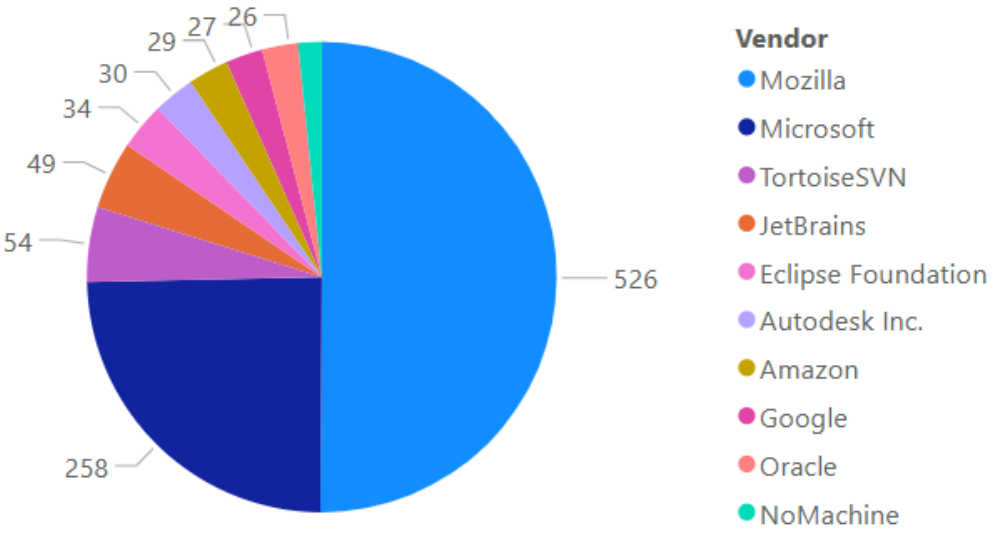


Flexera's Vendor Patch Module (VPM) statistics

Flexera has the largest third-party patch catalog **(7500+)** 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
07 January 2025	CVE-2020-2883	Oracle	WebLogic Server	28 January 2025
07 January 2025	CVE-2024-41713	Mitel	MiCollab	28 January 2025
07 January 2025	CVE-2024-55550	Mitel	MiCollab	28 January 2025
08 January 2025	CVE-2025-0282	Ivanti	Connect Secure, Policy Secure, and ZTA Gateways	15 January 2025
13 January 2025	CVE-2023-48365	Qlik	Sense	03 February 2025
13 January 2025	CVE-2024-12686	BeyondTrust	Privileged Remote Access (PRA) and Remote Support (RS)	03 February 2025
14 January 2025	CVE-2024-55591	Fortinet	FortiOS and FortiProxy	21 January 2025
14 January 2025	CVE-2025-21333	Microsoft	Windows	04 February 2025
14 January 2025	CVE-2025-21334	Microsoft	Windows	04 February 2025
14 January 2025	CVE-2025-21335	Microsoft	Windows	04 February 2025
16 January 2025	CVE-2024-50603	Aviatrix	Controllers	06 February 2025
23 January 2025	CVE-2020-11023	JQuery	JQuery	13 February 2025
24 January 2025	CVE-2025-23006	SonicWall	SMA1000 Appliances	14 February 2025
29 January 2025	CVE-2025-24085	Apple	Multiple Products	19 February 2025

Top 10 (YTD) KEV vendors

Vendors added this year with Known Exploited Vulnerabilities

Vendor	# of CVEs
Microsoft	3
Mitel	2
Apple	1
Aviatrix	1
BeyondTrust	1
Fortinet	1
Ivanti	1
JQuery	1
Oracle	1
Qlik	1
SonicWall	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
January	3	CVE-2024-50623	Cleo	Multiple Products
January	6	CVE-2024-20767	Adobe	ColdFusion
January	6	CVE-2024-35250	Microsoft	Windows
January	7	CVE-2024-55956	Cleo	Multiple Products
January	8	CVE-2018-14933	NUUO	NVRmini Devices
January	8	CVE-2019-11001	Reolink	Multiple IP Cameras
January	8	CVE-2021-40407	Reolink	RLC-410W IP Camera
January	8	CVE-2022-23227	NUUO	NVRmini2 Devices
January	13	CVE-2021-44207	Acclaim Systems	USAHERDS
January	15	CVE-2025-0282	Ivanti	Connect Secure, Policy Secure, and ZTA Gateways
January	20	CVE-2024-3393	Palo Alto Networks	PAN-OS
January	21	CVE-2024-55591	Fortinet	FortiOS and FortiProxy
January	28	CVE-2020-2883	Oracle	WebLogic Server
January	28	CVE-2024-41713	Mitel	MiCollab
January	28	CVE-2024-55550	Mitel	MiCollab

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