



MONTHLY VULNERABILITY INSIGHTS

Based on Data from Secunia Research

MAY 2025

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

Reuse	2
Introduction	4
<i>Secunia Research software vulnerability tracking process.</i>	4
<i>The anatomy of a Security Advisory</i>	4
<i>Monthly Summary</i>	5
Year-to-date overview	9
Monthly data	10
<i>Vulnerability information</i>	10
Advisories by attack vector	10
Advisories by criticality	10
Advisories per day	11
Advisories without CVE	11
<i>Rejected advisories.</i>	12
Addressing awareness with vulnerability insights	12
<i>Vendor view</i>	14
Top vendors with the most advisories	14
Top vendors with zero-day	15
Top Vendors with highest average threat score	15
<i>Browser-related advisories</i>	16
Advisories per browser	16
Browser zero-day vulnerabilities	16
Average CVSS (criticality) score per browser	16
Average threat score per browser	16
What's the Attack Vector?	16
Top networking related advisories	17
<i>Threat intelligence</i>	18
Count of malware-exploited CVEs	18
Count of advisories by CVE threat score	18
Threat intelligence advisory statistics	18
Patching	19
<i>Vulnerabilities that are vendor patched</i>	19
<i>Flexera's Vendor Patch Module (VPM) statistics</i>	20
<i>This month's top 10 vendor patches</i>	20
Other sources	21
CISA	21
This months' the additions to the KEV catalog	21
Due Date this month	23
More information	24

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: **1,394** (last month: **1,053**)

Important conclusions from this month report are:

- Where Q1 had a slightly lower number of advisories (270) . we are currently at 110 under last year's record (YTD)
Our team is expecting that despite the issues at MITRE, CISA and NIST , we will see an increase in advisories this year.
Next month could be a interesting since June'24 "only" had 880 advisories.
- Secunia reported **24** (last month : 26) Advisories without CVE that have a CVSS range from 9.8 to 3.3, the top 3 :
 - 9.8** for **RHEL extended Lifecycle Support 7**
 - 7.8** for **PDF X-Change Editor 10.x**
 - 7.5** for **Zimbra Collaboration Suite 10.x, 9.x**
- 10 Zero-day** Advisories reported for **Microsoft Windows 10,11 , Microsoft Server 2012,2016,2019,2022,2025, Google Chrome 136.x , Microsoft Edge , Android 13.x/14.x, Ivanti Endpoint Manager Mobile 11.x**
- The trend continues with the **Linux Foundation** producing a high volume of "vulnerabilities" with low threat or risk yet requiring significant validation effort , out of **208** advisories :
 - 125 rejection advisories
 - 75 Not Critical Advisories
 - 7 Less Critical Advisories
 - 1 Moderately Advisory
- Secunia Research** identified several **KEV's** that have not been added to the **CISA KEV**:

CVE	Versions	CVSS3 Score	Threat Score
CVE-2023-21768	Dell RecoverPoint	7.8	80
CVE-2023-6931	Dell RecoverPoint	7.8	79
CVE-2025-32433	Dell EMC VxRail 7.x	10	59
CVE-2024-2961	Dell RecoverPoint	7.3	56
CVE-2024-53677	IBM Security Guardium 11.x	0	56
CVE-2025-1094	Amazon Linux 2, Rocky Linux 8.x	8.1	55
CVE-2024-56337	Dell EMC VxRail 7.x, Red Hat JBoss Web Server 5.x, IBM Watson Speech Services Cartridge for IBM Cloud Pak for Data 4.x	9.8	53
CVE-2024-50379	Xerox FreeFlow Print Server 7.x, IBM Watson Speech Services Cartridge for IBM Cloud Pak for Data 4.x	9.8	53
CVE-2020-13756	Ubuntu Linux 16.04, Ubuntu Linux 18.04	9.8	53
CVE-2022-0995	Ubuntu Linux 22.04	7.8	53
CVE-2021-38001	Dell RecoverPoint	8.8	30
CVE-2025-0133	PAN-OS 10.x, PAN-OS 11.x	0	30
CVE-2025-47933	Argo CD 2.x	9	28
CVE-2020-10713	Oracle Solaris 11.x	8.2	22

Notable Vulnerability – and Threat Intelligence news:

Ivanti – Endpoint Manager Mobile 11.x

Secunia Advisory: **SA138998** | Secunia CVSS3: **9.8** (CVSS:3.1/AV:N/AC:L/PR:N/UI:H/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C) | Threat Score : **99** | Zero-Day: **Yes** | Secunia Criticality Rating: **Extremely Critical** | Impact: **System access, Security Bypass** | CVE references : CVE-2025-4428 , CVE-2025-4427

Multiple vulnerabilities have been [reported](#) in **Ivanti Endpoint Manager Mobile**, which can be exploited by malicious people to bypass certain security restrictions and compromise a vulnerable system.

- 1) An unspecified error can be exploited to bypass authentication requirements and subsequently access otherwise restricted resources.
- 2) An unspecified error can be exploited to execute arbitrary code. Note: The vulnerabilities are currently actively exploited in limited, targeted attacks. The vulnerability #2 can be [chained](#) with CVE-2025-4427. The vulnerabilities are reported in versions prior to 11.12.0.5.

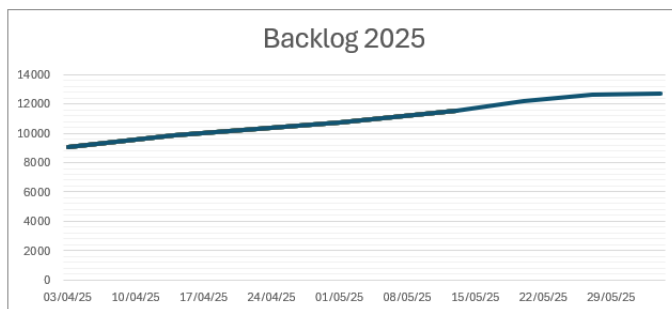
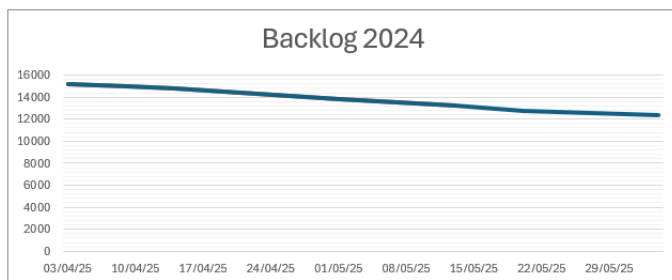
CVE	CVSS*	Threat Score	Threat Reason
CVE-2025-4428	CVSS v3: 7.2 CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	89	Historically Linked to Penetration Testing Tools Historically Linked to Malware Recently Linked to Remote Access Trojan Linked to Historical Cyber Exploit Recently exploited in the wild Recently Verified Intelligence Recent possible POC Recently Linked to Malware Linked to Recent Cyber Exploit
CVE-2025-4427	CVSS v3: 5.3 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	88	Linked to Historical Cyber Exploit Historically Linked to Malware Recently Linked to Remote Access Trojan Recently exploited in the wild Recently Verified Intelligence Recent possible POC Recently Linked to Malware Linked to Recent Cyber Exploit

Associated Exploits:

- DslogdRAT (Remote Access Trojan) (**CVE-2025-4428, CVE-2025-4427**)
- Auto-Color (Backdoor) (**CVE-2025-4428**)
- QakBot (Banking Trojan) (**CVE-2025-4428, CVE-2025-4427**)
- Fast Reverse Proxy (FRP) (Offensive Security Tools (OST)) (**CVE-2025-4428**)
- Authentication Bypass (**CVE-2025-4428, CVE-2025-4427**)
- LummaC2 (Stealware) (**CVE-2025-4428**)
- Auto-Color (Backdoor) (**CVE-2025-4428**)
- DslogdRAT (Remote Access Trojan)
- JSP Webshell (Backdoor)
- Brute Ratel C4 (Offensive Security Tools (OST))

NVD – CVE.org May update

The NVD Backlog Crisis – Why Secunia Research Is Now Critical



As of February 2024, the U.S. National Vulnerability Database (NVD) began significantly slowing its analysis of newly disclosed CVEs. By May, this delay had compounded into a backlog of over 25,000 vulnerabilities, with the 2025 backlog growing by approximately 2,500 CVEs per month.

At VulnCon25 in April, NIST officials acknowledged the crisis, attributing it to staffing and funding limitations. Despite promises to resolve the issue by end of April, delays persisted into May and continue to jeopardize the timeliness and reliability of vulnerability data.

It's clear that the NVD team is working on clearing the backlog in 2024 (slow pace but progressing daily) However this comes at a cost where the backlog for 2025 is increasing with average backlog of 2500 CVEs per publication month. (total 12,771)

The Risk of Overreliance on NVD

Many commercial threat intelligence providers still rely heavily on NVD and related government feeds such as CVE.org and CISA. This creates a dangerous bottleneck in the vulnerability management ecosystem. If your intelligence is lagging, so is your remediation response, potentially leaving your environment exposed for weeks or months.

Why Secunia Research Is Different

Flexera's **Secunia Research**, the foundation of our **Software Vulnerability Research (SVR)** solution, operates with **full independence from NVD constraints**. It provides:

- Timely, daily reviewed vulnerability data.
- Enriched advisories with threat scoring and product-specific impact.
- Intelligence mapped to exact software versions and vendor configurations.
- Verified exploit information and remediation guidance.

What This Means for Your Organization

By integrating SVR, businesses gain:

- Rapid vulnerability awareness, often **days or weeks ahead** of NVD.
- Improved prioritization and remediation workflows.
- Greater operational resilience through verified, enriched, and reliable intelligence.

Conclusion

In 2024, relying solely on government databases for vulnerability intelligence is no longer viable. Flexera's SVR and Secunia Research provide the **trusted, independent lens** needed to protect against modern cyber threats in real time.

Risk Scoring Model:

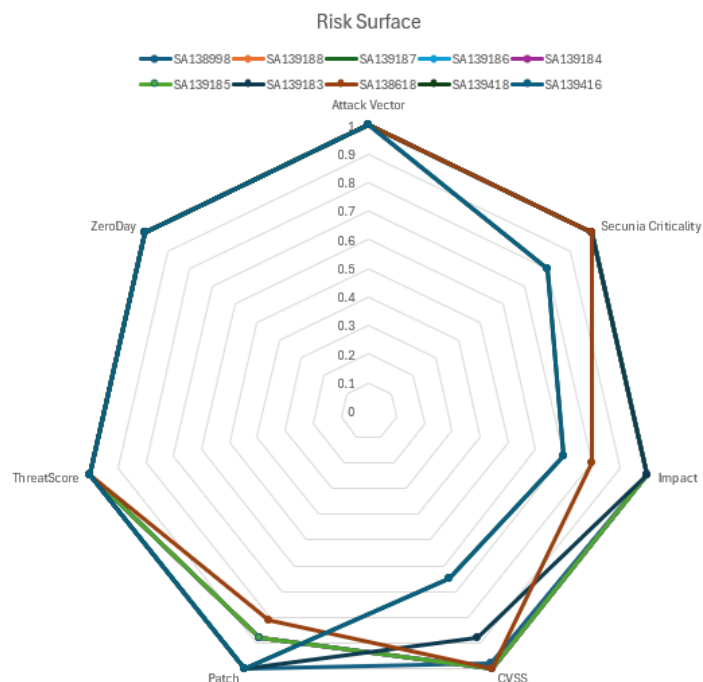
There are many ways to prioritize Software Vulnerabilities , a previous article I wrote on LinkedIn : [Key Elements of a Balanced Risk Scoring Model](#) I shared some key components that can build a balanced risk scoring model. There is no standard in prioritizing vulnerability remediation , but the 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 May based on the calculated Risk Score:



Advisories	Versions	impactName	OS?	Attack Vector	Secunia Criticality	Impact	CVSS	Patch	ThreatScore	ZeroDay	Risk Score
SA138998	Ivanti Endpoint Manager Mobile 11.x	System access	FALSE	1	1	1	0.98	1	1	1	6.98
SA139188	Microsoft Windows Server 2012	System access	TRUE	1	1	1	0.88	1	1	1	6.88
SA139187	Microsoft Windows 10, Microsoft Windows Server 2016	System access	TRUE	1	1	1	0.88	1	1	1	6.88
SA139186	Microsoft Windows Server 2019	System access	TRUE	1	1	1	0.88	1	1	1	6.88
SA139184	Microsoft Windows 11	System access	TRUE	1	1	1	0.88	1	1	1	6.88
SA139185	Microsoft Windows Server 2022	System access	TRUE	1	1	1	0.88	1	1	1	6.88
SA139183	Microsoft Windows Server 2025	System access	TRUE	1	1	1	0.88	1	1	1	6.88
SA138618	Android 13.x, Android 14.x	System access	TRUE	1	0.8	1	0.81	1	1	1	6.61
SA139418	Microsoft Edge (Chromium-Based)	Exposure of sensitive information	FALSE	1	0.8	0.7	0.65	1	1	1	6.15
SA139416	Google Chrome 136.x	Exposure of sensitive information	FALSE	1	0.8	0.7	0.65	1	1	1	6.15

Risk Score Thresholds

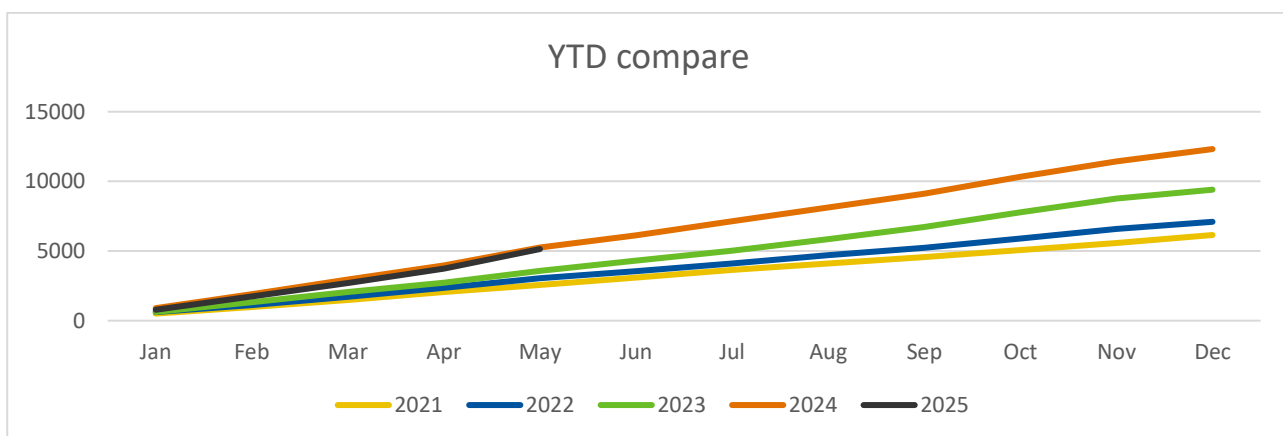
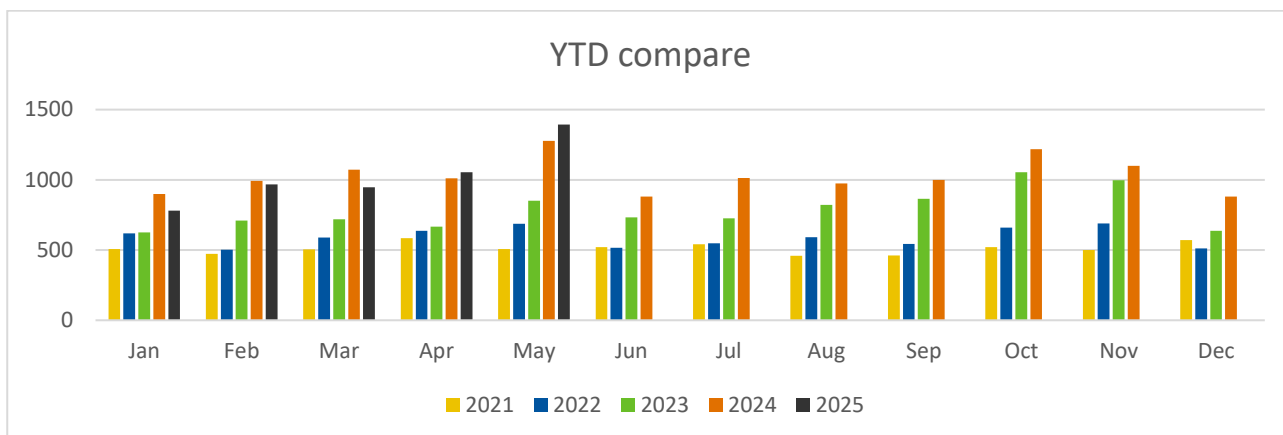
Attack Vector	Secunia Criticality	Impact Severity
Remote Network → 1.0	Extreme Critical → 1.0	System Access → 1.0
Local Network → 0.5	Highly Critical → 0.8	Privilege Escalation, Spoofing → 0.9
Local System → 0.2	Moderately Critical → 0.6	XSS, Hijacking → 0.8
Unknown → 0.0	Less Critical → 0.4	Info Exposure, 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 **May 31, 2025**, the year-to-date total is **5,141** Advisories ↓ which is slightly lower than 2023: **5,251** YTD Advisories)



Monthly data

This month, a total of **1,394** ↑ (last month: **1,053**) advisories were reported by the Secunia Research Team.

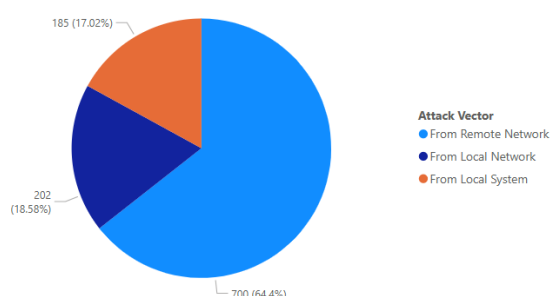
This month:	#	Change (last month):
Total # of advisories	1,394	↑ (1,053)
Unique Vendors	95	↑ (105)
Unique Products	314	↑ (322)
Unique Versions	369	↑ (377)
Rejected Advisories *	307	↑ (183)
NEW Advisories without CVE ID	24	↑ (26)
Advisories with Threat Score (>0)	843	↑ (675)
Total Unique CVE ID's reported	3,549	↑ (3,630)

↑ increased ↓ lower ↔ same

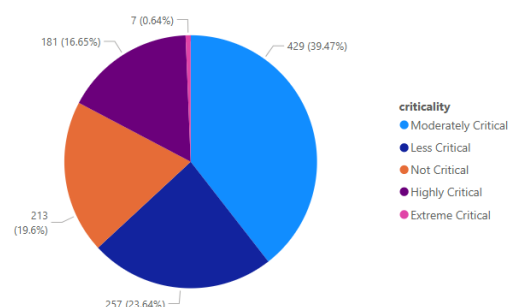
* **369** advisories have received the “rejected” status which means in general that leveraging it would require one or more violations of security best practices (e.g., product not securely configured or not used securely) or that it was “too weak of a gain” (e.g., administrative, local users already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

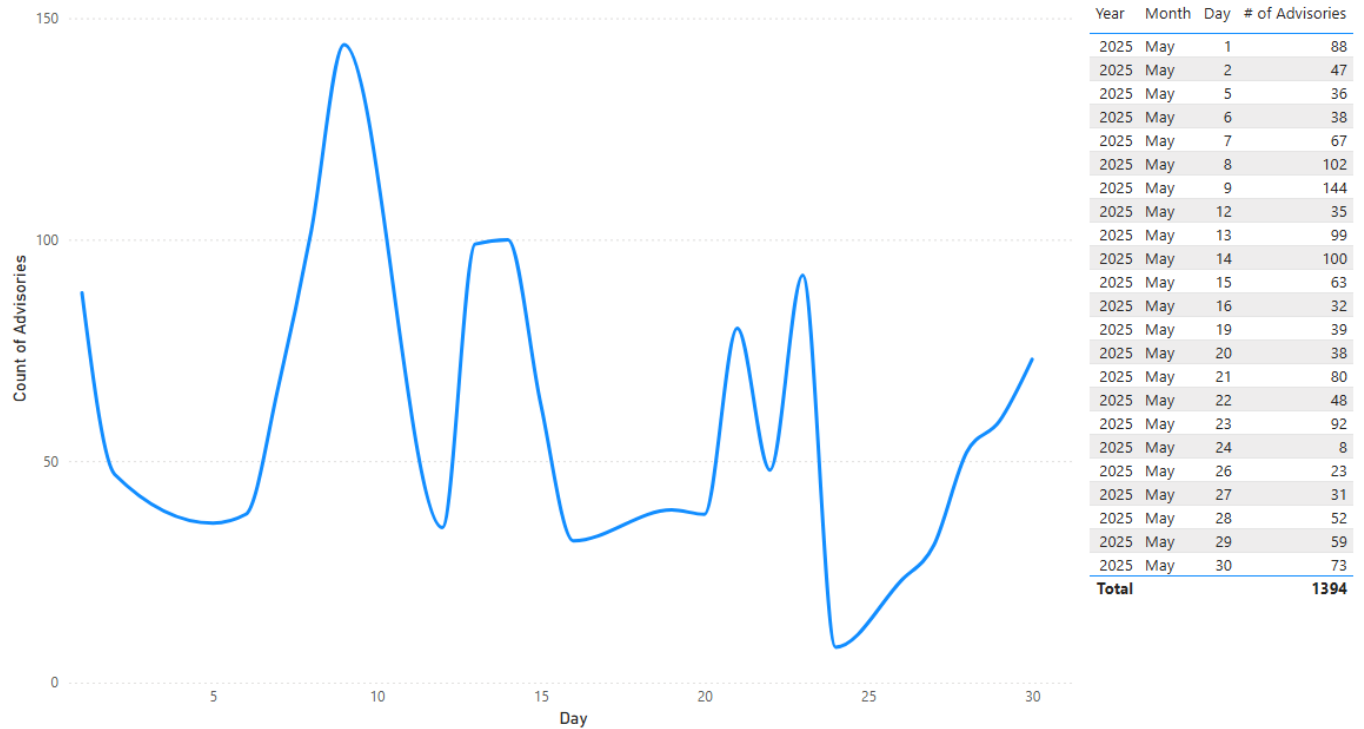


Advisories by criticality



Advisories per day

Below an overview of the daily advisory count.



Advisories without CVE

Advisories	Versions	Cvss3_score	criticality	Description	solution_status
SA139836	Red Hat Enterprise Linux Server Extended Lifecycle Support 7	9.80	Highly Critical	Red Hat update for zlib	Vendor Patched
SA138637	PDF-XChange Editor 10.x	7.80	Moderately Critical	PDF-XChange Editor Multiple Vulnerabilities	Vendor Patched
SA139437	Zimbra Collaboration Suite 10.x, Zimbra Collaboration Suite 9.x	7.50	Moderately Critical	Zimbra Collaboration Suite Denial of Service Vulnerability	Vendor Patched
SA139338	Tailscale 1.x	6.50	Less Critical	Tailscale DERP Server Side-Channel Vulnerability	Vendor Patched
SA139030	Cygwin 4.x	5.60	Moderately Critical	Cygwin update for weechat	Vendor Patched
SA139448	Mattermost 10.x, Mattermost 9.x	5.60	Moderately Critical	Mattermost Multiple Unspecified Vulnerabilities	Vendor Patched
SA139625	CA Aion Business Rules Expert 11.x	5.60	Moderately Critical	CA Aion Business Rules Expert for Windows Multiple Unspecified Vulnerabilities	Partial Fix
SA139739	Mattermost 10.x, Mattermost 9.x	5.60	Moderately Critical	Mattermost Multiple Unspecified Vulnerabilities	Vendor Patched
SA138363	Qlik Sense 14.x	5.30	Moderately Critical	Qlik Sense for Windows Security Bypass Vulnerability	Vendor Patched
SA138820	Linux Kernel 5.10.x, Linux Kernel 5.15.x, Linux Kernel 5.4.x, Linux Kernel 6.1.x	5.30	Not Critical	Linux Kernel "ieee80211_tx_dequeue0" Unspecified Vulnerability	Vendor Patched
SA139861	GitHub Enterprise 3.13.x	3.50	Less Critical	GitHub Enterprise Security Bypass Vulnerability	Vendor Patched
SA138121	SUSE Linux Enterprise Server (SLES) 15 SP6	3.30	Not Critical	SUSE update for brlty	Vendor Patched
SA139738	WinSCP 6.x	3.30	Not Critical	WinSCP File Upload Path Traversal Vulnerability	No Fix
SA133175	YAML::LibYAML 0.x (module for Perl)	0.00	Rejected	Perl YAML::LibYAML Module Rejection Notice	Unknown
SA138657	SUSE Linux Enterprise Server (SLES) 15 SP6	0.00	Rejected	SUSE govulncheck-vulndb Rejection Notice	likely Fixed
SA138779	Linux Kernel 5.15.x, Linux Kernel 6.1.x	0.00	Rejected	Linux Kernel s390/cpumf Rejection Notice	likely Fixed
SA138849	Autodesk Maya 2015, Autodesk Maya 2018	0.00	Rejected	Autodesk Maya Rejection Notice	Unknown
SA138891	SUSE Linux Enterprise Server (SLES) 15 SP6	0.00	Rejected	SUSE govulncheck-vulndb Rejection Notice	likely Fixed
SA139297	SUSE Linux Enterprise Server (SLES) 15 SP6	0.00	Rejected	SUSE govulncheck-vulndb Rejection Notice	likely Fixed
SA139744	SUSE Linux Enterprise Server (SLES) 15 SP6	0.00	Rejected	SUSE govulncheck-vulndb Rejection Notice	likely Fixed
SA139759	Cygwin 3.x	0.00	Rejected	Cygwin libarchive and mingw64-libarchive Rejection Notice	likely Fixed
SA139771	libarchive 3.x	0.00	Rejected	libarchive Rejection Notice	likely Fixed
SA139840	Tailscale 1.x	0.00	Rejected	Tailscale Rejection Notice	likely Fixed
SA140074	SUSE Linux Enterprise Micro 6.0	0.00	Rejected	SUSE ca-certificates-mozilla 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.

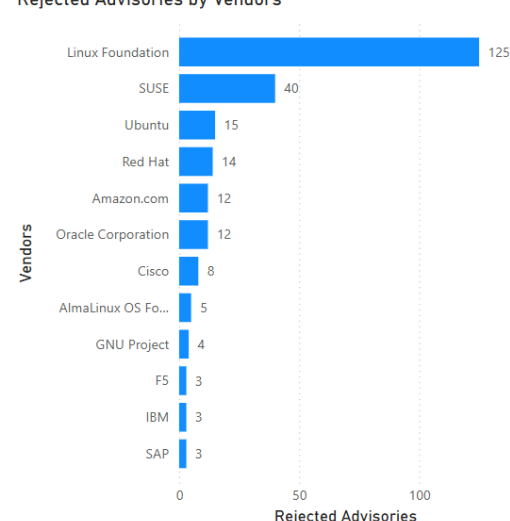


The Secunia Research team at Flexera evaluates vulnerabilities from hundreds of sources, rescors them when necessary and even rejects vulnerabilities not worth your attention. Rejection Advisories help you to reduce the volume of vulnerabilities to be mitigated by helping you focus only on those that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

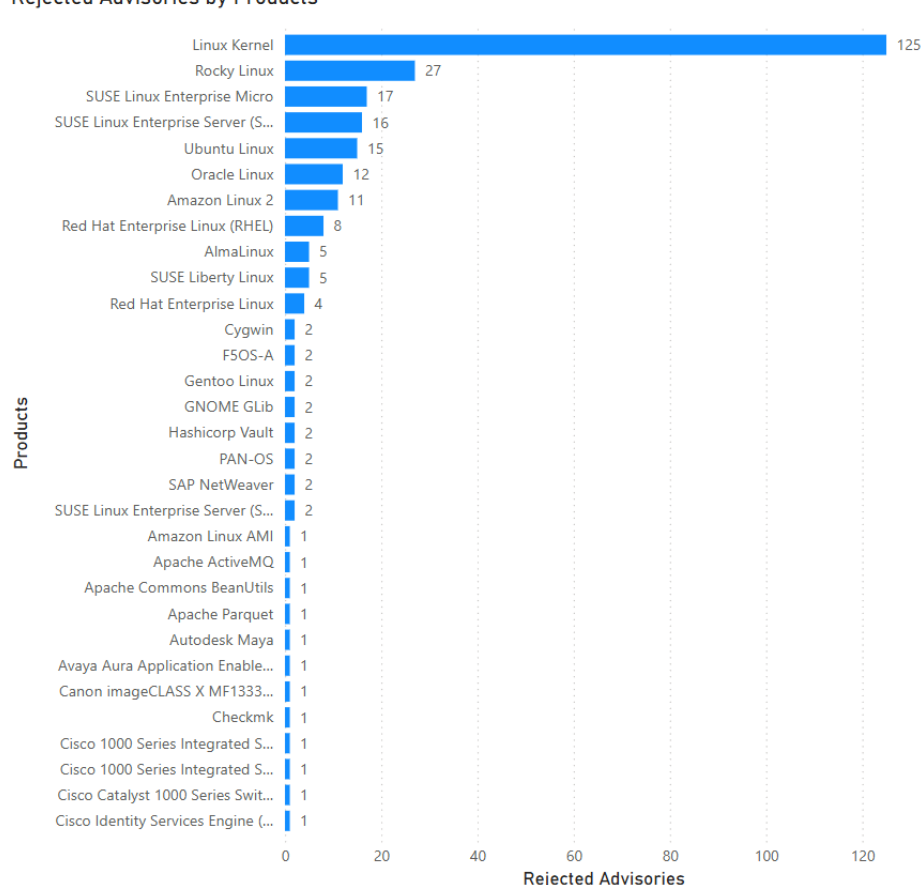
An advisory may be rejected many reasons. The most common are:

- **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.

Rejected Advisories by Vendors



Rejected Advisories by Products



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.

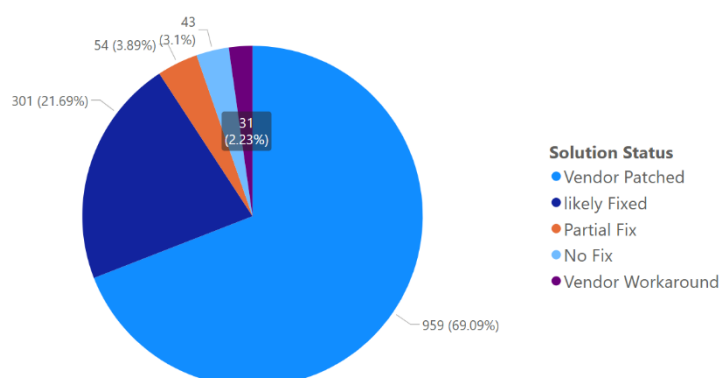
Leverage threat intelligence to better prioritize what demands your most urgent attention.

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).

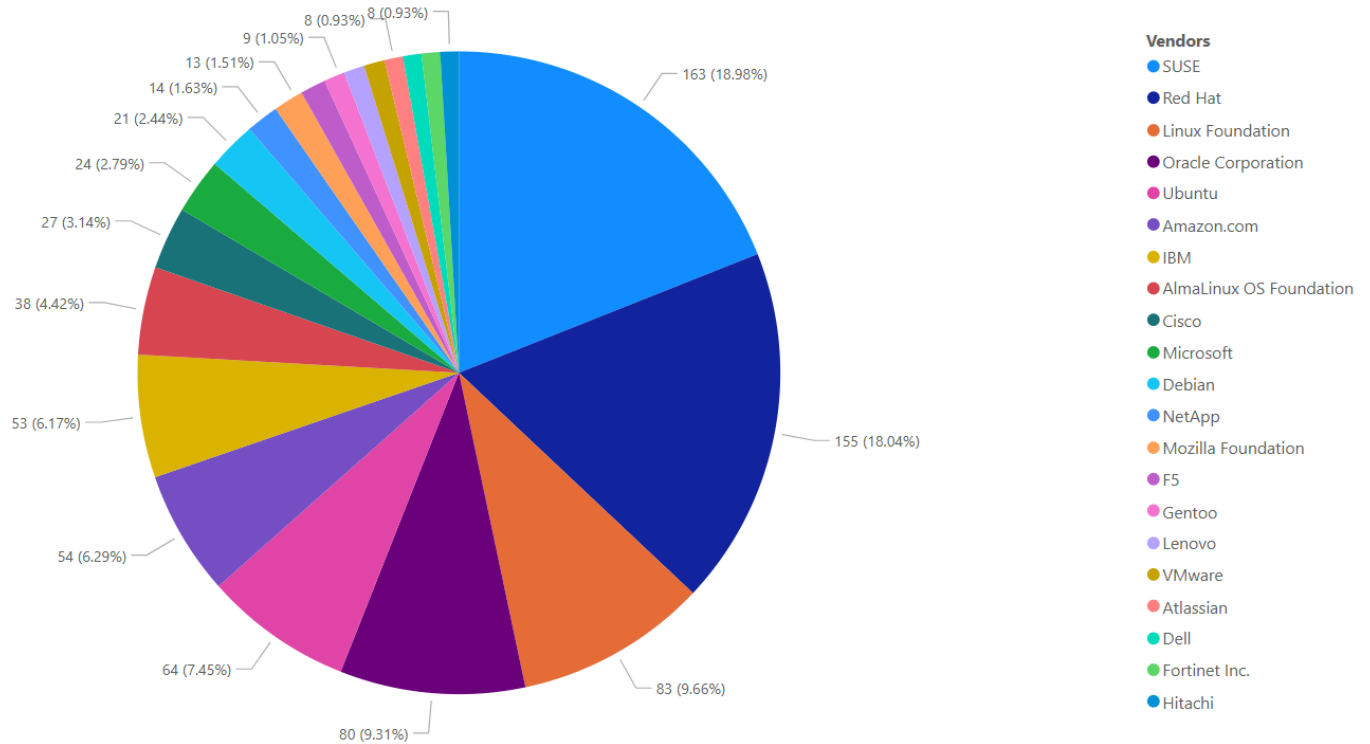
No fix: no patch available for this insecure version, therefore need to upgrade likely (Possibly) fixed: related to a rejection advisory



Vendor view

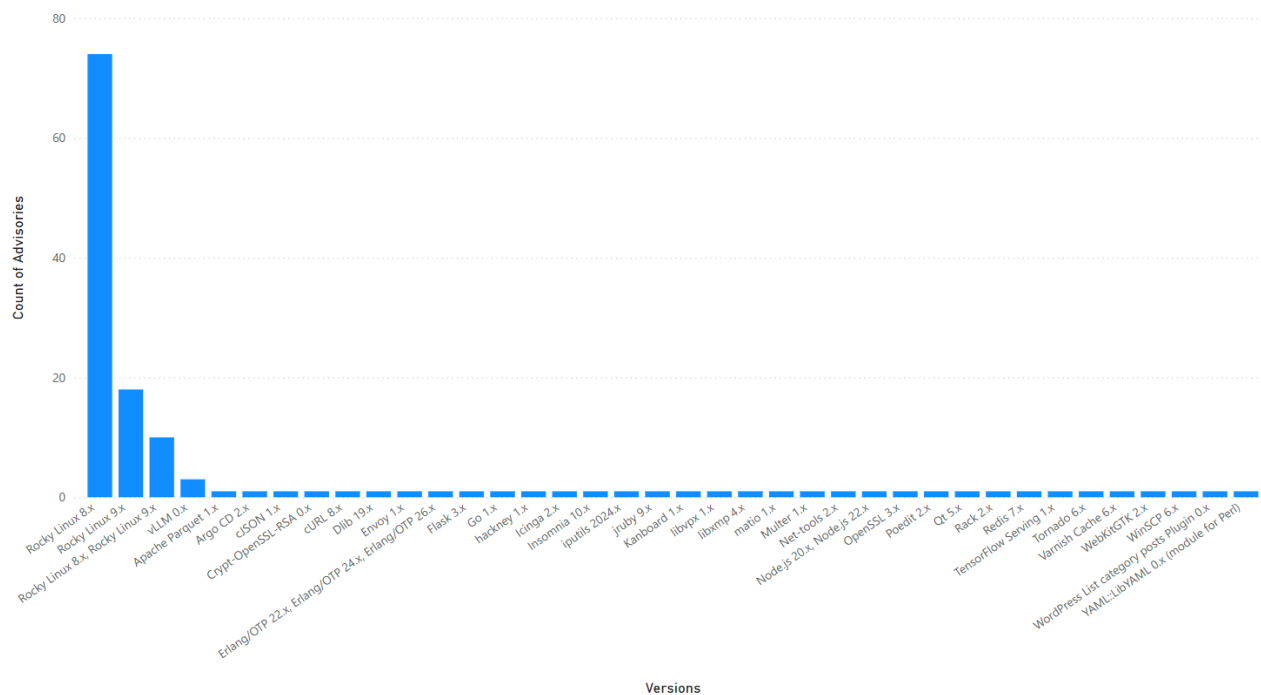
Top vendors with the most advisories

(Excl. Rejection Advisories)

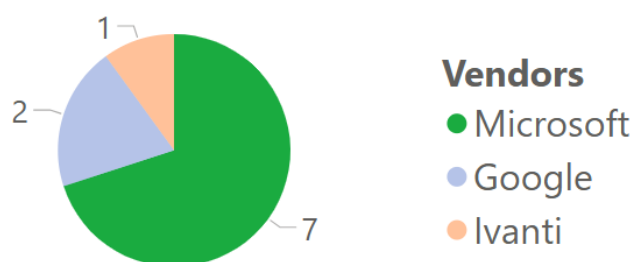


104 Advisories this month were open-source products or plugin

Open-Source Product Versions

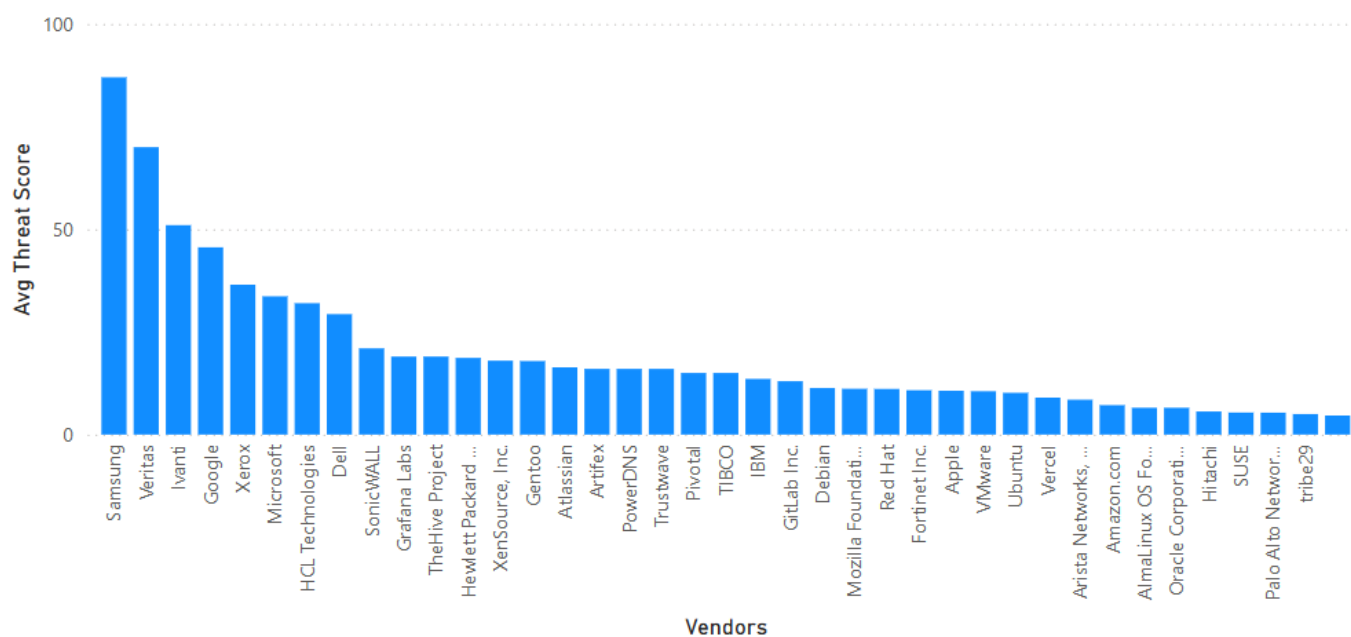


Top vendors with zero-day



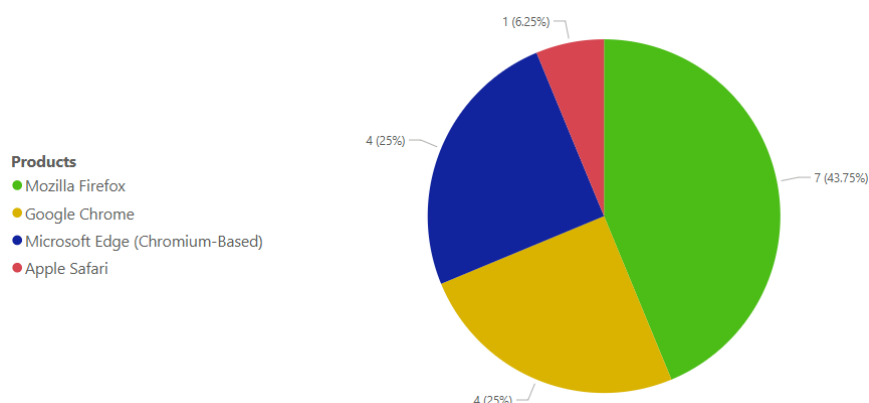
Advisories	Versions	Threatscore
SA138998	Ivanti Endpoint Manager Mobile 11.x	99.00
SA139187	Microsoft Windows 10, Microsoft Windows Server 2016	99.00
SA139184	Microsoft Windows 11	99.00
SA139188	Microsoft Windows Server 2012	99.00
SA139186	Microsoft Windows Server 2019	99.00
SA139185	Microsoft Windows Server 2022	99.00
SA139183	Microsoft Windows Server 2025	99.00
SA139416	Google Chrome 136.x	92.00
SA139418	Microsoft Edge (Chromium-Based)	92.00
SA138618	Android 13.x, Android 14.x	87.00

Top Vendors with highest average threat score



Browser-related advisories

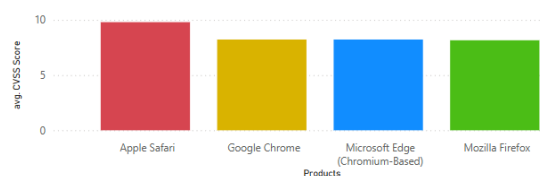
Advisories per browser



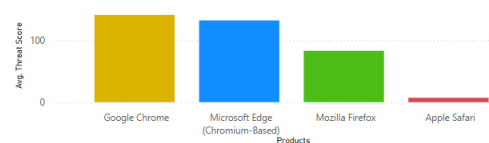
Browser zero-day vulnerabilities

Description	Advisories	Cvss3	ThreatScore	Consequence	is_zero_day
Google Chrome Multiple Vulnerabilities	SA139416	6.50	92.00	Exposure of sensitive information	True
Microsoft Edge (Chromium-Based) Multiple Vulnerabilities	SA139418	6.50	92.00	Exposure of sensitive information	True

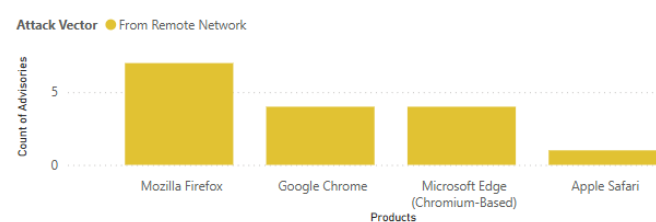
Average CVSS (criticality) score per browser



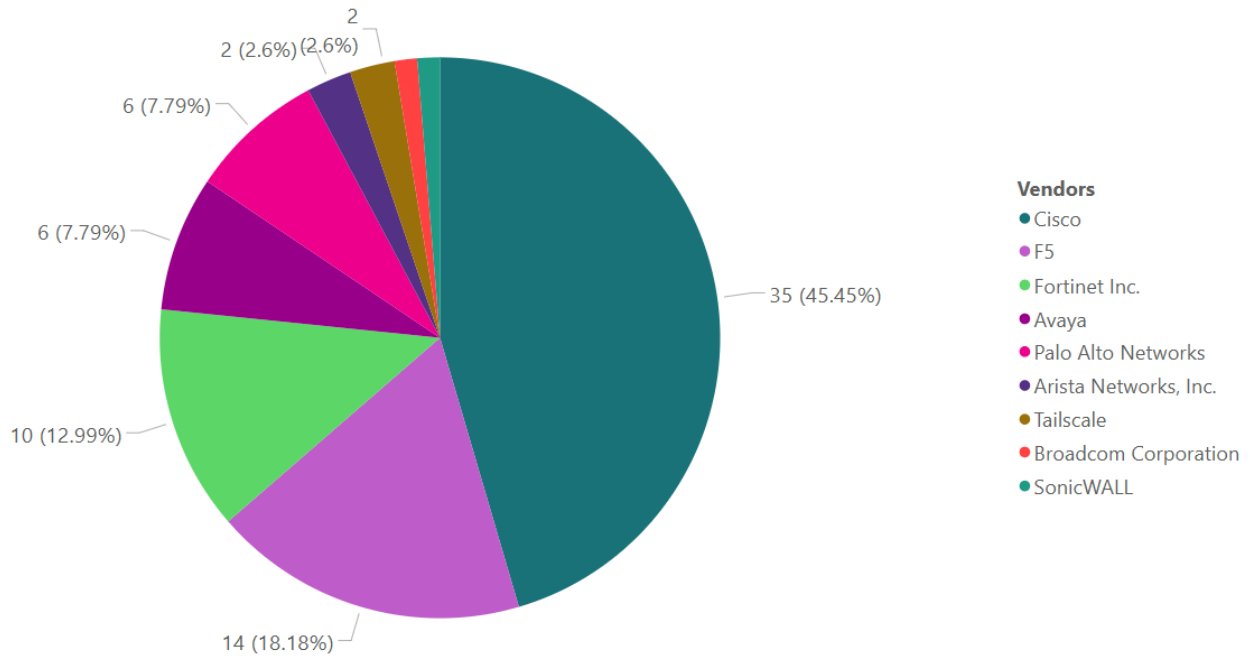
Average threat score per browser



What's the Attack Vector?



Top networking related advisories

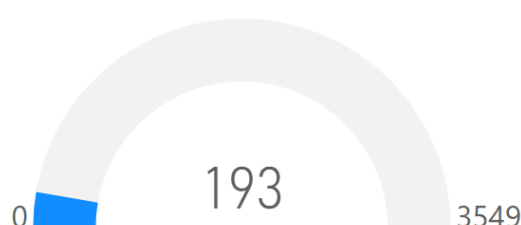


Threat intelligence

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+)	843 ↑ (675)
SAIDs with no threat score (=0)	551 ↑ (378)

SAID: Secunia Advisory Identifier

Range	# SAIDS	Last month
Low-range threat score SAIDs (1-12)	631 ↑ (37)	
Medium-range threat score SAIDs (13-23)	159 ↓ (330)	
Critical-range threat score SAIDs (45-70)	26 ↓ (142)	
Very critical threat score SAIDs (71-99)	25 ↓ (59)	
High-range threat score SAIDs (24-44)	2 ↑ (107)	

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

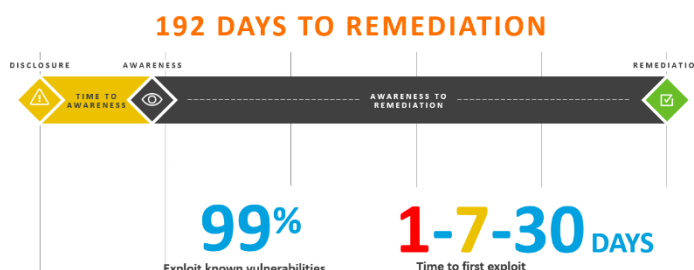
- [Evidence of exploitation](#)
- [Criteria for the threat Score Calculation](#)
- [Threat Score Calculation - Examples](#)

Patching

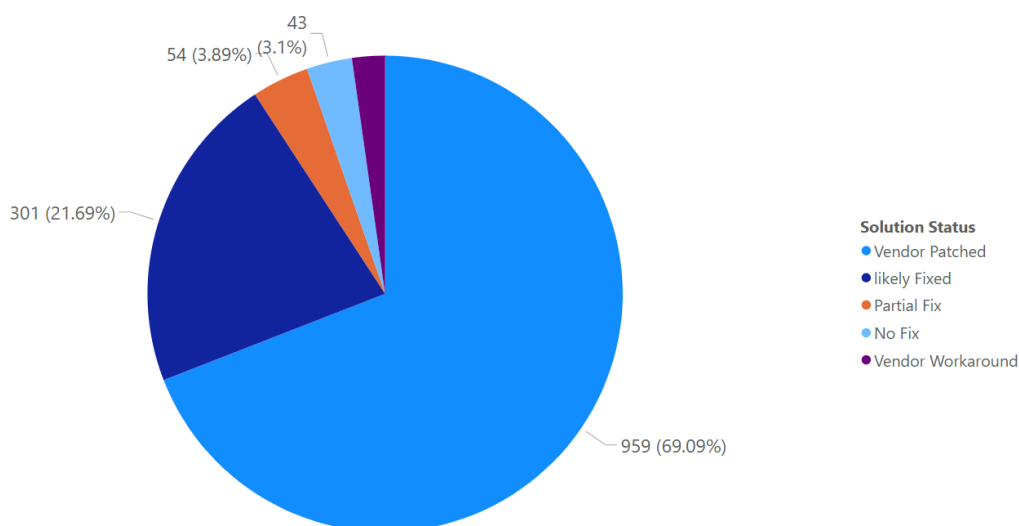
Most of this month's vulnerabilities are vendor patched. In fact, most vulnerabilities are patched within 24 hours after disclosure.

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).

The Risk Window



Vulnerabilities that are vendor patched



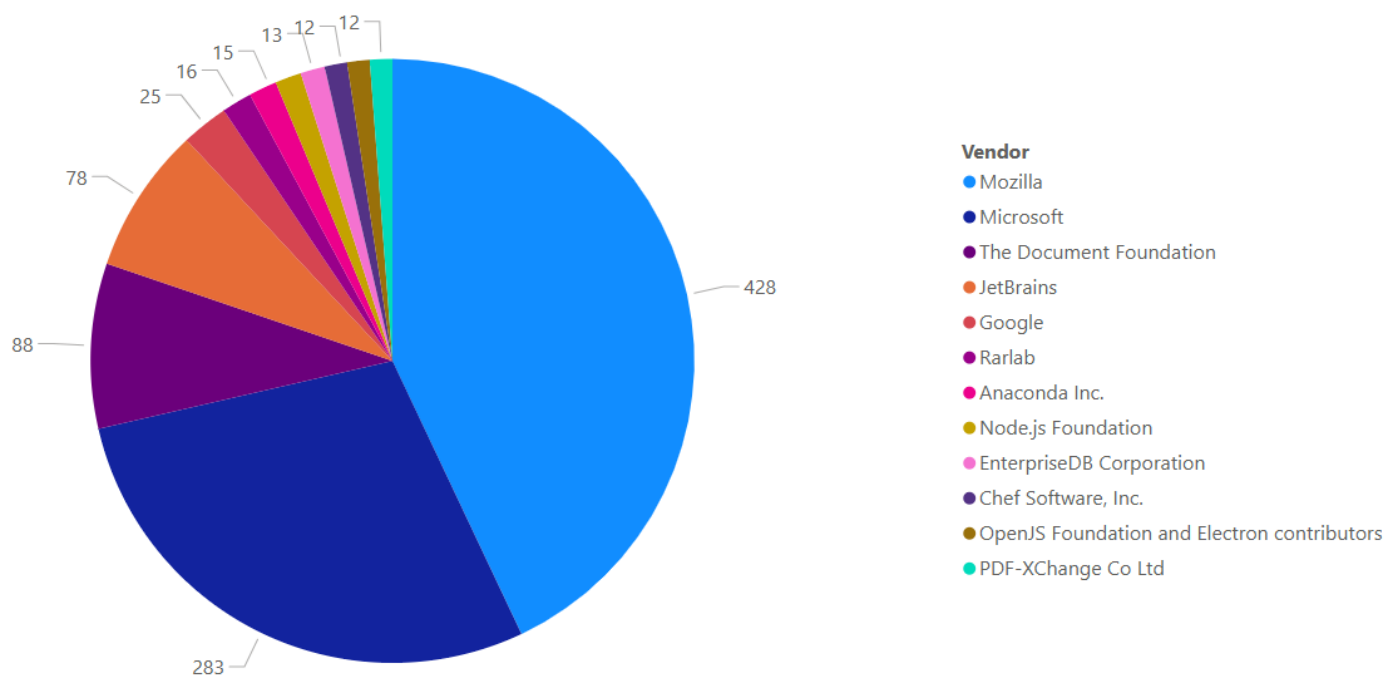
Flexera's Vendor Patch Module (VPM) statistics

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 month's the additions to the KEV catalog

dateAdded	CVE	Vendor	Product	dueDate
01 May 2025	CVE-2023-44221	SonicWall	SMA100 Appliances	22 May 2025
01 May 2025	CVE-2024-38475	Apache	HTTP Server	22 May 2025
02 May 2025	CVE-2024-58136	Yiiframework	Yii	23 May 2025
02 May 2025	CVE-2025-34028	Commvault	Command Center	23 May 2025
05 May 2025	CVE-2025-3248	Langflow	Langflow	26 May 2025
06 May 2025	CVE-2025-27363	FreeType	FreeType	27 May 2025
07 May 2025	CVE-2024-11120	GeoVision	Multiple Devices	28 May 2025
07 May 2025	CVE-2024-6047	GeoVision	Multiple Devices	28 May 2025
12 May 2025	CVE-2025-47729	TeleMessage	TM SGNL	02 June 2025
13 May 2025	CVE-2025-30397	Microsoft	Windows	03 June 2025
13 May 2025	CVE-2025-30400	Microsoft	Windows	03 June 2025
13 May 2025	CVE-2025-32701	Microsoft	Windows	03 June 2025
13 May 2025	CVE-2025-32706	Microsoft	Windows	03 June 2025
13 May 2025	CVE-2025-32709	Microsoft	Windows	03 June 2025
14 May 2025	CVE-2025-32756	Fortinet	Multiple Products	04 June 2025
15 May 2025	CVE-2024-12987	DrayTek	Vigor Routers	05 June 2025
15 May 2025	CVE-2025-42999	SAP	NetWeaver	05 June 2025
15 May 2025	CVE-2025-4664	Google	Chromium	05 June 2025
19 May 2025	CVE-2023-38950	ZKTeco	BioTime	09 June 2025
19 May 2025	CVE-2024-11182	MDaemon	Email Server	09 June 2025
19 May 2025	CVE-2024-27443	Synacor	Zimbra Collaboration Suite (ZCS)	09 June 2025
19 May 2025	CVE-2025-27920	Srimax	Output Messenger	09 June 2025
19 May 2025	CVE-2025-4427	Ivanti	Endpoint Manager Mobile (EPMM)	09 June 2025
19 May 2025	CVE-2025-4428	Ivanti	Endpoint Manager Mobile (EPMM)	09 June 2025
22 May 2025	CVE-2025-4632	Samsung	MagicINFO 9 Server	12 June 2025

Top (YTD) KEV vendors

Vendors added this year with Known Exploited Vulnerabilities according to CISA

Vendor	# of CVEs
Microsoft	23
Ivanti	7
Apple	5
Linux	4
SonicWall	4
Apache	3
Craft CMS	3
Fortinet	3
Mitel	3
SAP	3
VMware	3
Advantive	2
ASUS	2
Cisco	2
Commvault	2
GeoVision	2
Google	2
Hitachi Vantara	2
Oracle	2
Paessler	2
Palo Alto Networks	2
Sitecore	2
Sophos	2
Synacor	2
Zyxel	2
7-Zip	1
Adobe	1
Audinate	1
Aviatrix	1
BeyondTrust	1
Broadcom	1
ConnectWise	1
CrushFTP	1
DrayTek	1
Edimax	1
FreeType	1
Gladinet	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
April	1	CVE-2025-24983	Microsoft	Windows
April	1	CVE-2025-24984	Microsoft	Windows
April	1	CVE-2025-24985	Microsoft	Windows
April	1	CVE-2025-24991	Microsoft	Windows
April	1	CVE-2025-24993	Microsoft	Windows
April	1	CVE-2025-26633	Microsoft	Windows
April	3	CVE-2025-21590	Juniper	Junos OS
April	3	CVE-2025-24201	Apple	Multiple Products
April	8	CVE-2025-24472	Fortinet	FortiOS and FortiProxy
April	8	CVE-2025-30066	tj-actions	changed-files GitHub Action
April	9	CVE-2017-12637	SAP	NetWeaver
April	9	CVE-2024-48248	NAKIVO	Backup and Replication
April	9	CVE-2025-1316	Edimax	IC-7100 IP Camera
April	11	CVE-2025-22457	Ivanti	Connect Secure, Policy Secure, and ZTA Gateways
April	14	CVE-2025-30154	reviewdog	action-setup GitHub Action
April	16	CVE-2019-9874	Sitecore	CMS and Experience Platform (XP)
April	16	CVE-2019-9875	Sitecore	CMS and Experience Platform (XP)
April	17	CVE-2025-2783	Google	Chromium Mojo
April	21	CVE-2024-20439	Cisco	Smart Licensing Utility
April	22	CVE-2025-24813	Apache	Tomcat
April	28	CVE-2025-31161	CrushFTP	CrushFTP
April	29	CVE-2025-29824	Microsoft	Windows
April	29	CVE-2025-30406	Gladinet	CentreStack
April	30	CVE-2024-53150	Linux	Kernel
April	30	CVE-2024-53197	Linux	Kernel

More information

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

- [Flexera'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