MONTHLY VULNERABILITY INSIGHTS

Based on Data from Secunia Research

APRIL 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: **1,010** ↓ (last month: **1073**)

Important conclusions from this month report are:

- **April has become the third month with more than 1,000 advisories (third highest in history)**
- Since the start of 2024 we've seen a serious increase in the number of advisories: **+ 46%**
- Less than half (**48.91%**) of all vulnerabilities reported in this month have a "Remote Attack Vector" (last month **43.8%**)
- The Secunia Research Team reported **2 Extremely** critical advisory this month. (Last month: **2**)
- **2 Zero-Day** Advisories reported. (last month :7) for **Cisco (ASA and FTD)** and **Palo Alto Networks (PAN-OS)**
- Threat Intelligence indicates again that **Moderately Critical Vulnerabilities** are targeted by hackers.
- This month **132 (*last month:110*)** advisories contain at least one vulnerability linked to a **Recent Cyber Exploit** and **412** (***last month: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**:
    - **Linux, RedHat and SUSE** reported **141 out of 203** advisories were rejected by the Secunia Research Team.
- **Juniper (45%) and Cisco (18%)** contributed to more than half of all Networking related Advisories this month with **38 advisories.**

Last month we reported that **53.59%** of all Secunia Advisories had a **Threat** (exploits, malware, ransomware, etc.) associated with them, **this month** the number has been **HIGHER to 62.97%**

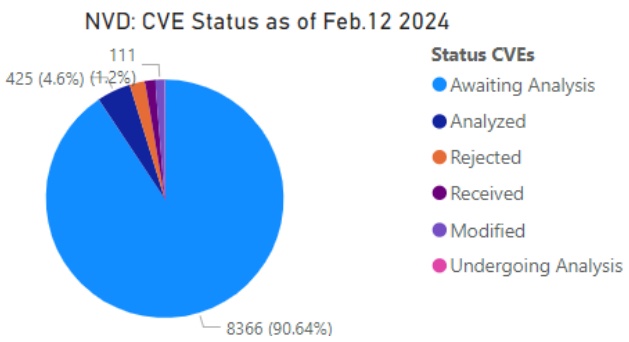
Using Threat Intelligence is going to help you with prioritizing what needs to be **patched** immediately.

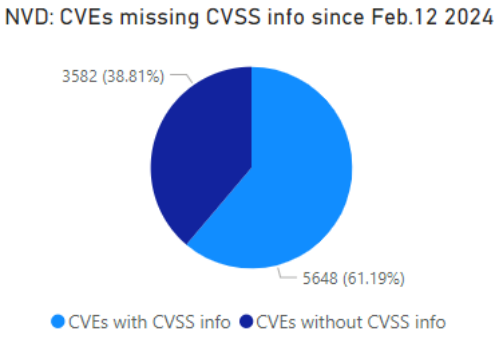
NVD Challenges:

Currently more than 8,000 CVEs are awaiting analysis!

Issues at **NVD** are still ongoing, where the entire vulnerability community is seriously concerned about the potential delays in vulnerability analysis efforts. (Latest news: https://nvd.nist.gov/general/news/nvd-program-transition-announcement)

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.



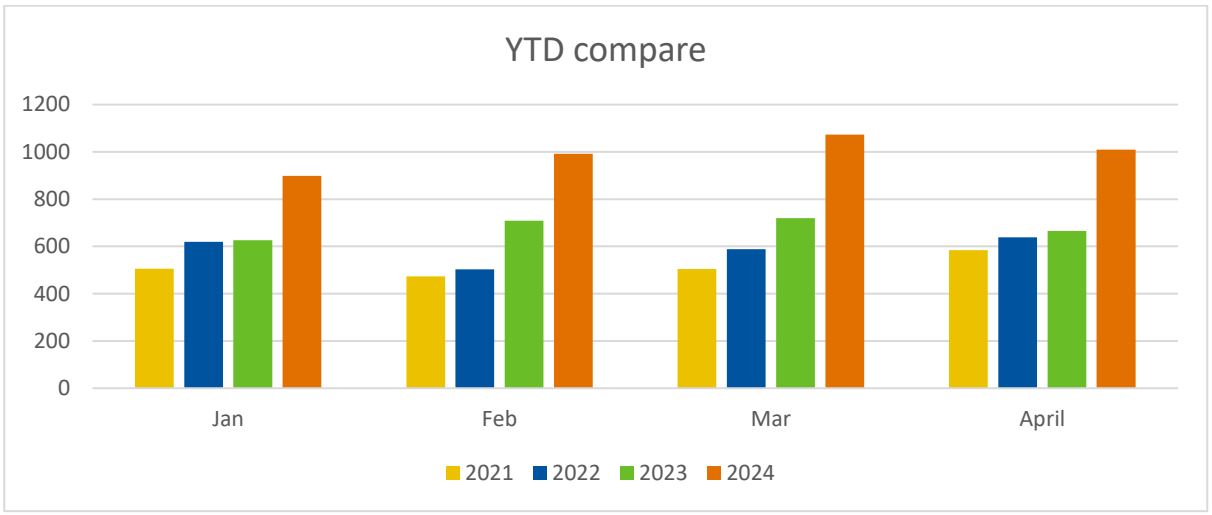


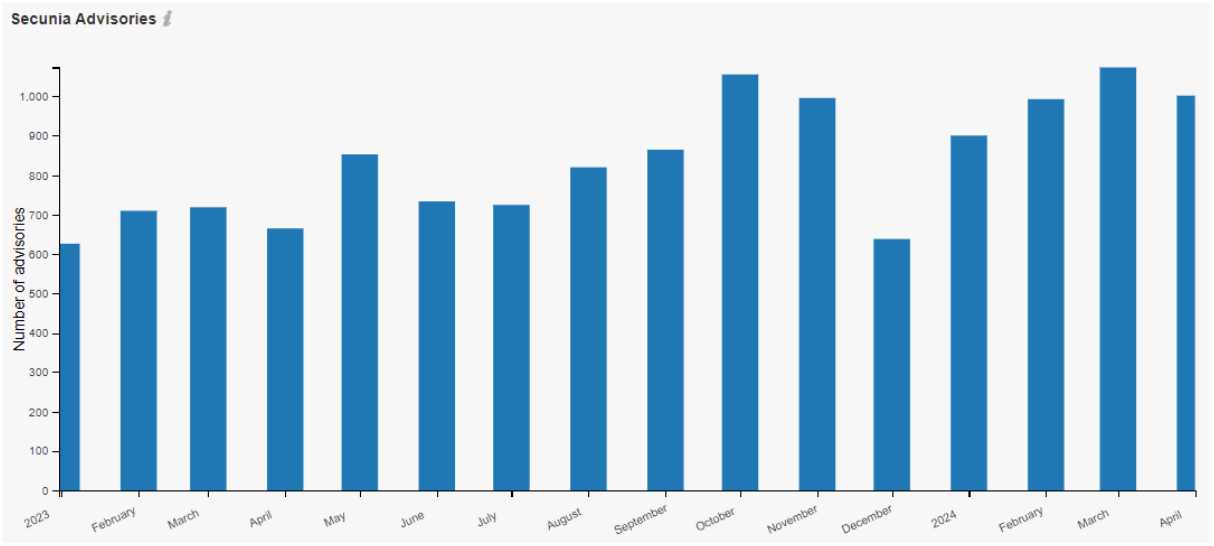
(data from Feb.12 - May 1 , 2024)

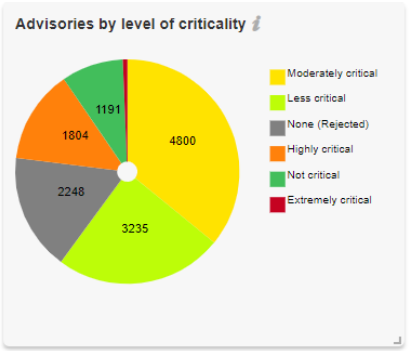
Having said that Flexera's Software Vulnerability Research (Secunia Research), is completely unperturbed with these delays from NVD. We recognize the importance of timely and accurate vulnerability intelligence for our customers. We understand that delays in analysis efforts can impact decision-making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

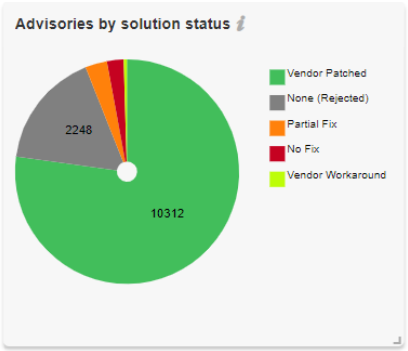
Year-to-date overview

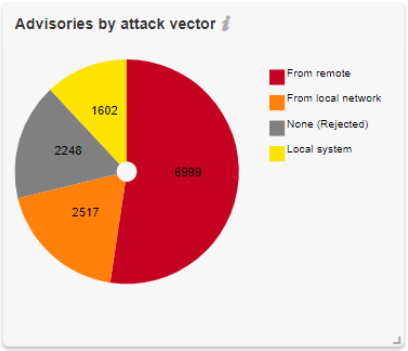
As of **April 30, 2024**, the year-to-date total is at **3,974** Advisories ↑ which is **46%** higher than 2023: **2,720** YTD Advisories)











Monthly data

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

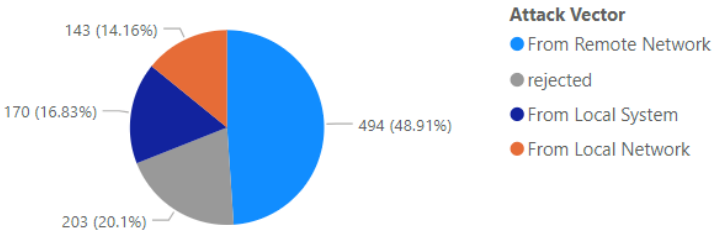
This month:	#	Change *(last month):*
Total # of advisories	**1,010**	↓ *(**1,073**)*
Unique Vendors	**86**	↓ *(**93**)*
Unique Products	**394**	↑ **(368***)*
Unique Versions	**488**	↑ *(**480**)*
Rejected Advisories *	**203**	↓ *(**276**)*
NEW Advisories without CVE ID	**13**	↓ *(**24**)*
Advisories with Threat Score (>0)	**635**	↑ **(575)**
Total Unique CVE ID's reported	**1,762**	↓ **(1,810)**

↑ increased ↓lower ↔ same

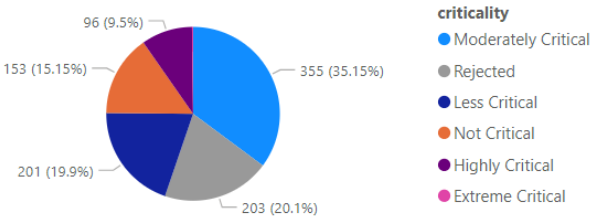
** **203** advisories have received the "rejected" status which means in general that leveraging it would require one or more violations of security best practices (e.g., product not securely configured or not used securely) or that it was "too weak of a gain" (e.g., administrative, local users already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



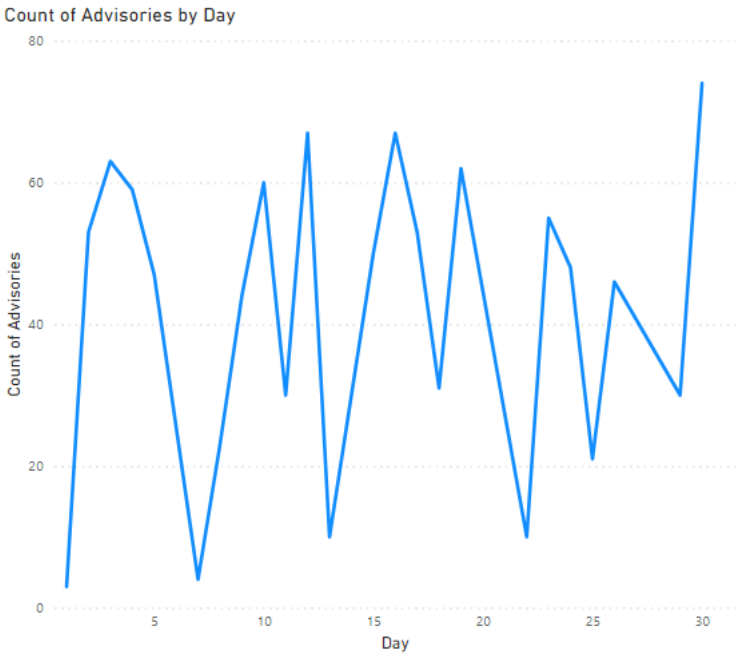
Advisories by criticality



Advisories per day

Below an overview of the daily advisory count.

Year	Month	Day	# of Advisories
2024	April	1	3
2024	April	2	53
2024	April	3	63
2024	April	4	59
2024	April	5	47
2024	April	7	4
2024	April	8	23
2024	April	9	44
2024	April	10	60
2024	April	11	30
2024	April	12	67
2024	April	13	10
2024	April	15	50
2024	April	16	67
2024	April	17	53
2024	April	18	31
2024	April	19	62
2024	April	22	10
2024	April	23	55
2024	April	24	48
2024	April	25	21
2024	April	26	46
2024	April	29	30
2024	April	30	74
Total			**1010**



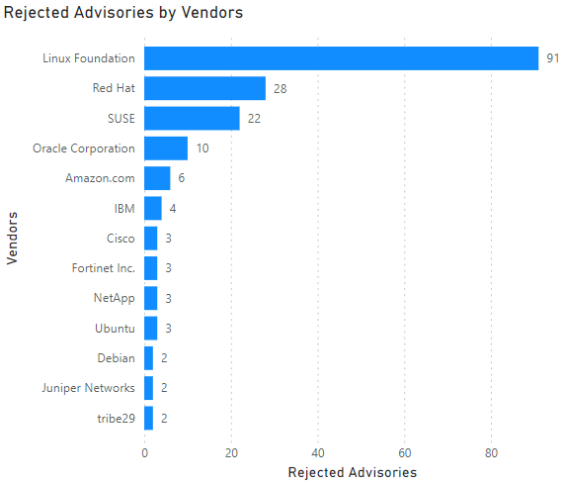
Rejected advisories.

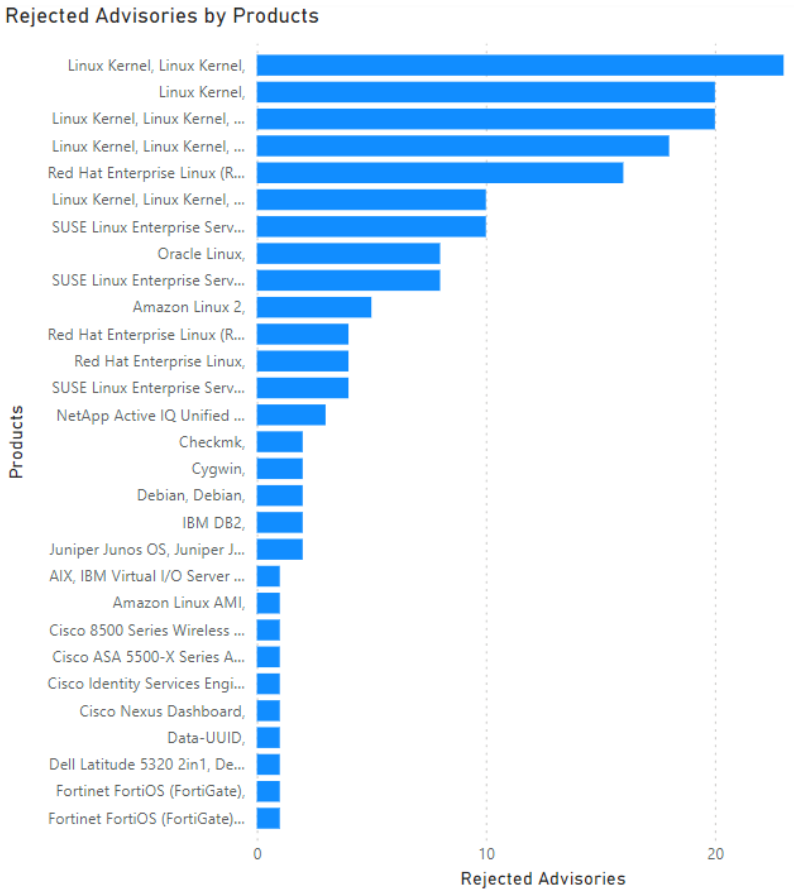
There are many vulnerabilities posted to the National Vulnerability Database (NVD) by a lot of people and companies. They are not always valid, assigned a proper criticality, and in some cases, a vulnerability may be legitimate but not afford the attacker any benefit.

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:

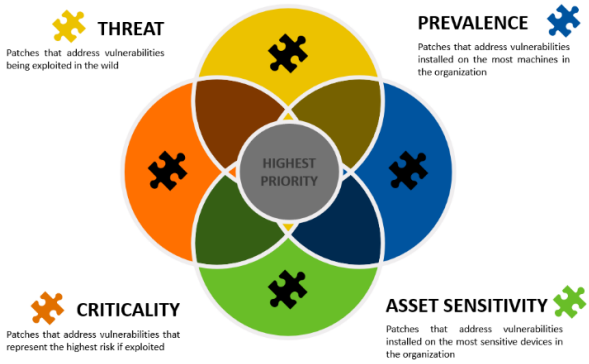
- What systems would result in the most risk if compromised?
- Is it a high-risk device? **Patch**.

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.

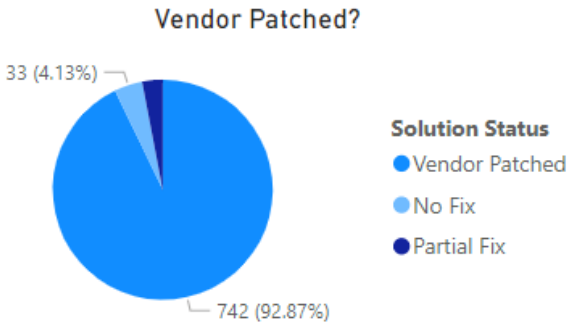
criticality	avg threat score x # of advisories
Moderately Critical	5,828.00
Less Critical	5,001.00
Highly Critical	2,628.00
Not Critical	992.00
Extreme Critical	184.00
Total	**14,633.00**

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.

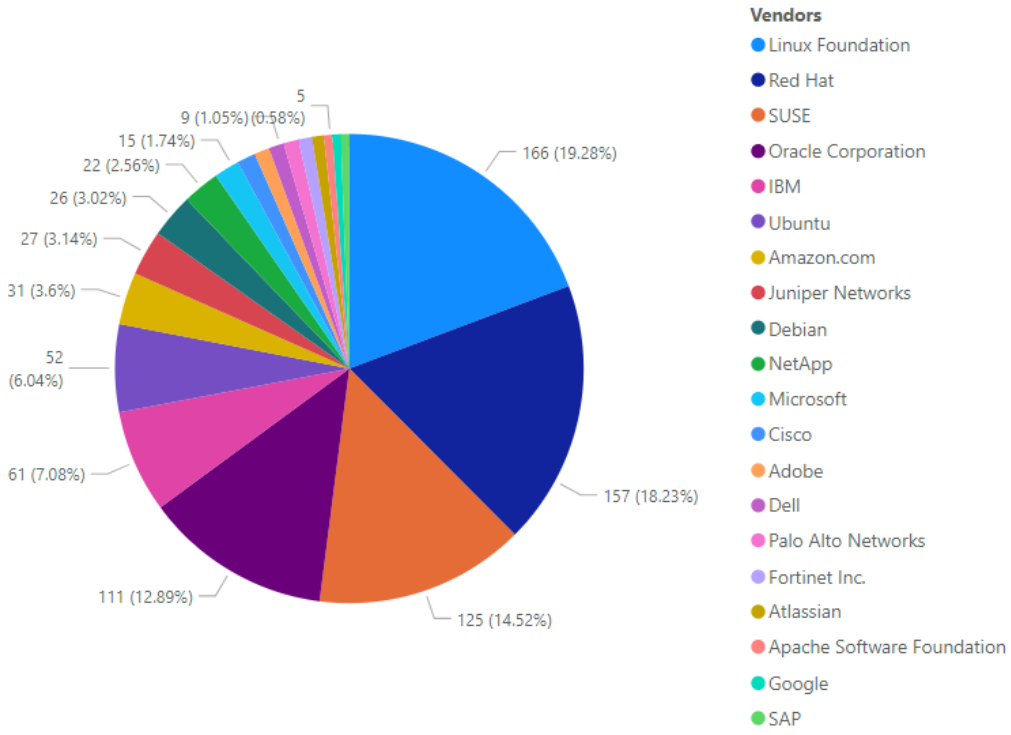
Take away 2:

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)



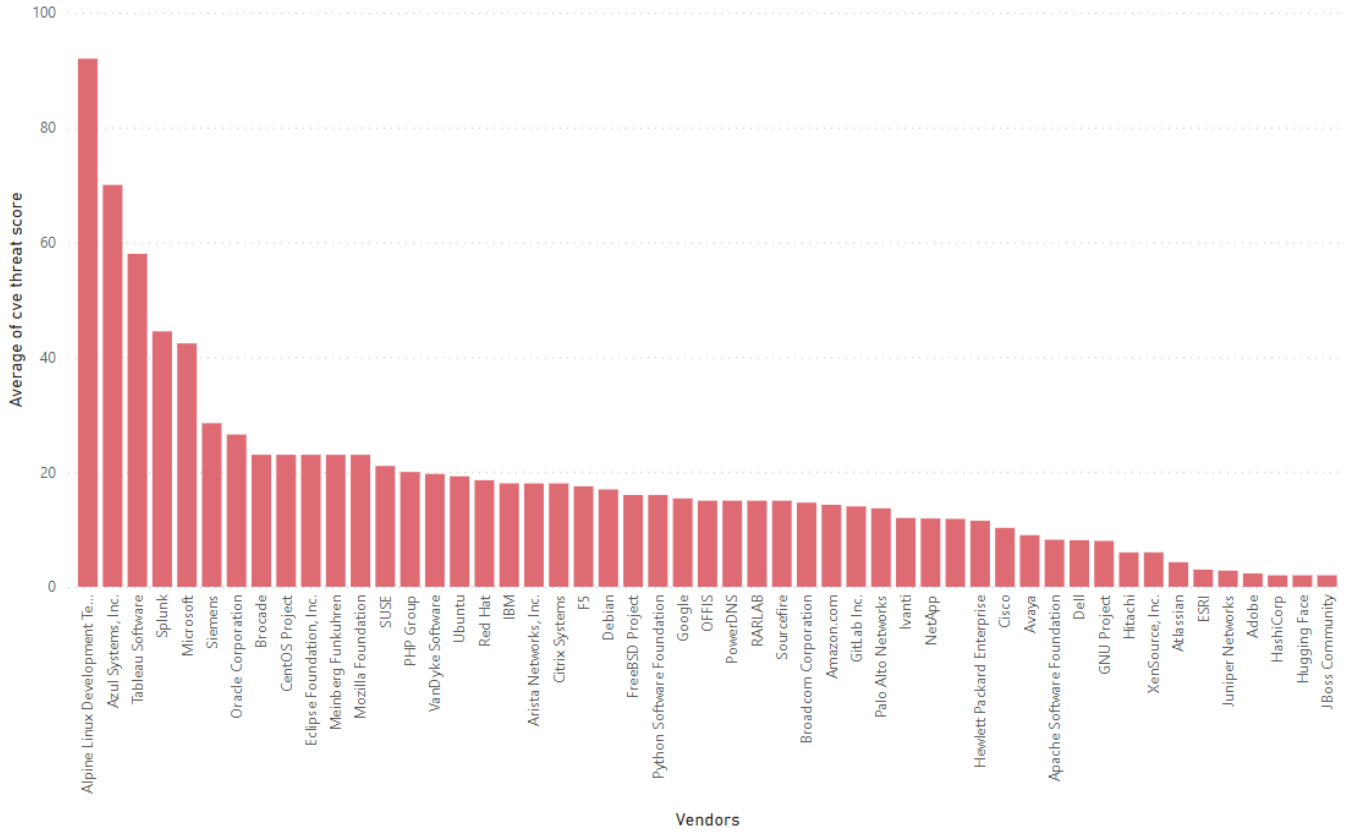
Vendor view

Top vendors with the most advisories



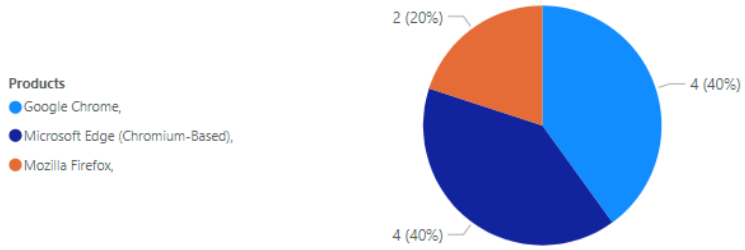
Top vendors with zero-day

Top Vendors with highest average threat score



Browser-related advisories

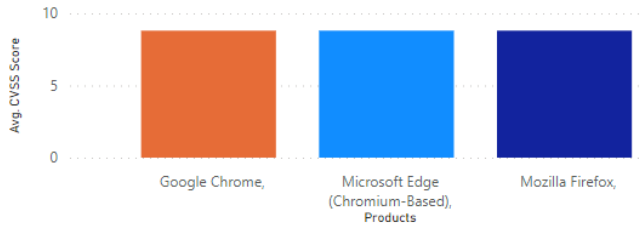
Advisories per browser



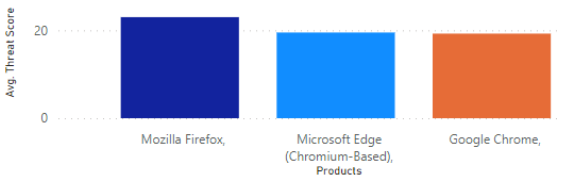
Browser zero-day vulnerabilities

No zero-day vulnerabilities reported this month.

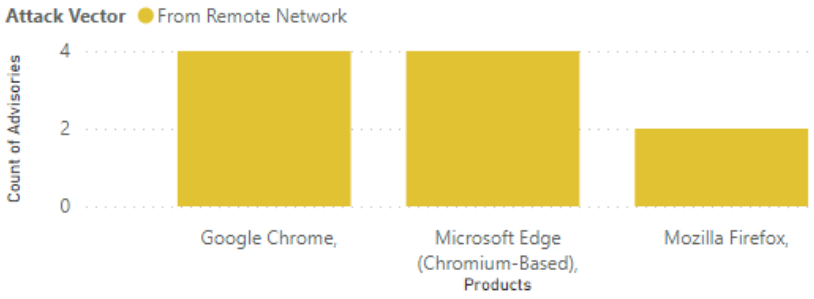
Average CVSS (criticality) score per browser



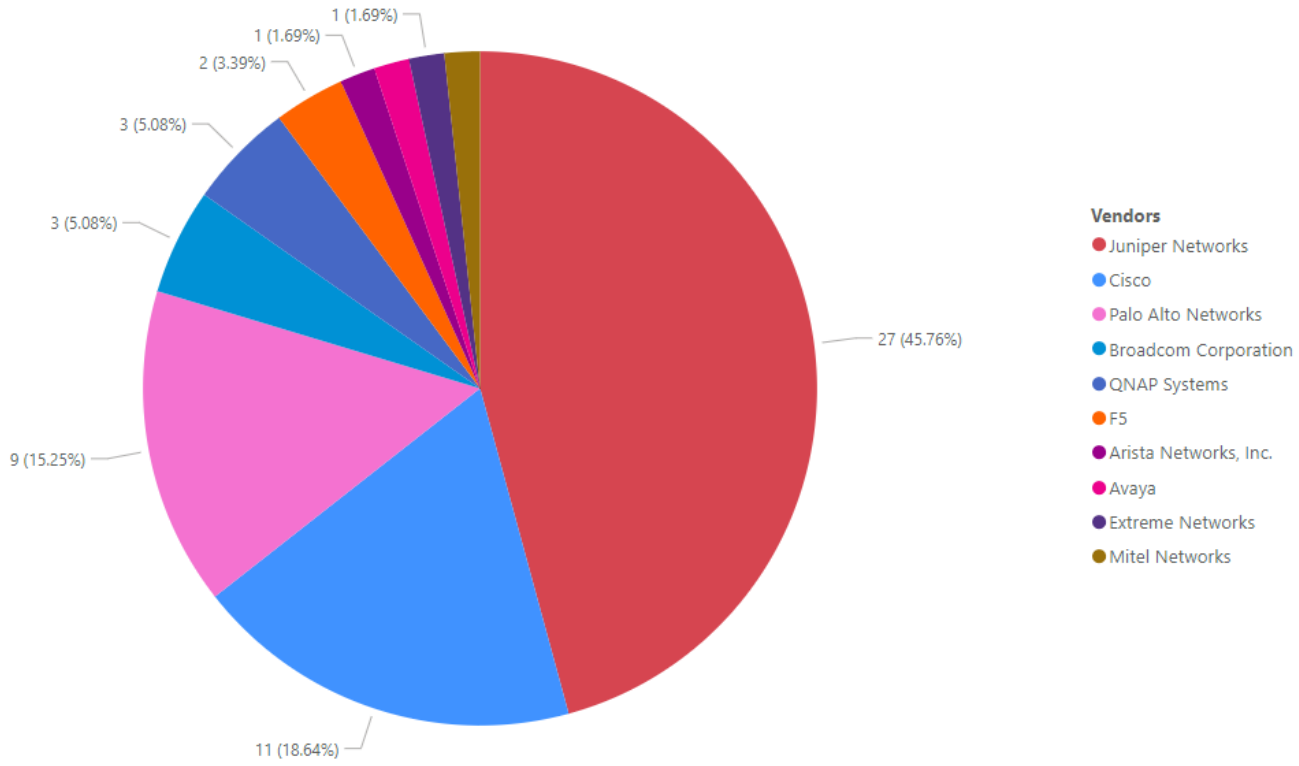
Average threat score per browser



What's the Attack Vector?



Networking related advisories

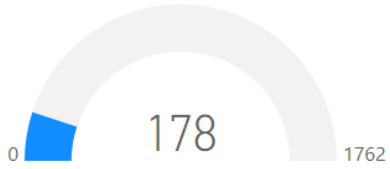


Threat intelligence

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+)	**635** ↓ (575)	62.87%
SAIDs with no threat score (=0)	**375** ↑ (*498*)	37.13%

SAID: Secunia Advisory Identifier

Range	# SAIDS	*Last month*
Medium-range threat score SAIDs (13-23)	**468** ↑	*(289)*
Low-range threat score SAIDs (1-12)	**106** ↓	*(248)*
Very critical threat score SAIDs (71-99)	41 ↑	*(9)*
Critical-range threat score SAIDs (45-70)	20 ↓	*(25)*
High-range threat score SAIDs (24-44)	0 =	*(4)*

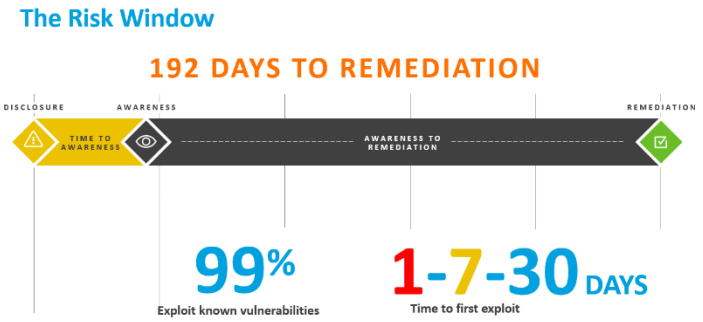
More information about how the Secunia team calculates the threat score:

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

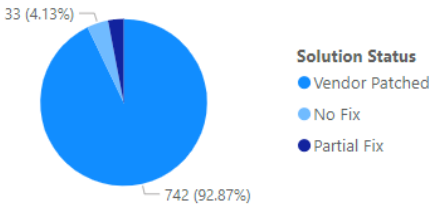
Patching

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).



Vulnerabilities that are vendor patched

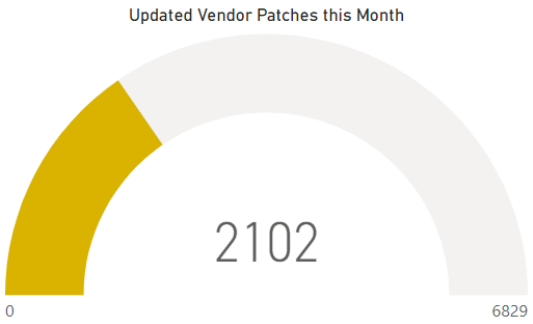


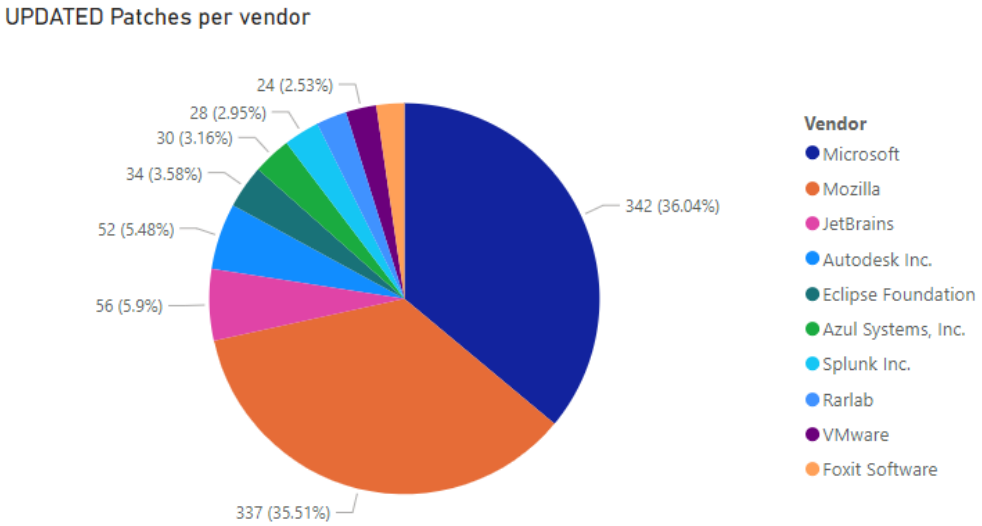
Flexera's Vendor Patch Module (VPM) statistics

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 months' the additions to the KEV catalog

dateAdded	CVE	Vendor	Product	dueDate
Thursday, April 04, 2024	CVE-2024-29745	Android	Pixel	Thursday, April 25, 2024
Thursday, April 04, 2024	CVE-2024-29748	Android	Pixel	Thursday, April 25, 2024
Thursday, April 11, 2024	CVE-2024-3272	D-Link	Multiple NAS Devices	Thursday, May 02, 2024
Thursday, April 11, 2024	CVE-2024-3273	D-Link	Multiple NAS Devices	Thursday, May 02, 2024
Friday, April 12, 2024	CVE-2024-3400	Palo Alto Networks	PAN-OS	Friday, April 19, 2024
Tuesday, April 23, 2024	CVE-2022-38028	Microsoft	Windows	Tuesday, May 14, 2024
Wednesday, April 24, 2024	CVE-2024-20353	Cisco	Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)	Wednesday, May 01, 2024
Wednesday, April 24, 2024	CVE-2024-20359	Cisco	Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)	Wednesday, May 01, 2024
Wednesday, April 24, 2024	CVE-2024-4040	CrushFTP	CrushFTP	Wednesday, May 01, 2024
Tuesday, April 30, 2024	CVE-2024-29988	Microsoft	SmartScreen Prompt	Tuesday, May 21, 2024

Top 10 (YTD) KEV vendors

Vendor	# of CVEs
Microsoft	9
Apple	5
Ivanti	5
Android	3
Cisco	3
D-Link	3
Google	3
Adobe	2
Citrix	2
Fortinet	2

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	15	CVE-2019-7256	Nice	Linear eMerge E3-Series
April	15	CVE-2021-44529	Ivanti	Endpoint Manager Cloud Service Appliance (EPM CSA)
April	15	CVE-2023-48788	Fortinet	FortiClient EMS
April	16	CVE-2023-24955	Microsoft	SharePoint Server
April	19	CVE-2024-3400	Palo Alto Networks	PAN-OS
April	25	CVE-2024-29745	Android	Pixel
April	25	CVE-2024-29748	Android	Pixel

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 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