MONTHLY VULNERABILITY INSIGHTS

Based on Data from Secunia Research

NOVEMBER 2024

flexera™

Author: Jeroen Braak

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.

Summary

Total advisories: **1,100 (**last month: **1,217**)

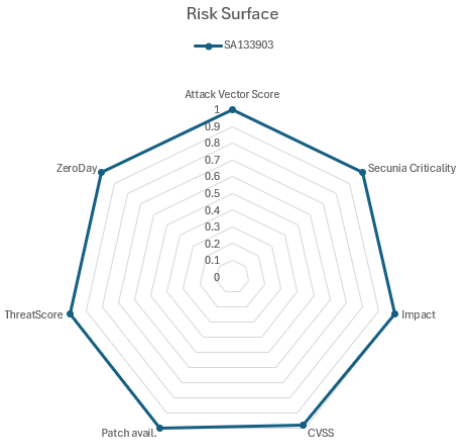
Important conclusions from this month report are:

- **Patch Availability**: An increase from 61.96% in October to 66% in November
- **Advisory Count and Severity**: November saw 1,100 advisories (down from 1,217 in October) with a slight decrease in highly critical (9.73%) and extremely critical advisories (0.27%).
- **Vendor/Product Scope**: November expanded coverage to 93 vendors and 333 products, reflecting a growing attack surface and the importance of comprehensive vulnerability tracking.
- **Attack Vectors**: Remote exploit vulnerabilities increased (40.6% to 45.64%)
- **CVSS3 Scores**: High-risk advisories (7-10) increased from 41.8% to 44.18%, yet a substantial risk remains, emphasizing the value of risk-based prioritization since attackers will aim for medium critical vulnerabilities
- **Threat Intelligence**: Advisories with positive threat scores increased from 49.55% to 52.82% , but only 20 (last month 32) advisories with a threat score between 77-99.

Using Threat Intelligence is going to help you with prioritizing what needs to be **patched** immediately.

Risk Scoring Model for November 2024:

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)

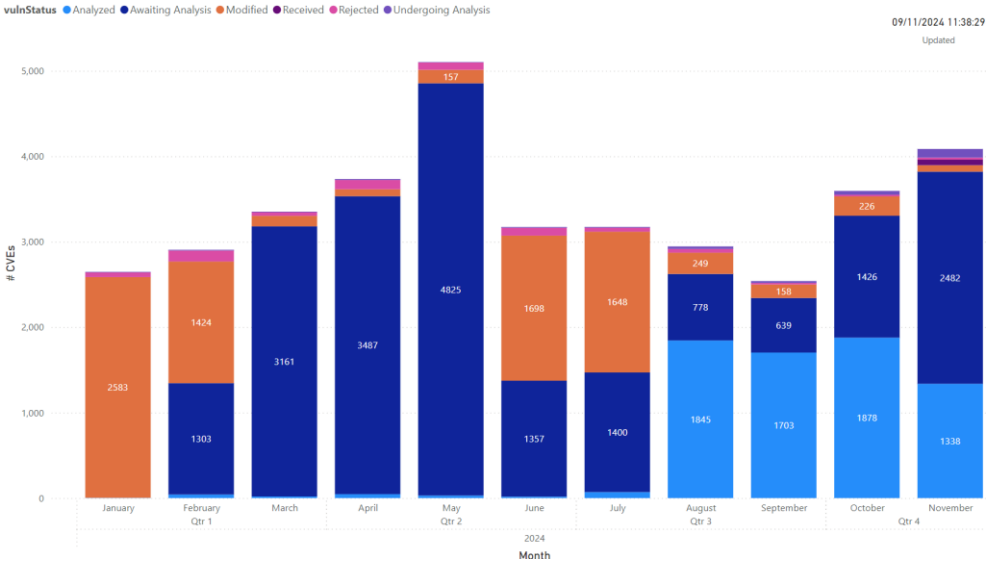
- Attack Vector
- Secunia Criticality Score
- Impact / Consequence
- CVSS Score
- Patch Availability
- Threat Intelligence
- Zero Day

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

My top 10 Advisories released in November:

Advisories	Versions	impactName	Is OS	Description	criticality	CVSS3	ZeroDay	Threat Score	Attack Vector	Vendor Patch	Risk Score
SA133903	WebKitGTK 2.x,	System access	FALSE	WebKitGTK Multiple Vulnerabilities	Extreme Critical	9.8	TRUE	97	Remote Network	Yes	6.98
SA133732	Apple Safari 18.x,	System access	FALSE	Apple Safari Multiple Vulnerabilities	Extreme Critical	9.8	TRUE	97	Remote Network	Yes	6.98
SA133730	Apple macOS 15.x,	System access	TRUE	Apple macOS Sequoia Multiple Vulnerabilities	Extreme Critical	9.8	TRUE	97	Remote Network	Yes	6.98
SA132695	Android 12.x, Android 13.x, Android 14.x,	System access	TRUE	Android Multiple Vulnerabilities	Highly Critical	9.8	TRUE	95	Remote Network	Yes	6.78
SA133346	Microsoft Windows 10, Microsoft Windows Server 2016,	System access	TRUE	Microsoft Windows Server 2016 / Windows 10 Multiple Vulnerabilities	Highly Critical	9	TRUE	99	Remote Network	Yes	6.7
SA133343	Microsoft Windows 11,	System access	TRUE	Microsoft Windows 11 Multiple Vulnerabilities	Highly Critical	9	TRUE	99	Remote Network	Yes	6.7
SA133344	Microsoft Windows Server 2022,	System access	TRUE	Microsoft Windows Server 2022 Multiple Vulnerabilities	Highly Critical	9	TRUE	99	Remote Network	Yes	6.7
SA133342	Microsoft Windows Server 2025,	System access	TRUE	Microsoft Server 2025 Multiple Vulnerabilities	Highly Critical	9	TRUE	99	Remote Network	Yes	6.7
SA133347	Microsoft Windows Server 2012,	System access	TRUE	Microsoft Windows Server 2012 Multiple Vulnerabilities	Highly Critical	8.8	TRUE	97	Remote Network	Yes	6.68
SA133731	Apple iOS 18.x, Apple iPadOS 18.x,	System access	TRUE	Apple iOS / iPadOS Multiple Vulnerabilities	Highly Critical	9.8	FALSE	97	Remote Network	Yes	5.78

The Growing Challenges with NVD: Why It's Time to Rethink Vulnerability Data Reliance



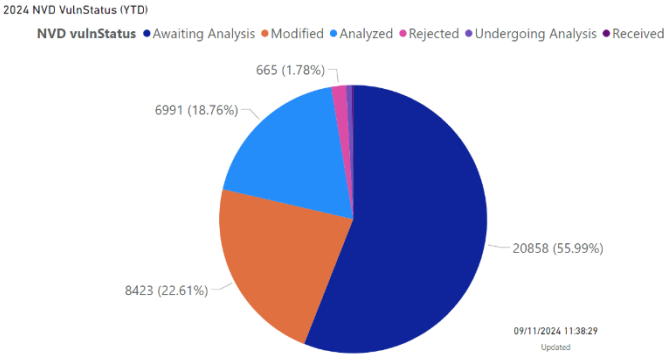
In today's high-stakes cybersecurity landscape, where an average of 150 CVEs are disclosed daily, global tensions escalate, and AI empowers malicious actors to craft and deploy exploits within minutes, timely and accurate vulnerability intelligence is more critical than ever.

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

The Decline of NVD: A Data-Driven Crisis

Recent data exposes a growing backlog within the NVD, casting doubt on its ability to keep pace with the demands of modern cybersecurity:

- **Backlog Explosion:** November 2024 recorded 20,858 CVEs awaiting analysis, constituting 56% of all CVEs reported that year. Only 18.7% of 2024 vulnerabilities have been analysed—a troubling statistic.
- **Accuracy Erosion:** Over 8,423 CVEs have been amended by their respective CNA sources, creating discrepancies between NVD data and the actual state of vulnerabilities.
- **Operational Disruptions:** Persistent API performance issues, including recent outages, have rendered automated data retrieval and integrations unreliable. This further complicates vulnerability management workflows for organizations dependent on the NVD.



The Human and Business Costs of NVD Challenges

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

1. **Extended Risk Windows:** The lag in vulnerability analysis prolongs the time it takes to detect, prioritize, and remediate vulnerabilities. With some exploits weaponized in as little as 1-7 days after disclosure, the risk window is dangerously wide.
2. **Resource Strain:** Security teams often resort to manual research and cross-referencing, sapping valuable resources that could otherwise be directed toward proactive measures.
3. **Compliance Challenges:** Delayed and incomplete data impacts an organization's ability to meet regulatory requirements, such as NIS2 or industry-specific mandates.

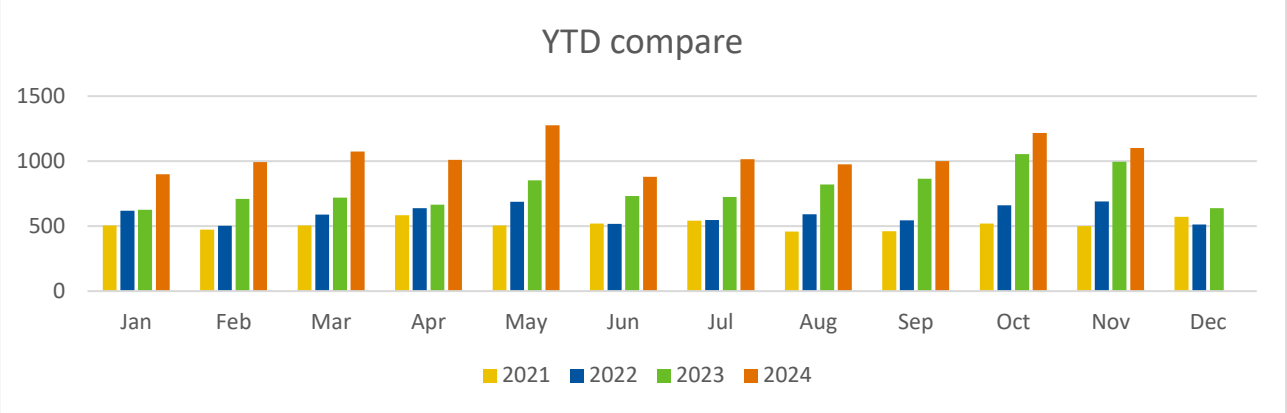
Flexera: A Trusted Alternative for Comprehensive Vulnerability Intelligence

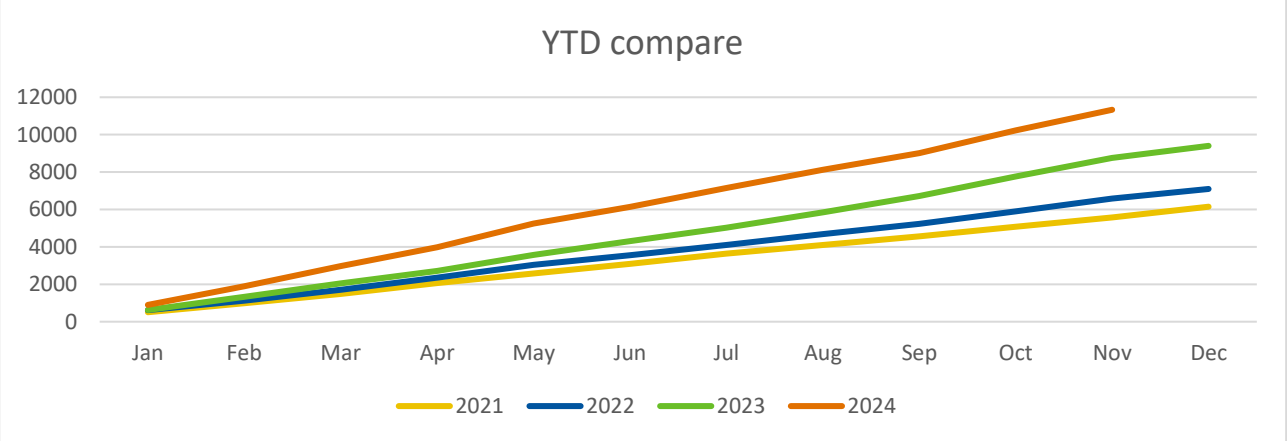
Flexera's Software Vulnerability Research (SVR) and Software Vulnerability Manager (SVM) offer a reliable solution to the growing limitations of the NVD. Backed by Secunia Research, these tools provide:

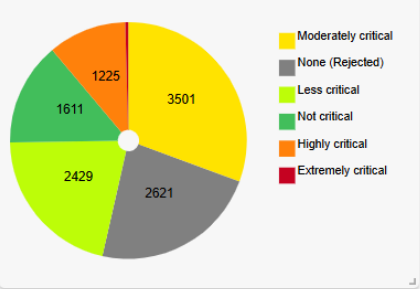
- Timely and Verified Data: Vulnerability advisories are tested, verified, and continuously updated, ensuring that customers receive accurate and actionable intelligence.
- Comprehensive Coverage: Secunia Research draws from hundreds of sources to validate vulnerabilities across diverse environments, ensuring no gaps in visibility.
- Automation and Efficiency: Flexera solutions integrate seamlessly into existing workflows, enabling automated vulnerability detection, prioritization, and patching, significantly reducing manual effort and human error.

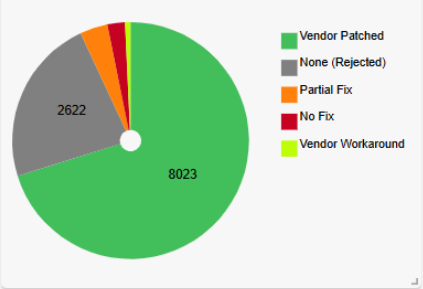
Year-to-date overview

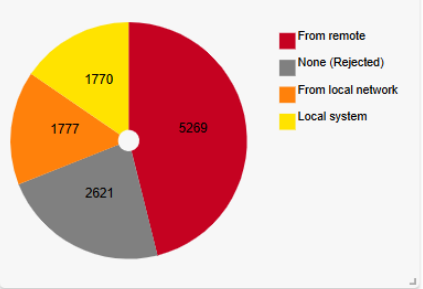
As of **November 30, 2024**, the year-to-date total is 11,437 Advisories ↑ which is **30%** higher than 2023: **8,765** YTD Advisories)

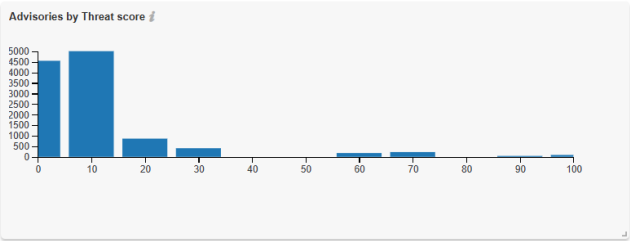


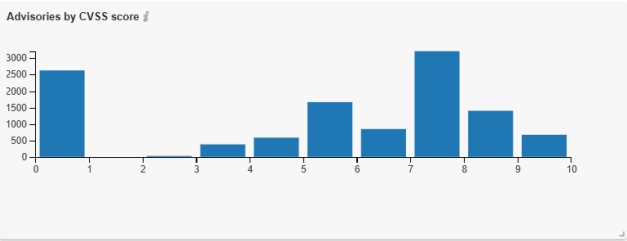












Monthly data

This month, a total of **1,100** ↓ (last month: **1,217**) advisories were reported by the Secunia Research Team.

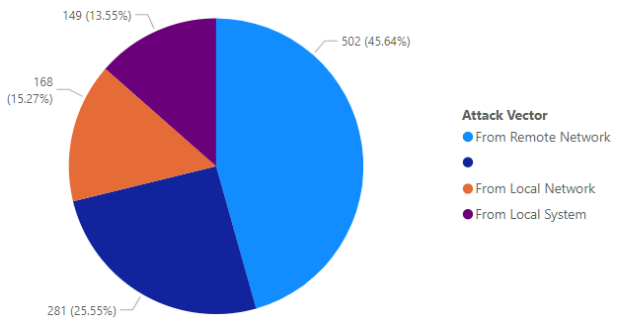
This month:	#	Change *(last month):*
Total # of advisories	**1,100**	↓ *(**1,247**)*
Unique Vendors	**93**	↑ *(**88**)*
Unique Products	**333**	↓ **(357***)*
Unique Versions	**426**	↓ ***(440)***
Rejected Advisories *	**281**	↓ ***(333)***
NEW Advisories without CVE ID	**18**	= *(**18**)*
Advisories with Threat Score (>0)	**581**	↓ **(603)**
Total Unique CVE ID's reported	**2,678**	↓ **(2,589)**

↑ increased ↓lower ↔ same

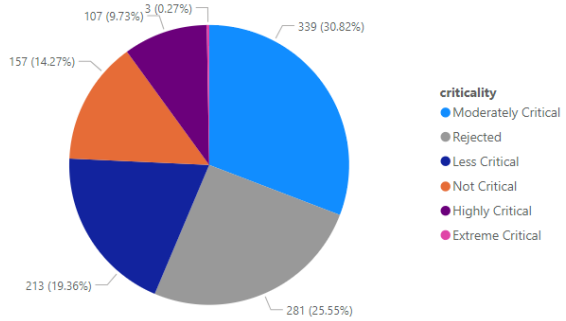
** **281** advisories have received the "rejected" status which means in general that leveraging it would require one or more violations of security best practices (e.g., product not securely configured or not used securely) or that it was "too weak of a gain" (e.g., administrative, local users already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

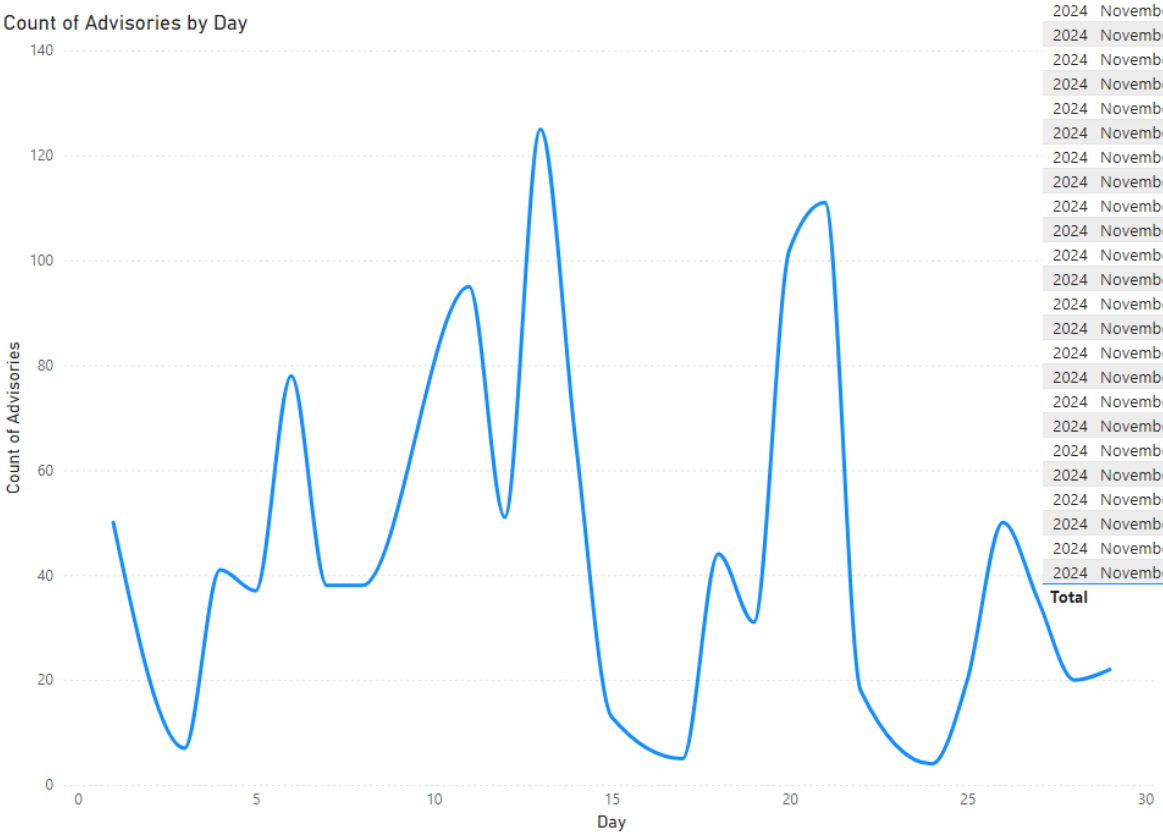


Advisories by criticality



Advisories per day

Below an overview of the daily advisory count.



Year	Month	Day	# of Advisories
2024	November	1	50
2024	November	3	7
2024	November	4	41
2024	November	5	37
2024	November	6	78
2024	November	7	38
2024	November	8	38
2024	November	11	95
2024	November	12	51
2024	November	13	125
2024	November	14	65
2024	November	15	13
2024	November	17	5
2024	November	18	44
2024	November	19	31
2024	November	20	102
2024	November	21	111
2024	November	22	18
2024	November	24	4
2024	November	25	20
2024	November	26	50
2024	November	27	35
2024	November	28	20
2024	November	29	22
Total			**1100**

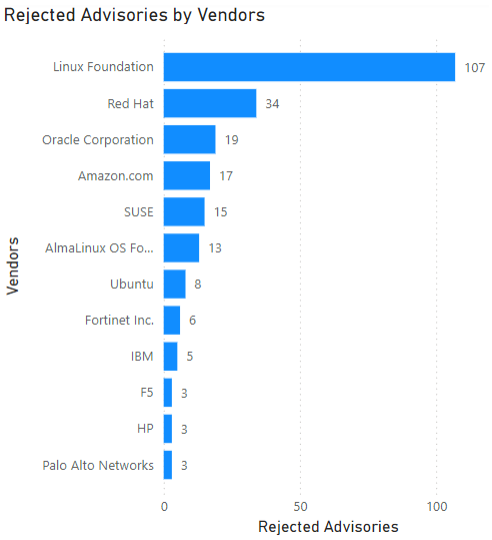
Rejected advisories.

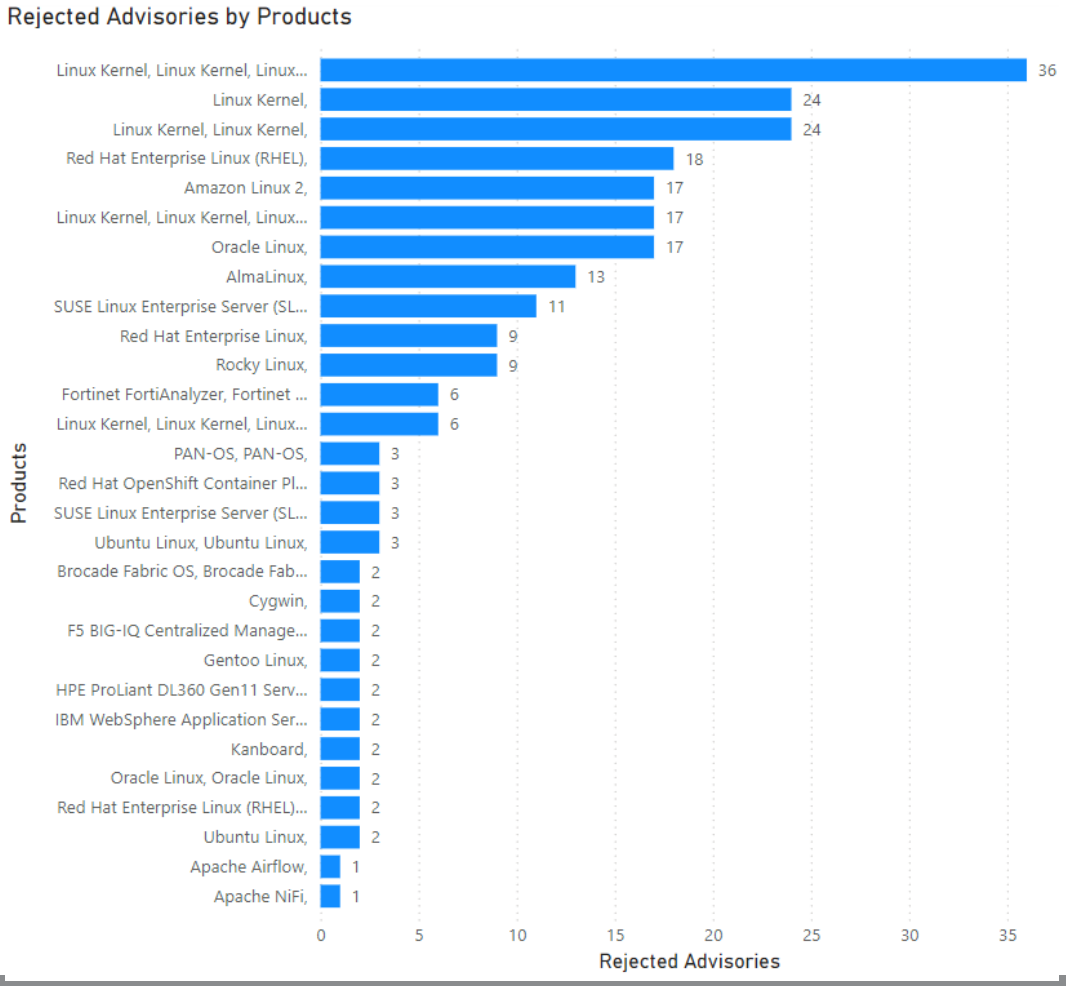
There are many vulnerabilities posted to the National Vulnerability Database (NVD) by a lot of people and companies. They are not always valid, assigned a proper criticality, and in some cases, a vulnerability may be legitimate but not afford the attacker any benefit.

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:

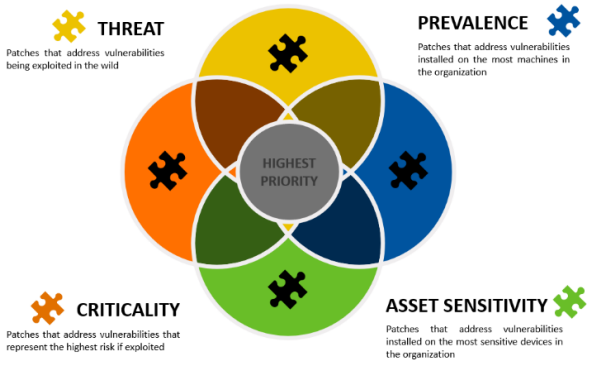
- What systems would result in the most risk if compromised?
- Is it a high-risk device? **Patch**.

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?

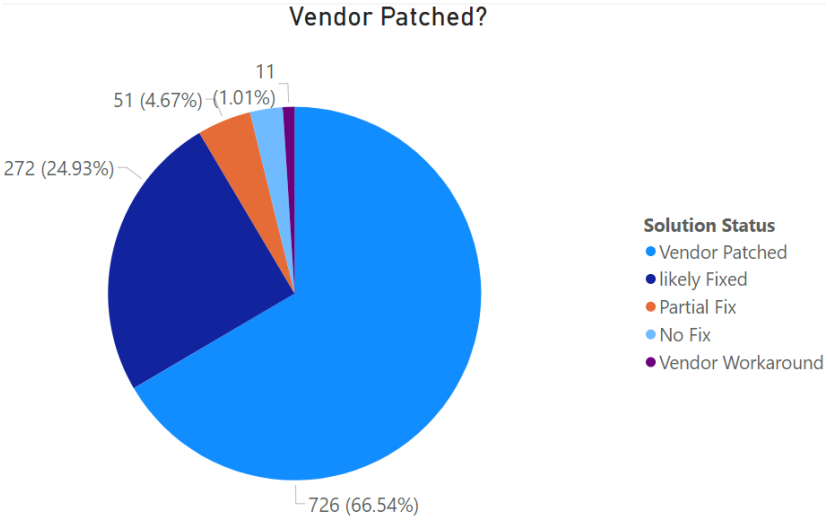
Focusing on vulnerabilities with CVSS 7 or higher would address about 50 percent of exploits. Most exploits are CVSS scored between 4 and 7. Focusing
on vulnerabilities for the top 20 vendors would address only about 20 percent.

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.

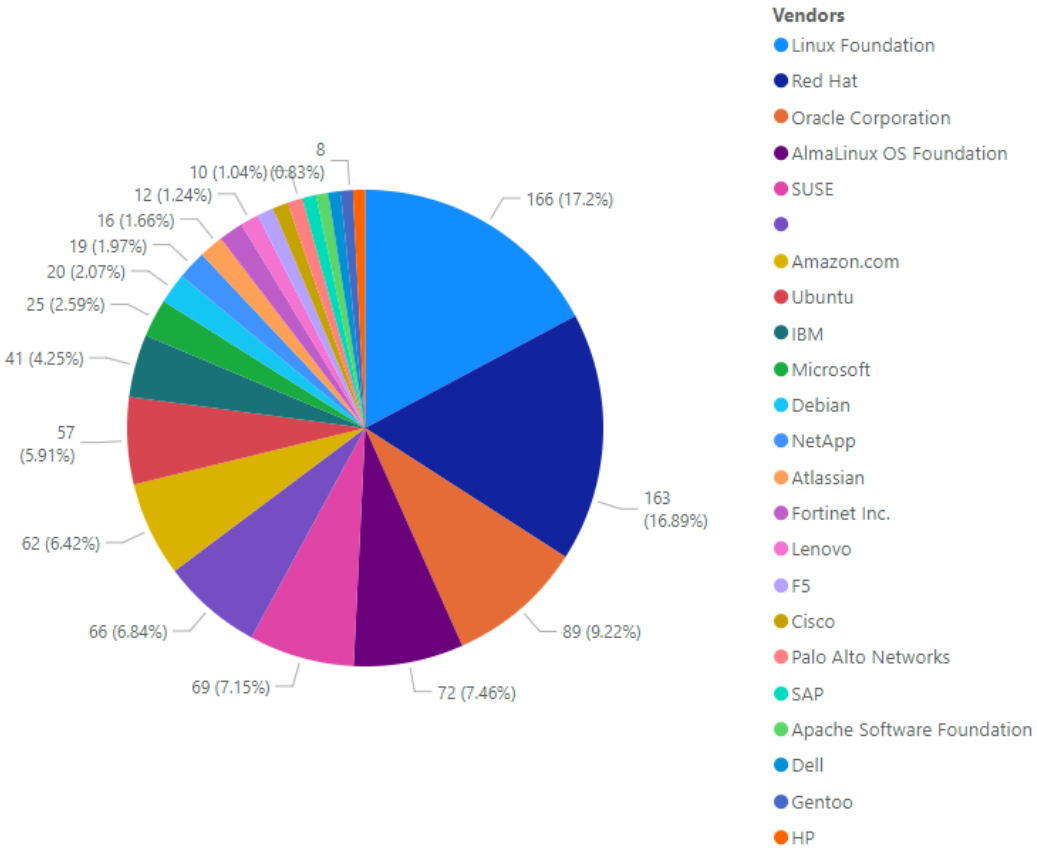
Take away 2:

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

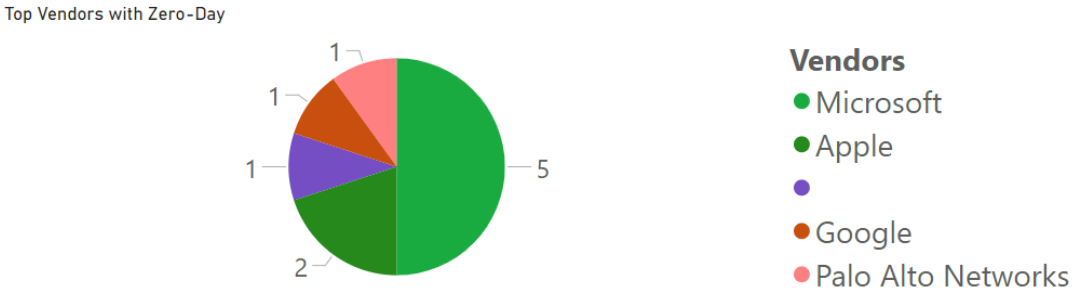


Vendor view

Top vendors with the most advisories

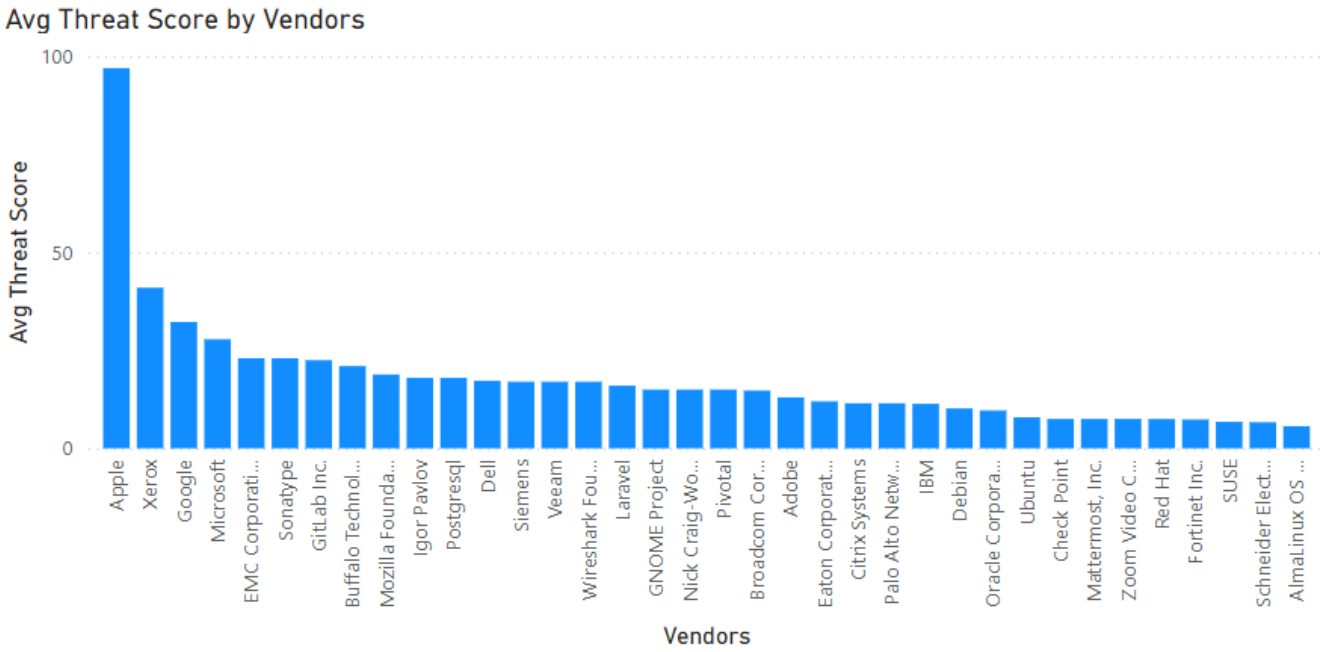


Top vendors with zero-day



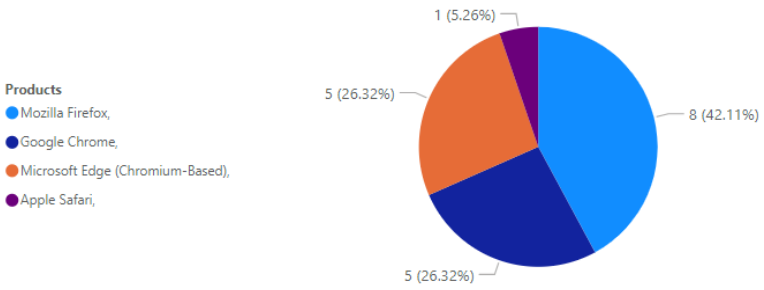
Advisories	Versions
SA132695	Android 12.x, Android 13.x, Android 14.x,
SA133730	Apple macOS 15.x,
SA133732	Apple Safari 18.x,
SA133346	Microsoft Windows 10, Microsoft Windows Server 2016,
SA133343	Microsoft Windows 11,
SA133347	Microsoft Windows Server 2012,
SA133344	Microsoft Windows Server 2022,
SA133342	Microsoft Windows Server 2025,
SA133088	PAN-OS 10.x, PAN-OS 11.x,
SA133903	WebKitGTK 2.x,

Top Vendors with highest average threat score



Browser-related advisories

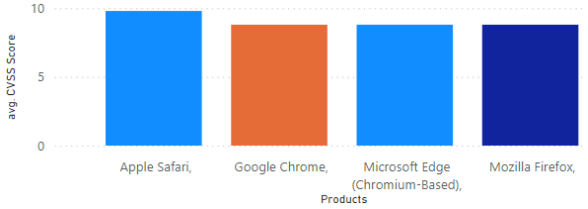
Advisories per browser



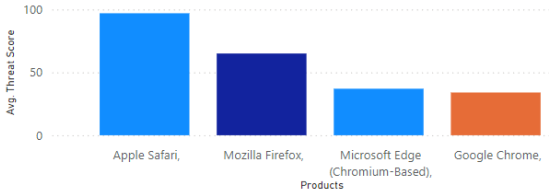
Browser zero-day vulnerabilities

Description	Advisories	Cvss3	ThreatScore	Consequence
Microsoft Edge (Chromium-Based) Multiple Arbitrary Code Execution Vulnerabilities	SA132949	8.80	3.00	System access
Google Chrome Multiple Arbitrary Code Execution Vulnerabilities	SA133085	8.80	3.00	System access
Google Chrome Multiple Vulnerabilities	SA133354	8.80	16.00	System access
Microsoft Edge (Chromium-Based) Multiple Vulnerabilities	SA133466	8.80	18.00	System access
Google Chrome Multiple Vulnerabilities	SA133672	8.80	15.00	System access
Apple Safari Multiple Vulnerabilities	SA133732	9.80	97.00	System access
Microsoft Edge (Chromium-Based) Multiple Vulnerabilities	SA133835	8.80	16.00	System access
Mozilla Firefox Multiple Vulnerabilities	SA133973	8.80	23.00	System access
Mozilla Firefox ESR Multiple Vulnerabilities	SA133977	8.80	19.00	System access
Mozilla Firefox ESR Multiple Vulnerabilities	SA133978	8.80	23.00	System access

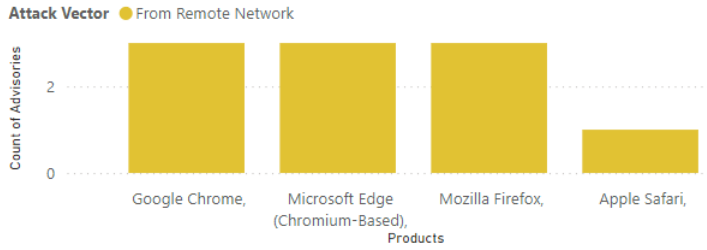
Average CVSS (criticality) score per browser



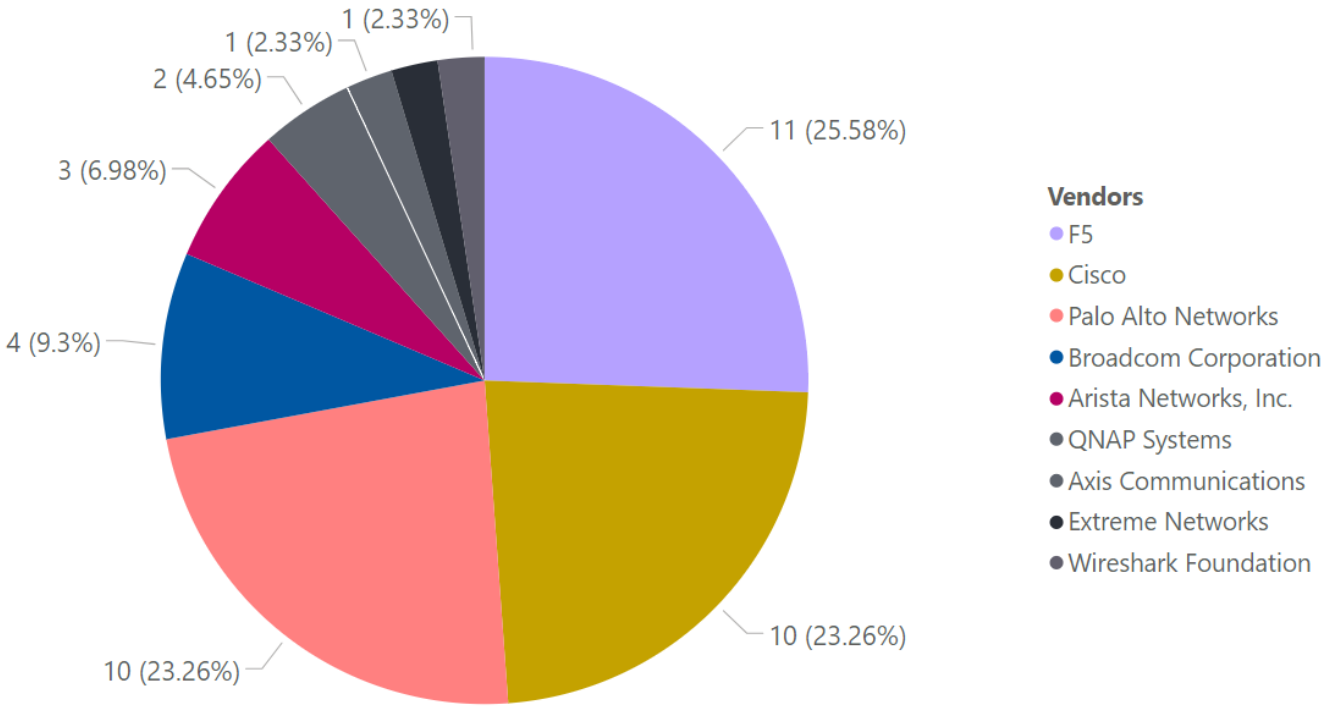
Average threat score per browser



What's the Attack Vector?



Networking related advisories

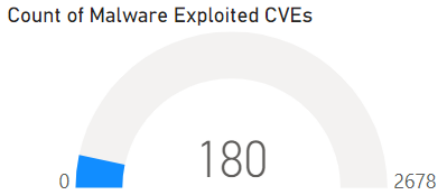


Threat intelligence

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+)	**581** ↑ (603)	52.82%
SAIDs with no threat score (=0)	**519** ↓ (614)	47.18%

SAID: Secunia Advisory Identifier

Range	# SAIDS	Last month
Low-range threat score SAIDs (1-12)	402 ↑	(377)
Medium-range threat score SAIDs (13-23)	142 ↓	(171)
Very critical threat score SAIDs (71-99)	**20** ↓	(34)
Critical-range threat score SAIDs (45-70)	14 ↓	(16)
High-range threat score SAIDs (24-44)	3 =	(3)

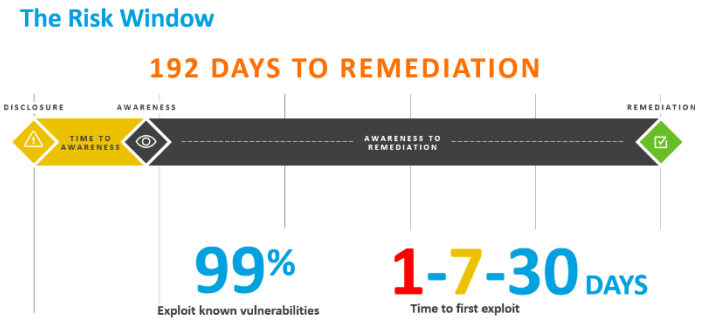
More information about how the Secunia team calculates the threat score:

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

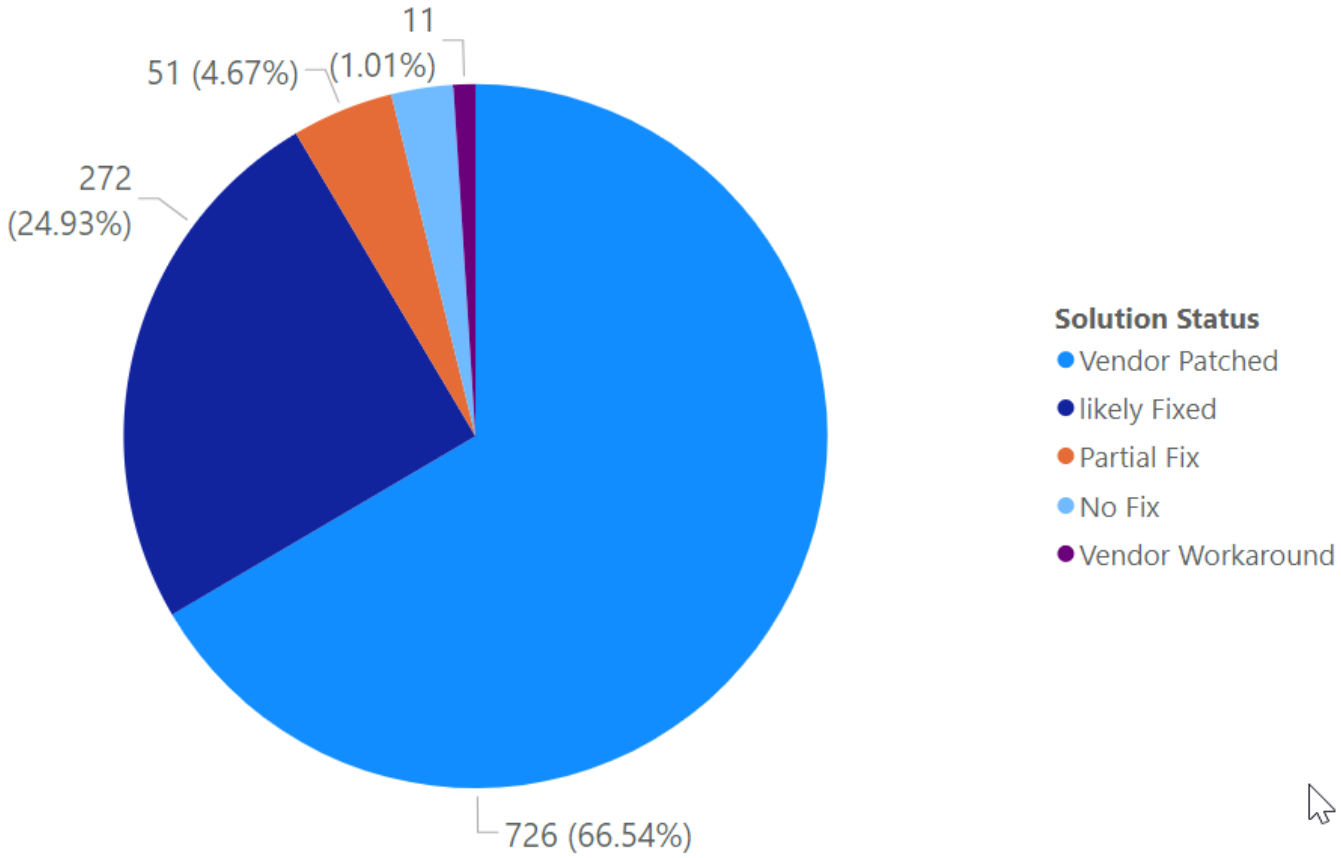
Patching

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

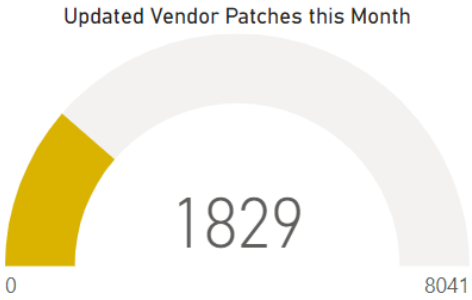


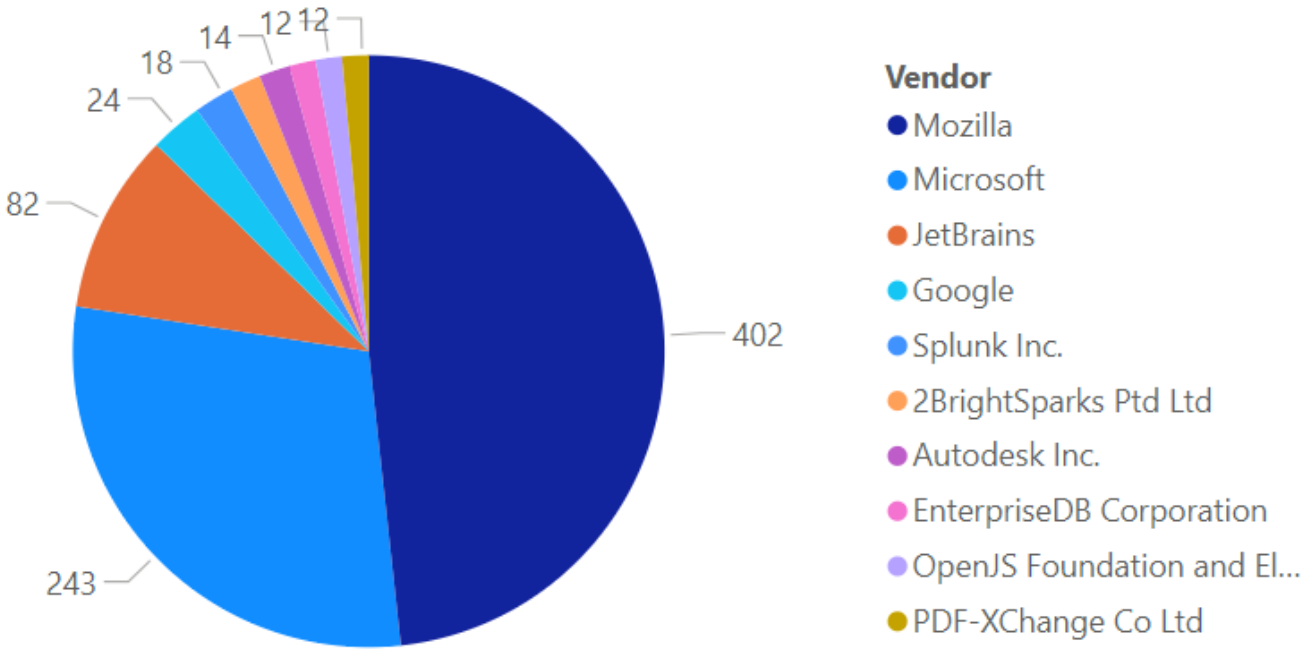
Flexera's Vendor Patch Module (VPM) statistics

Flexera has the largest third-party patch catalog **(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
04 November 2024	CVE-2024-8956	PTZOptics	PT30X-SDI/NDI Cameras	25 November 2024
04 November 2024	CVE-2024-8957	PTZOptics	PT30X-SDI/NDI Cameras	25 November 2024
07 November 2024	CVE-2019-16278	Nostromo	nhttpd	28 November 2024
07 November 2024	CVE-2024-43093	Android	Framework	28 November 2024
07 November 2024	CVE-2024-51567	CyberPersons	CyberPanel	28 November 2024
07 November 2024	CVE-2024-5910	Palo Alto Networks	Expedition	28 November 2024
12 November 2024	CVE-2014-2120	Cisco	Adaptive Security Appliance (ASA)	03 December 2024
12 November 2024	CVE-2021-26086	Atlassian	Jira Server and Data Center	03 December 2024
12 November 2024	CVE-2021-41277	Metabase	Metabase	03 December 2024
12 November 2024	CVE-2024-43451	Microsoft	Windows	03 December 2024
12 November 2024	CVE-2024-49039	Microsoft	Windows	03 December 2024
14 November 2024	CVE-2024-9463	Palo Alto Networks	Expedition	05 December 2024
14 November 2024	CVE-2024-9465	Palo Alto Networks	Expedition	05 December 2024
18 November 2024	CVE-2024-0012	Palo Alto Networks	PAN-OS	09 December 2024
18 November 2024	CVE-2024-1212	Progress	Kemp LoadMaster	09 December 2024
18 November 2024	CVE-2024-9474	Palo Alto Networks	PAN-OS	09 December 2024
20 November 2024	CVE-2024-38812	VMware	vCenter Server	11 December 2024
20 November 2024	CVE-2024-38813	VMware	vCenter Server	11 December 2024
21 November 2024	CVE-2024-21287	Oracle	Agile Product Lifecycle Management (PLM)	12 December 2024
21 November 2024	CVE-2024-44308	Apple	Multiple Products	12 December 2024
21 November 2024	CVE-2024-44309	Apple	Multiple Products	12 December 2024
25 November 2024	CVE-2023-28461	Array Networks	AG/vxAG ArrayOS	16 December 2024

Top 10 (YTD) KEV vendors

Vendor	# of CVEs
Microsoft	32
Ivanti	11
Google	9
Adobe	7
Android	6
D-Link	6
Apache	5
Apple	5
Cisco	5
Fortinet	4

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
November	5	CVE-2024-28987	SolarWinds	Web Help Desk
November	5	CVE-2024-30088	Microsoft	Windows
November	5	CVE-2024-9680	Mozilla	Firefox
November	7	CVE-2024-40711	Veeam	Backup & Replication
November	11	CVE-2024-9537	ScienceLogic	SL1
November	12	CVE-2024-38094	Microsoft	SharePoint
November	13	CVE-2024-47575	Fortinet	FortiManager
November	14	CVE-2024-20481	Cisco	Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)
November	14	CVE-2024-37383	Roundcube	Webmail
November	25	CVE-2024-8956	PTZOptics	PT30X-SDI/NDI Cameras
November	25	CVE-2024-8957	PTZOptics	PT30X-SDI/NDI Cameras
November	28	CVE-2019-16278	Nostromo	nhttpd
November	28	CVE-2024-43093	Android	Framework
November	28	CVE-2024-51567	CyberPersons	CyberPanel
November	28	CVE-2024-5910	Palo Alto Networks	Expedition

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

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)**.

Flexera's Software Vulnerability Management (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 **Secunia Software Vulnerability Research (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

More than 50,000 customers subscribe to Flexera's technology value optimization solutions, delivered by 2,000+ team members worldwide. Learn more at **flexera.com**