

MONTHLY VULNERABILITY INSIGHTS

Based on Data from Secunia Research

MARCH 2024

flexera™

Author: Jeroen Braak

Inhoud

Introduction	3
<i>Secunia Research software vulnerability tracking process</i>	3
<i>The anatomy of a Security Advisory</i>	3
<i>Summary</i>	4
Year-to-date overview	5
Monthly data	6
<i>Vulnerability information</i>	6
Advisories by attack vector	6
Advisories by criticality	6
Advisories per day	7
<i>Rejected advisories.</i>	8
<i>Addressing awareness with vulnerability insights</i>	9
<i>Vendor view</i>	10
Top vendors with the most advisories	10
Top vendors with zero-day	11
Top Vendors with highest average threat score	11
<i>Browser-related advisories</i>	12
Advisories per browser	12
Browser zero-day vulnerabilities	12
Average CVSS (criticality) score per browser	12
Average threat score per browser	12
What's the Attack Vector?	12
Networking related advisories	13
<i>Threat intelligence</i>	14
Count of malware-exploited CVEs	14
Count of advisories by CVE threat score	14
Threat intelligence advisory statistics:	14
Patching	15
<i>Vulnerabilities that are vendor patched</i>	15
<i>Flexera's Vendor Patch Module (VPM) statistics</i>	15
<i>This month's top vendor patches</i>	15
Other sources	16
<i>CISA</i>	16
This months' the additions to the KEV catalog	16
Due Date this month	17
More information	18

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: **1,073** ↑ (last month: **992**)

Another **record-breaking month** (and quarter) with the highest advisory count in the history of Secunia Research (since 2002) and a record breaking Q1 with a whopping 44% increase compared to last years Q1.

NVD Challenges: Ensuring Unwavering Vulnerability Intelligence with Flexera's Software Vulnerability Research

The biggest news are the ongoing issues at **NVD**, where the entire vulnerability community is seriously concerned about the potential delays in vulnerability analysis efforts.

While it's unclear on the exact reasons on what's cooking at NVD, we are positive that NIST will bounce back strongly. However, the gap between enriched and pending analysis is simply increasing by the day. After doing some rough math, we noticed that over 40% of vulnerabilities from the beginning of 2024 are pending enrichment from NVD.

Having said that Flexera's Software Vulnerability Research (Secunia Research), is completely unperturbed with these delays from NVD. We recognize the importance of timely and accurate vulnerability intelligence for our customers. We understand that delays in analysis efforts can impact decision-making and cybersecurity strategies. However, we want to assure our clients that our solution remains unaffected by these challenges.

Since our inception in 2002, Flexera's SVR has been committed to providing the most accurate and reliable source of vulnerability intelligence. Our dedication to excellence has enabled us to build a reputation for delivering unparalleled insights into the vulnerabilities of software applications. Unlike some solutions that rely solely on NVD for vulnerability data, Software Vulnerability Research utilizes a diverse range of data sources to ensure comprehensive coverage and independence from any single provider. In addition to NVD, we leverage vendor information, community data, threat feeds, dark web sources, and our own dedicated research team to gather intelligence on vulnerabilities across more than 70,000 products.

Linux Kernel Vulnerability Trends

A notable (ongoing) trend that our Research Team has detected is that there is a high increase of **Linux Kernel** vulnerabilities. There are some concerns about this increase:

- Many of these "vulnerabilities" are not really vulnerabilities and descriptions are "fuzzy" at best. (see rejections)
- It seems like "spring cleaning" where they issue CVEs for ager-old GIT commit fixes.
- Or worst, users are "forced" to adapt to Kernel version updates instead of picking GIT Commits.

The result is a high workload on not only vulnerability researchers around the world, but also organizations having Linux assets.

Important conclusions from this month report are:

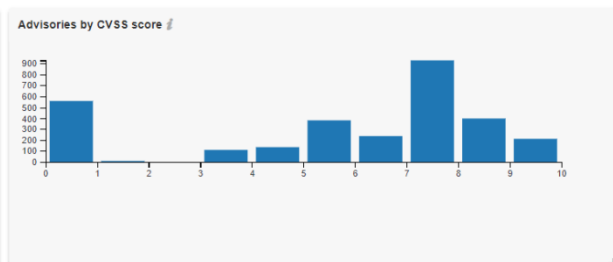
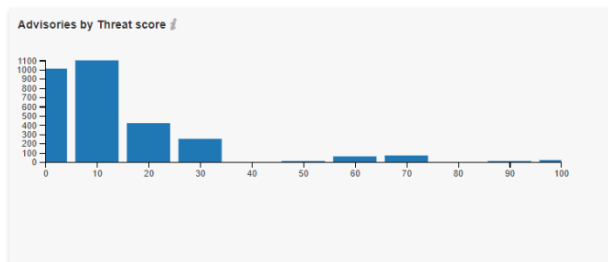
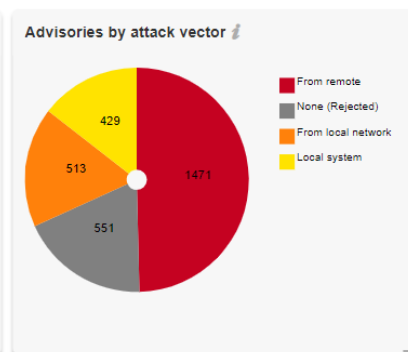
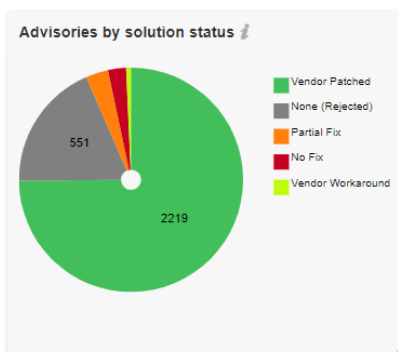
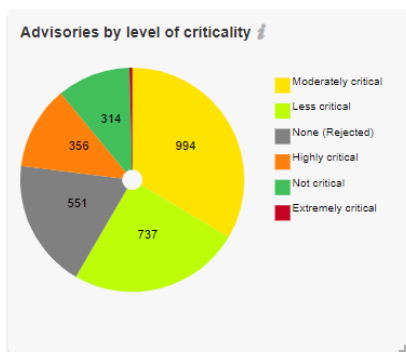
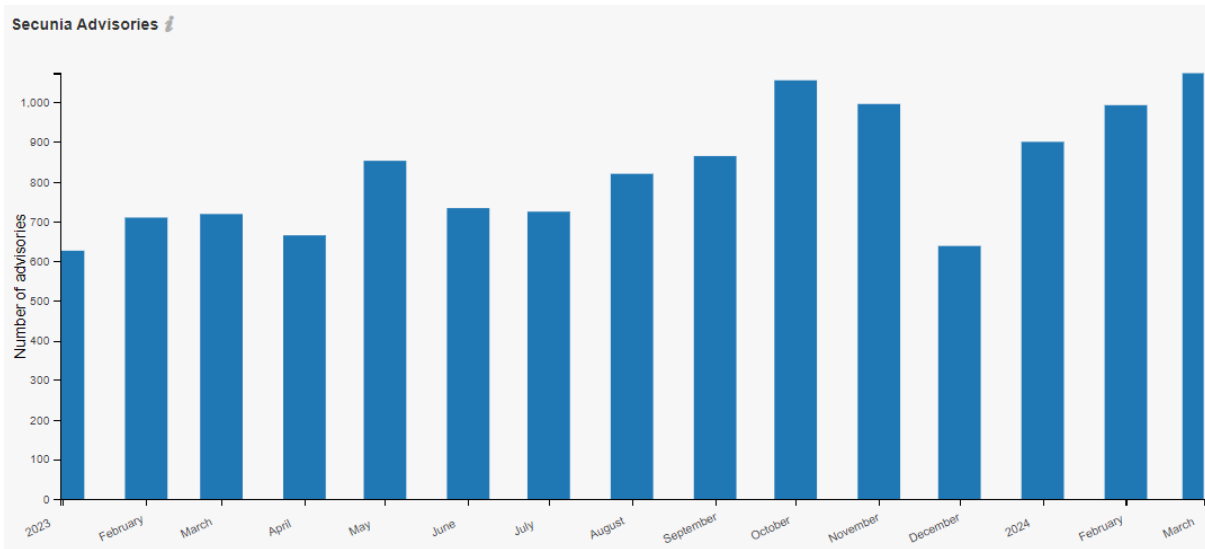
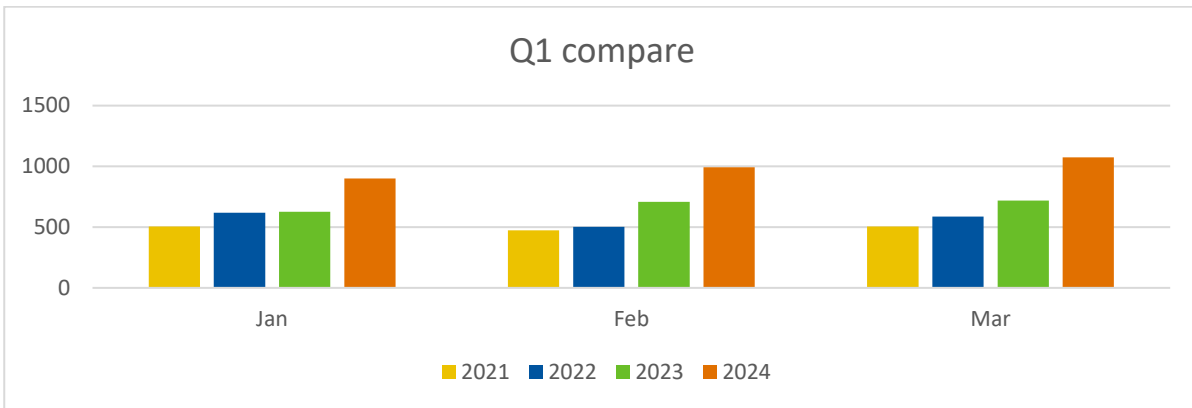
- **A new record with 1,073 advisories**, breaking the record of October '23 (1,055 advisories)
- Last 3 months we've seen a serious increase in the number of advisories: **+ 44%**
- Less than half (**43.8%**) of all vulnerabilities reported in this month have a "**Remote Attack Vector**" (last month **49.29%**)
- The Secunia Research Team reported **2 Extremely** critical advisory this month. (Last month: **1**)
- **7 Zero-Day** Advisories reported. (last month :5) for mostly **Apple (5), Microsoft (1) and Tukaani Project XZ Utils (1)**
- Threat Intelligence indicates again that **Moderately Critical Vulnerabilities** are targeted by hackers.
- This month **110** advisories contain at least one vulnerability linked to a **Recent Cyber Exploit** and **402** advisories contained at least one vulnerability linked to a **Historical Cyber Exploit**.
- More than **half** of all advisories are disclosed by these 3 usual (Linux) suspect vendors (**SUSE, Linux, Red Hat**)
- Interestingly among these vendors are also the ones with the most **rejected advisories**:
 - **Record breaking: Linux Foundation:** 176 out of 276 advisories were rejected by the Secunia Research Team.
- **Cisco** contributed to more than half of all Networking related Advisories this month with **25 advisories**.

Last month we reported that **66.53%** of all Secunia Advisories had a **Threat** (exploits, malware, ransomware, etc.) associated with them, **this month** the number has been **lower again for at least 2 months in a row to 53.59%**

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

Year-to-date overview

As of **March 31, 2024**, the year-to-date total is at **2,964** Advisories **↑** which is **44%** higher than 2023: **2,054** YTD Advisories)



Monthly data

This month, a total of **1,073** ↑ (last month: **992**) advisories were reported by the Secunia Research Team.

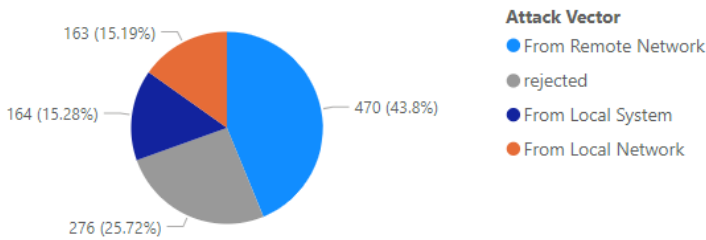
This month:	#	Change (last month):
Total # of advisories	1,073	↑ (992)
Unique Vendors	93	↔ (93)
Unique Products	368	↓ (438)
Unique Versions	480	↓ (508)
Rejected Advisories *	276	↑ (141)
Total Unique CVE ID's reported	1,810	↓ (2,024)

↑ increased ↓ lower ↔ same

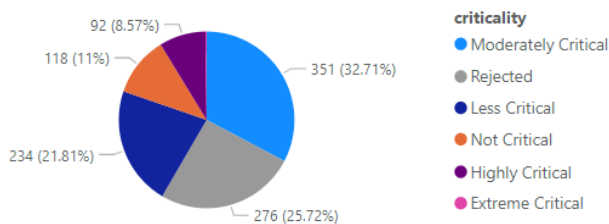
* **276** advisories have received the “rejected” status which means in general that leveraging it would require one or more violations of security best practices (e.g., product not securely configured or not used securely) or that it was “too weak of a gain” (e.g., administrative, local users already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

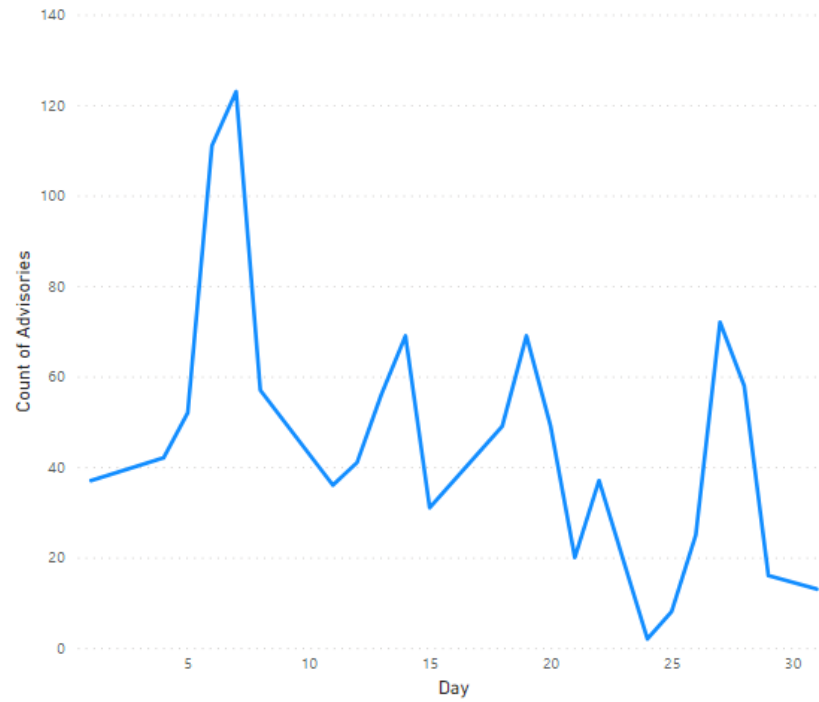


Advisories per day

Below an overview of the daily advisory count.

Year	Month	Day	# of Advisories
2024	March	1	37
2024	March	4	42
2024	March	5	52
2024	March	6	111
2024	March	7	123
2024	March	8	57
2024	March	11	36
2024	March	12	41
2024	March	13	56
2024	March	14	69
2024	March	15	31
2024	March	18	49
2024	March	19	69
2024	March	20	49
2024	March	21	20
2024	March	22	37
2024	March	24	2
2024	March	25	8
2024	March	26	25
2024	March	27	72
2024	March	28	58
2024	March	29	16
2024	March	31	13
Total			1073

Count of Advisories by Day



Rejected advisories.

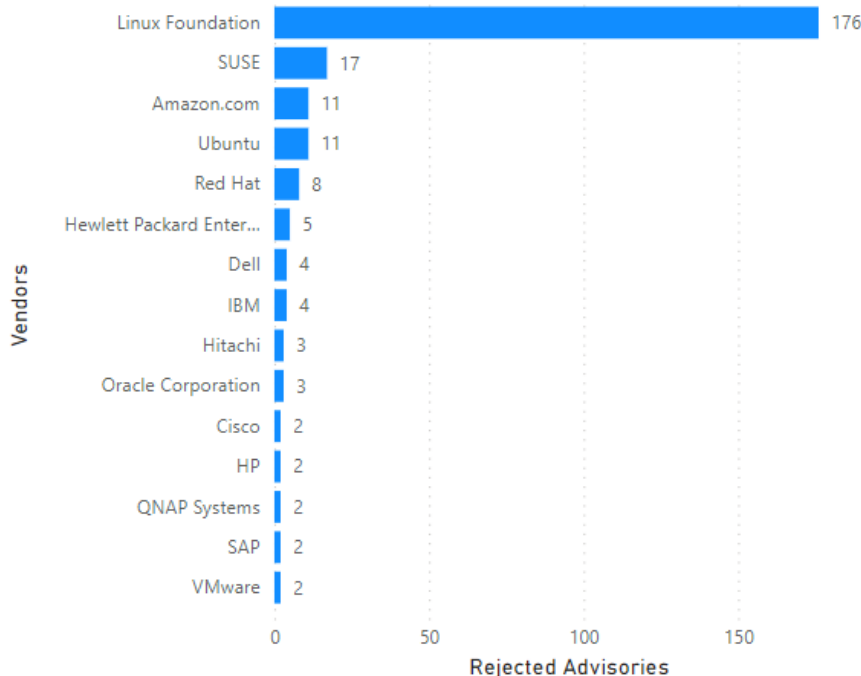
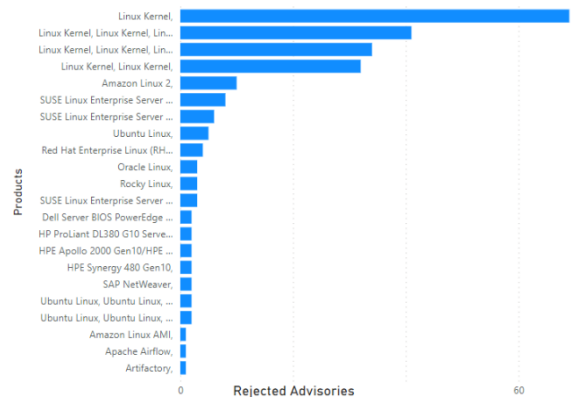
There are many vulnerabilities posted to the National Vulnerability Database (NVD) by a lot of people and companies. They are not always valid, assigned a proper criticality, and in some cases, a vulnerability may be legitimate but not afford the attacker any benefit.



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.



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.

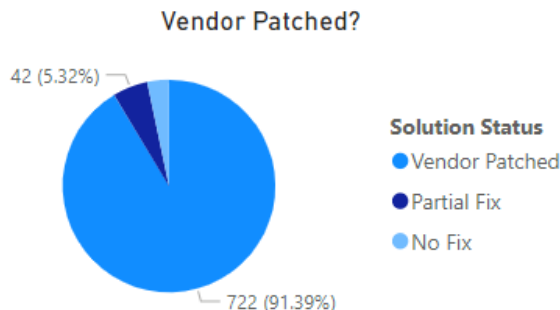
criticality	avg threat score x # of advisories
Moderately Critical	4,716.00
Less Critical	2,493.00
Highly Critical	1,752.00
Not Critical	286.00
Extreme Critical	0.00
Total	9,247.00

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.

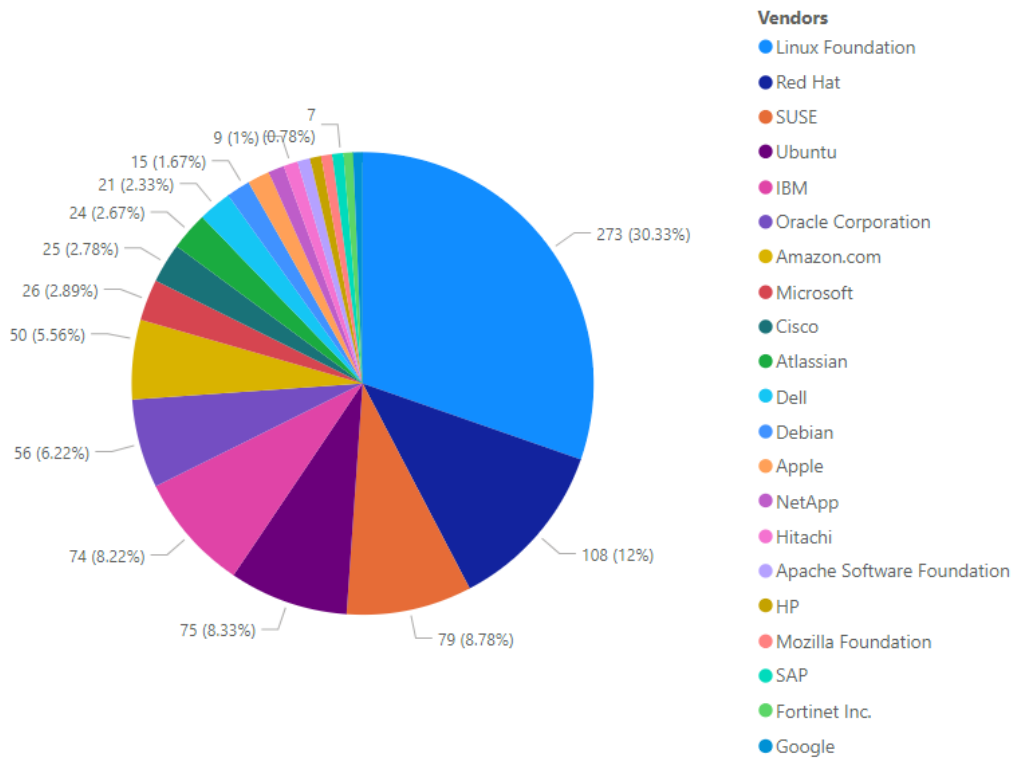
Take away 2:

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)*

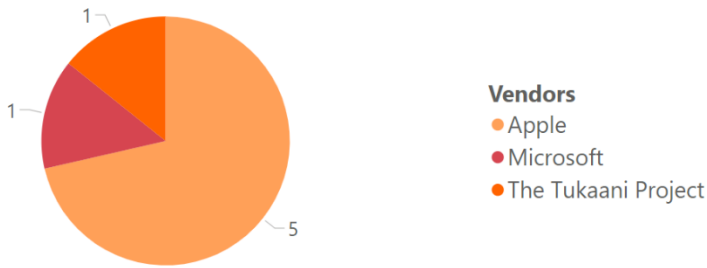


Vendor view

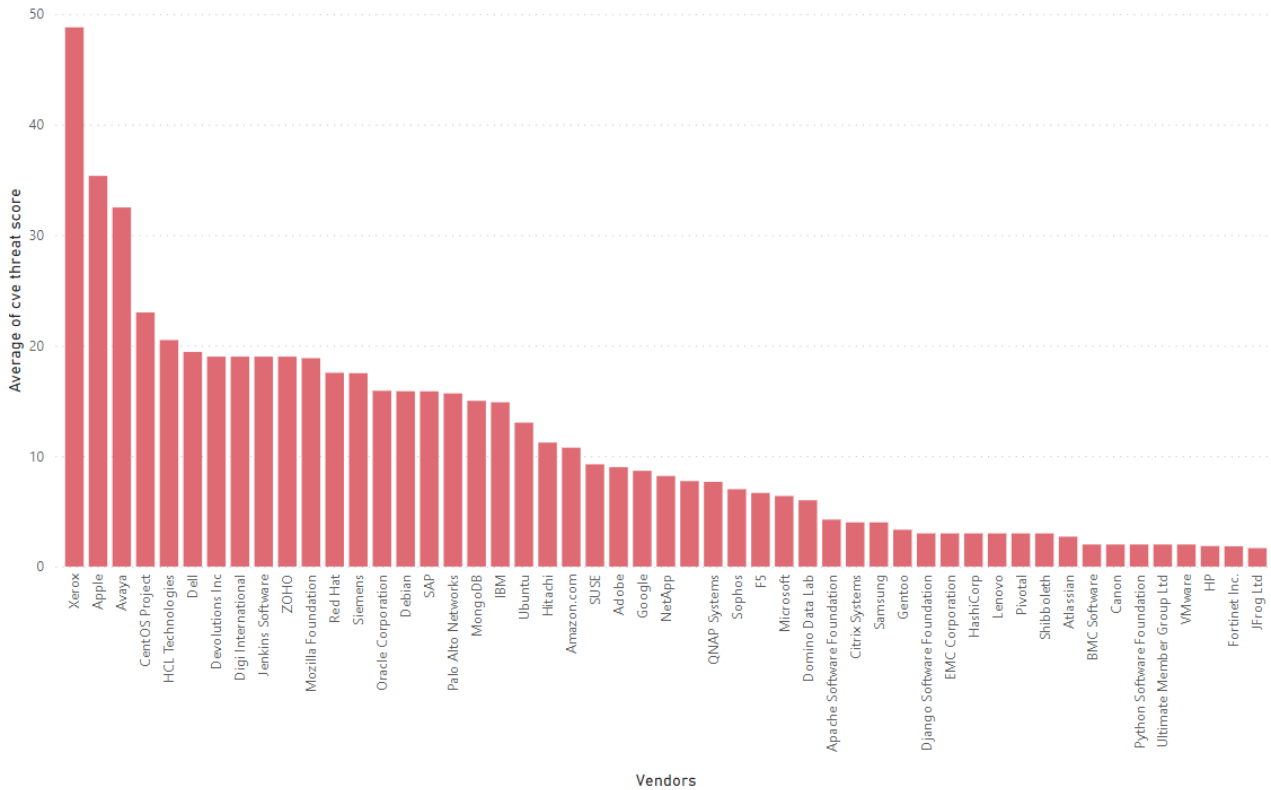
Top vendors with the most advisories



Top vendors with zero-day

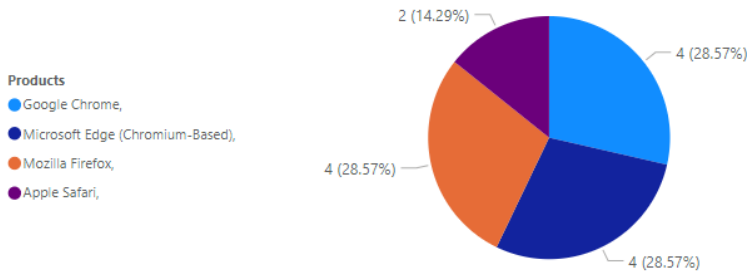


Top Vendors with highest average threat score



Browser-related advisories

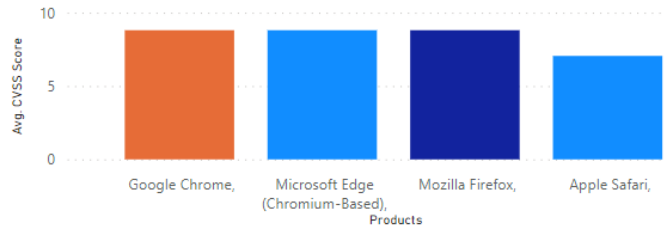
Advisories per browser



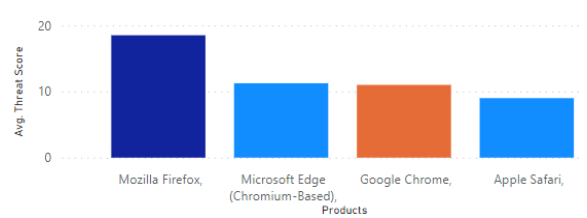
Browser zero-day vulnerabilities

Count of Advisories	Products	Advisories
1	Microsoft Edge (Chromium-Based),	SA125595
1		

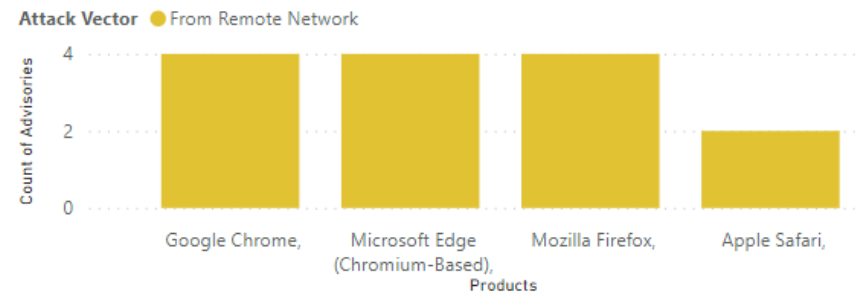
Average CVSS (criticality) score per browser



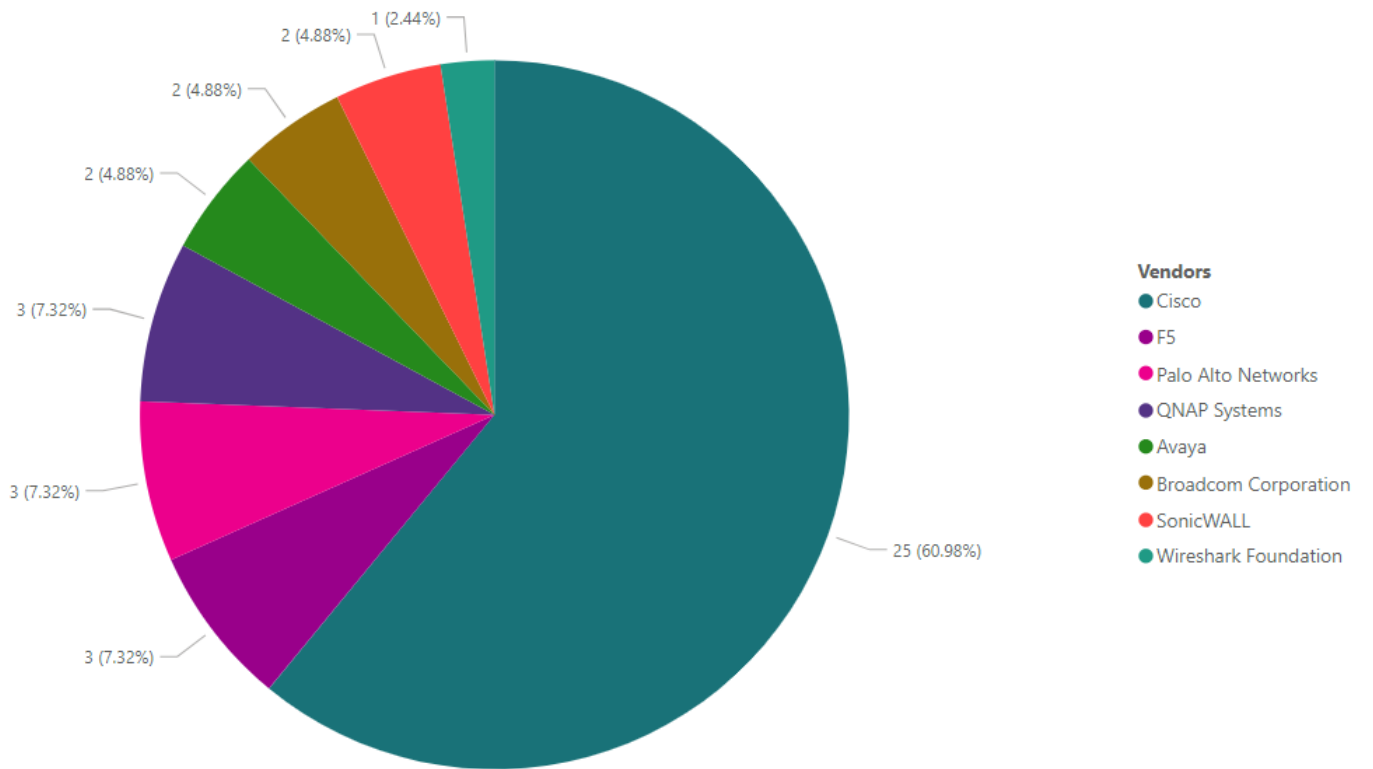
Average threat score per browser



What's the Attack Vector?



Networking related advisories

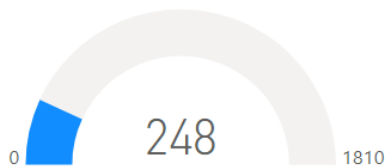


Threat intelligence

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+)	575 ↓ (660)	53.59%
SAIDs with no threat score (=0)	498 ↑ (332)	46.41%

SAID: Secunia Advisory Identifier

Range	# SAIDS	Last month
Medium-range threat score SAIDs (13-23)	289 ↓	(432)
Low-range threat score SAIDs (1-12)	248 ↑	(169)
Critical-range threat score SAIDs (45-70)	25 ↓	(34)
Very critical threat score SAIDs (71-99)	9 ↓	(21)
High-range threat score SAIDs (24-44)	4 =	(4)

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

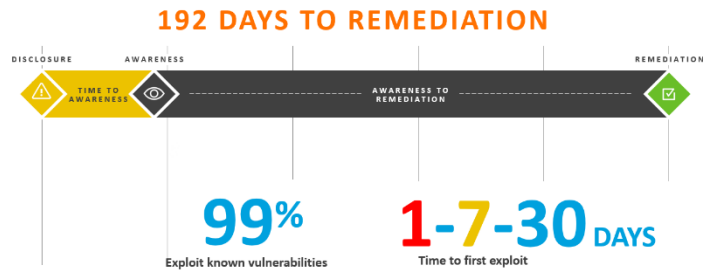
- [Evidence of exploitation](#)
- [Criteria for the threat Score Calculation](#)
- [Threat Score Calculation - Examples](#)

Patching

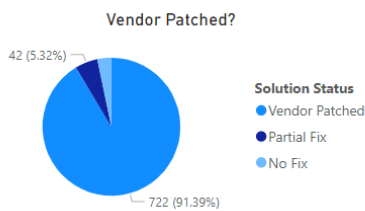
Most of this month's vulnerabilities are vendor patched. In fact, most vulnerabilities are patched within 24 hours after disclosure.

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

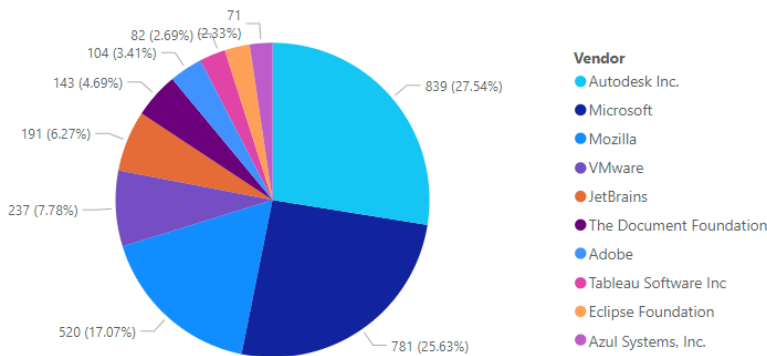
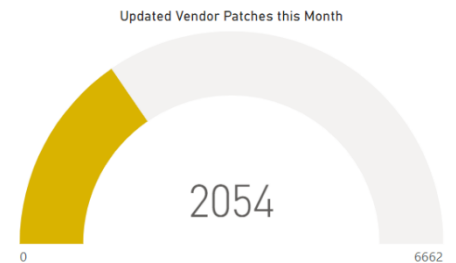


Flexera's Vendor Patch Module (VPM) statistics

Flexera has the largest third-party patch catalog (**More than 6,400**) 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 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 additions to the KEV catalog

First column "Day" is the day of this month that the CVE was added to KEV Catalog.

Day	CVE	Vendor	Product	Month	Day
4	CVE-2024-21338	Microsoft	Windows	March	25
5	CVE-2021-36380	Sunhillo	SureLine	March	26
5	CVE-2023-21237	Android	Pixel	March	26
6	CVE-2024-23225	Apple	Multiple Products	March	27
6	CVE-2024-23296	Apple	Multiple Products	March	27
7	CVE-2024-27198	JetBrains	TeamCity	March	28
25	CVE-2019-7256	Nice	Linear eMerge E3-Series	April	15
25	CVE-2021-44529	Ivanti	Endpoint Manager Cloud Service Appliance (EPM CSA)	April	15
25	CVE-2023-48788	Fortinet	FortiClient EMS	April	15
26	CVE-2023-24955	Microsoft	SharePoint Server	April	16

Due Date this month

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

CISA strongly encourages all organizations to do the same:

Month	Day	CVE	Vendor	Product
March	4	CVE-2023-43770	Roundcube	Webmail
March	5	CVE-2024-21351	Microsoft	Windows
March	5	CVE-2024-21412	Microsoft	Windows
March	7	CVE-2020-3259	Cisco	Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)
March	7	CVE-2024-21410	Microsoft	Exchange Server
March	21	CVE-2023-29360	Microsoft	Streaming Service
March	25	CVE-2024-21338	Microsoft	Windows
March	26	CVE-2021-36380	Sunhillo	SureLine
March	26	CVE-2023-21237	Android	Pixel
March	27	CVE-2024-23225	Apple	Multiple Products
March	27	CVE-2024-23296	Apple	Multiple Products
March	28	CVE-2024-27198	JetBrains	TeamCity

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 delivers SaaS-based IT management solutions that enable enterprises to accelerate digital transformation and multiply the value of their technology investments. We help organizations inform their IT with unparalleled visibility into complex hybrid ecosystems. And we help them transform their IT with tools that deliver the actionable intelligence to effectively manage, govern and optimize their hybrid IT estate.

More than 50,000 customers subscribe to our technology value optimization solutions, delivered by 1,300+ passionate team members worldwide. To learn more, visit flexera.com