MONTHLY VULNERABILITY INSIGHTS

Based on Data from Secunia Research

SEPTEMBER 2023

flexera™

Author: Jeroen Braak

Contents

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: **864** ↑ (last month: **821**).

Important **conclusions** from this month report are:

- Again a record breaking month, with **864** advisories being reported this month (May'23 : **856**)
- 2022 was already the record-breaking year with the highest number of Secunia Advisories reported, however 2023 is shaping up to destroy that previous record since we are already **28.2%** Year-to-date. (Last month YTD was 24.7%)
- Almost **52.2%** of all vulnerabilities reported in this month have a "**Remote Attack Vector**" (last month 47.99%)
- The Secunia Research Team reported **11 Extremely** critical advisories this month. (Last month: **1**)
- **17 Zero-Day** Advisories reported. (last month :5) **Microsoft, Apple , Google and Adobe**
- Over **1,892 unique** CVE's (last month: **1,491**) were covered in the **864** Advisories.
- Threat Intelligence indicates again that **Highly and Moderately Critical Vulnerabilities** are targeted by hackers.
- More than half of all advisories are disclosed by these 4 usual suspect vendors (**Amazon**,**Suse,Ubuntu**,**RedHat**)
- Interestingly these vendors are also the ones with the most **rejected advisories**: (more than 50%)
    - **Amazon**: 41 out of 131 advisories were rejected by the Secunia Research Team.
    - **Ubuntu** : 13/131
    - **SUSE** : 12/131
    - **RedHat** : 9/131
- **Cisco** contributes to almost 51**%** of all Networking related Advisories this month.

Last month we reported that **70.52%** of all Secunia Advisories had a **Threat** (exploits, malware, ransomware, etc.) associated with them, **this month** the number has been **higher** to **72.11%**

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

Software Vulnerability – and Patch Management is becoming more and more important.
Due to the ongoing global threats, attacks on critical infrastructures in many countries are increasing.
Back in 2019 (just before Covid) patching was recommended within 30 days (or 14 days for CVSS score 7 or higher)
Right now, hackers can deploy exploits **within 1 week** and even within **24 hours** . This means that organizations need to prioritize even better to quickly patch vulnerabilities (especially the ones with threats associated with them)

Noticeable information and/or events this month:

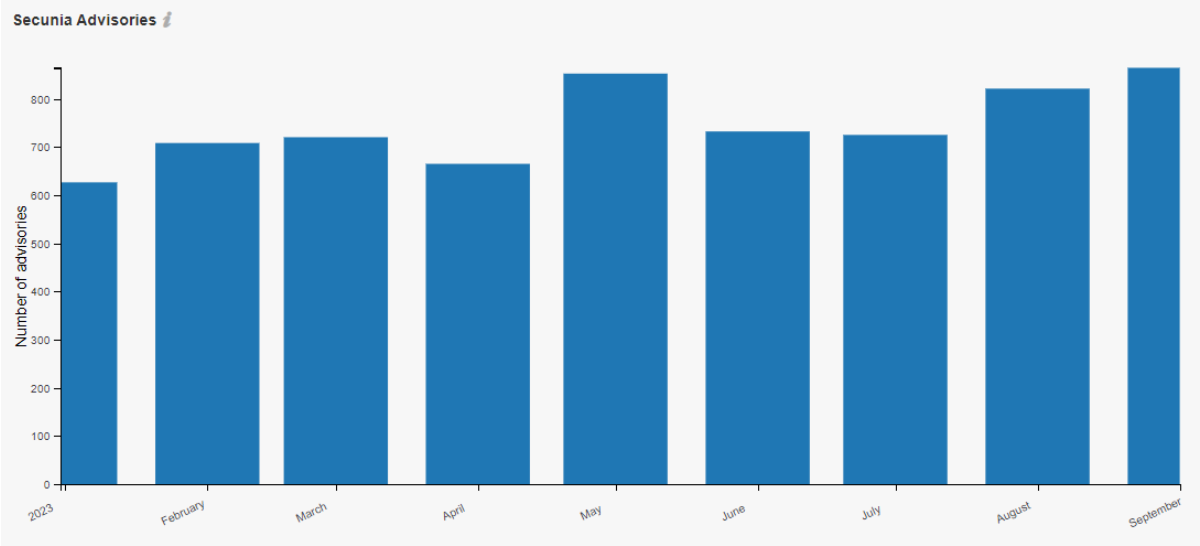
- On Sept. 7 , **Apple** released emergency security updates for iOS, iPadOS, macOS, and watchOS to address two zero-day flaws that have been exploited in the wild to deliver NSO Group's Pegasus mercenary spyware.
- **Google** on Sept. 11 rolled out out-of-band security patches to address a critical security flaw in its Chrome web browser that it said has been exploited in the wild.
- **Adobe's** Patch Tuesday update for September 2023 comes with a patch for a critical actively exploited security flaw in Acrobat and Reader that could permit an attacker to execute malicious code on susceptible systems.
- On Sept. 12, **Mozilla** released security updates to resolve a critical zero-day vulnerability in Firefox and Thunderbird that has been actively exploited in the wild, a day after Google released a fix for the issue in its Chrome browser.
- **Microsoft** has released software fixes to remediate 59 bugs spanning its product portfolio, including two zero-day flaws that have been actively exploited by malicious cyber actors.
- **Apple** has released yet another round of security patches to address three actively exploited zero-day flaws impacting iOS, iPadOS, macOS, watchOS, and Safari, taking the total tally of zero-day bugs discovered in its software this year to **16**.
- On 27 Sept. **Google** rolled out fixes to address a new actively exploited zero-day in the **Chrome** browser. Tracked as CVE-2023-5217

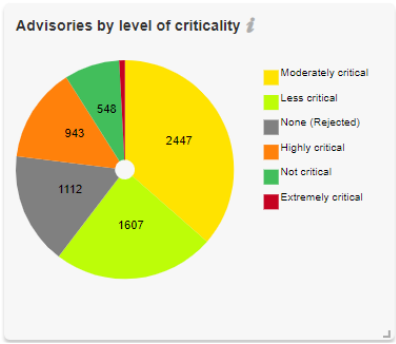
Interesting sources of information:

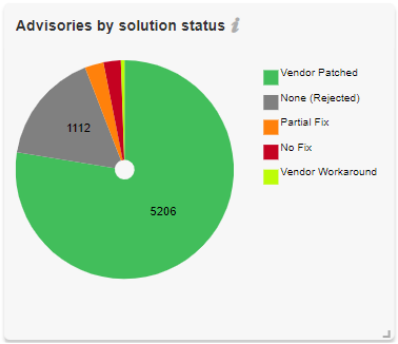
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- https://www.bleepingcomputer.com/news/security/
- https://thehackernews.com/search/label/Vulnerability
- https://www.darkreading.com/vulnerability-management?page=1
- https://portswigger.net/daily-swig/vulnerabilities
- https://www.securityweek.com/virus-threats/vulnerabilities

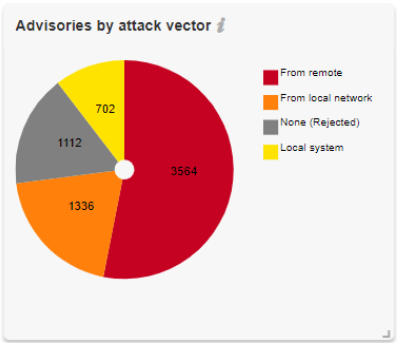
Year-to-date overview

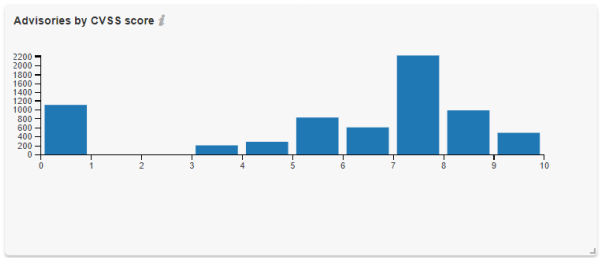
As of **October 1, 2023**, the year-to-date total is at **6,714** Advisories ↑ which is higher than 2022 : **5,236** YTD Advisories)

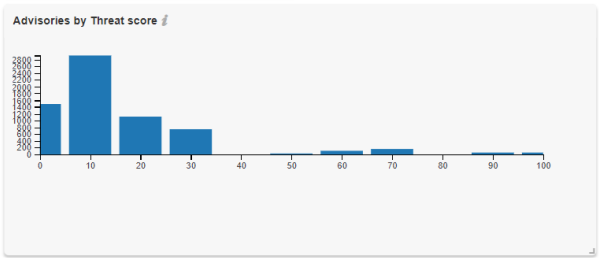












Monthly data

This month, a total of **864** ↑ (last month: **821**) advisories were reported by the Secunia Research Team.

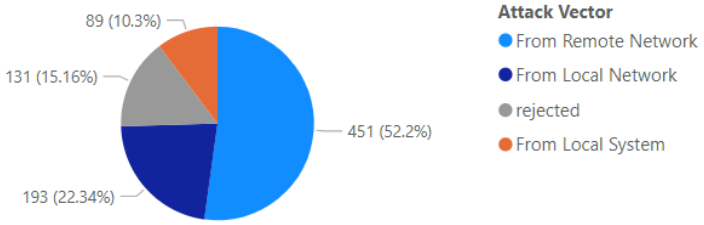
This month:	#	Change *(last month):*
Total # of advisories	**864**	↑ *(**821**)*
Unique Vendors	**89**	↓ *(**93**)*
Unique Products	**348**	↓ *(**381**)*
Unique Versions	**439**	↓ *(**492**)*
Rejected Advisories *	**131**	↓ *(**151**)*
Total Unique CVE ID's reported	**1893**	↑ **(1491)**

↑ increased ↓lower ↔ same

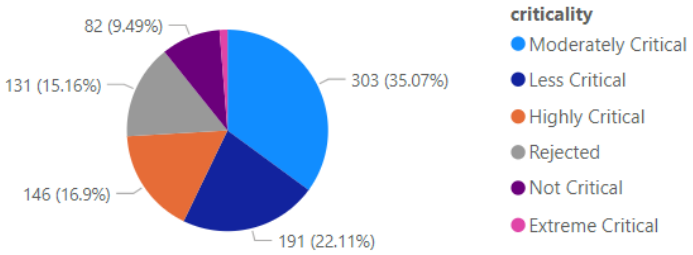
** **131** advisories have received the "rejected" status which means in general that leveraging it would require one or more violations of security best practices (e.g., product not securely configured or not used securely) or that it was "too weak of a gain" (e.g., administrative, local users already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



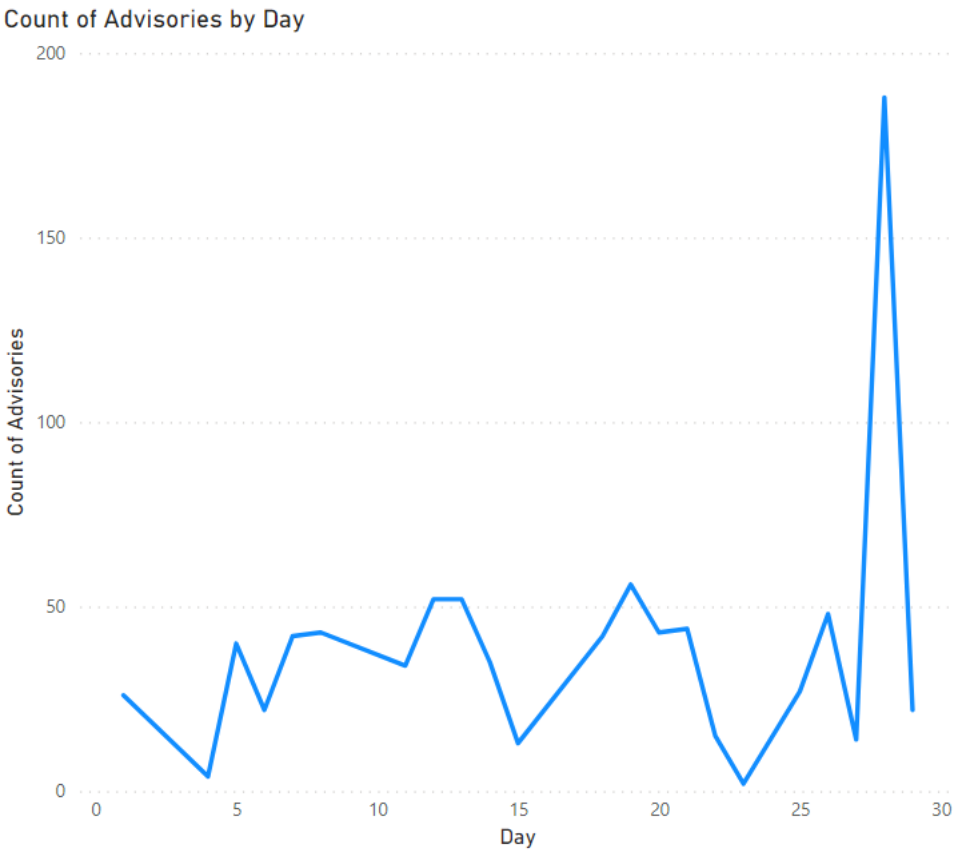
Advisories by criticality



Advisories per day

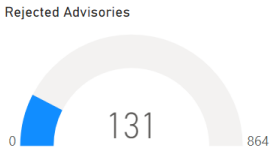
Below an overview of the daily advisory count.

Year	Month	Day	# of Advisories
2023	September	1	26
2023	September	4	4
2023	September	5	40
2023	September	6	22
2023	September	7	42
2023	September	8	43
2023	September	11	34
2023	September	12	52
2023	September	13	52
2023	September	14	35
2023	September	15	13
2023	September	18	42
2023	September	19	56
2023	September	20	43
2023	September	21	44
2023	September	22	15
2023	September	23	2
2023	September	25	27
2023	September	26	48
2023	September	27	14
2023	September	28	188
2023	September	29	22
Total			**864**



Rejected advisories.

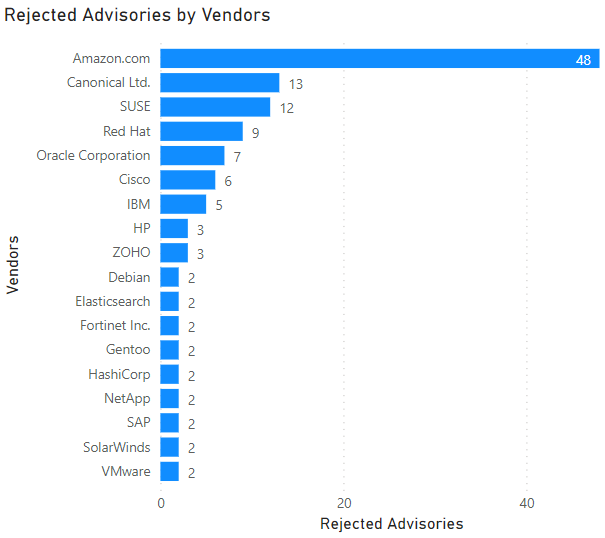
There are many vulnerabilities posted to the National Vulnerability Database (NVD) by a lot of people and companies. They are not always valid, assigned a proper criticality, and in some cases, a vulnerability may be legitimate but not afford the attacker any benefit.

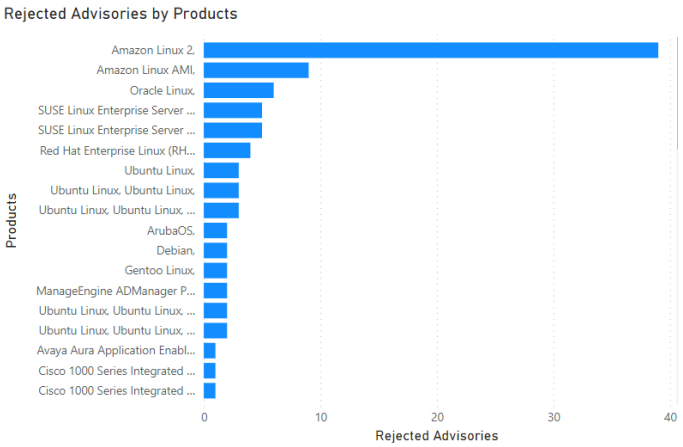


The Secunia Research team at Flexera evaluates vulnerabilities from hundreds of sources, rescores them when necessary and even rejects vulnerabilities not worth your attention. Rejection Advisories help you to reduce the volume of vulnerabilities to be mitigated by helping you focus only on those that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

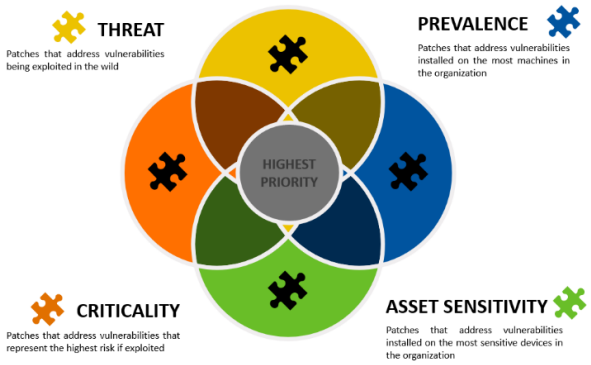
- What systems would result in the most risk if compromised?
- Is it a high-risk device? **Patch**.

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.

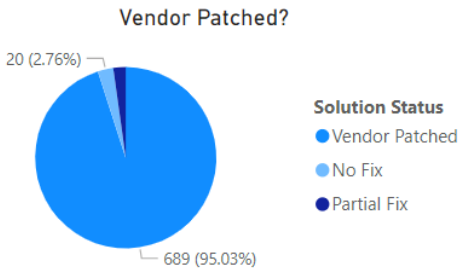
criticality	avg threat score x # of advisories
Highly Critical	5,529.00
Moderately Critical	4,370.00
Less Critical	2,626.00
Not Critical	1,056.00
Extreme Critical	906.00
Total	**14,487.00**

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.

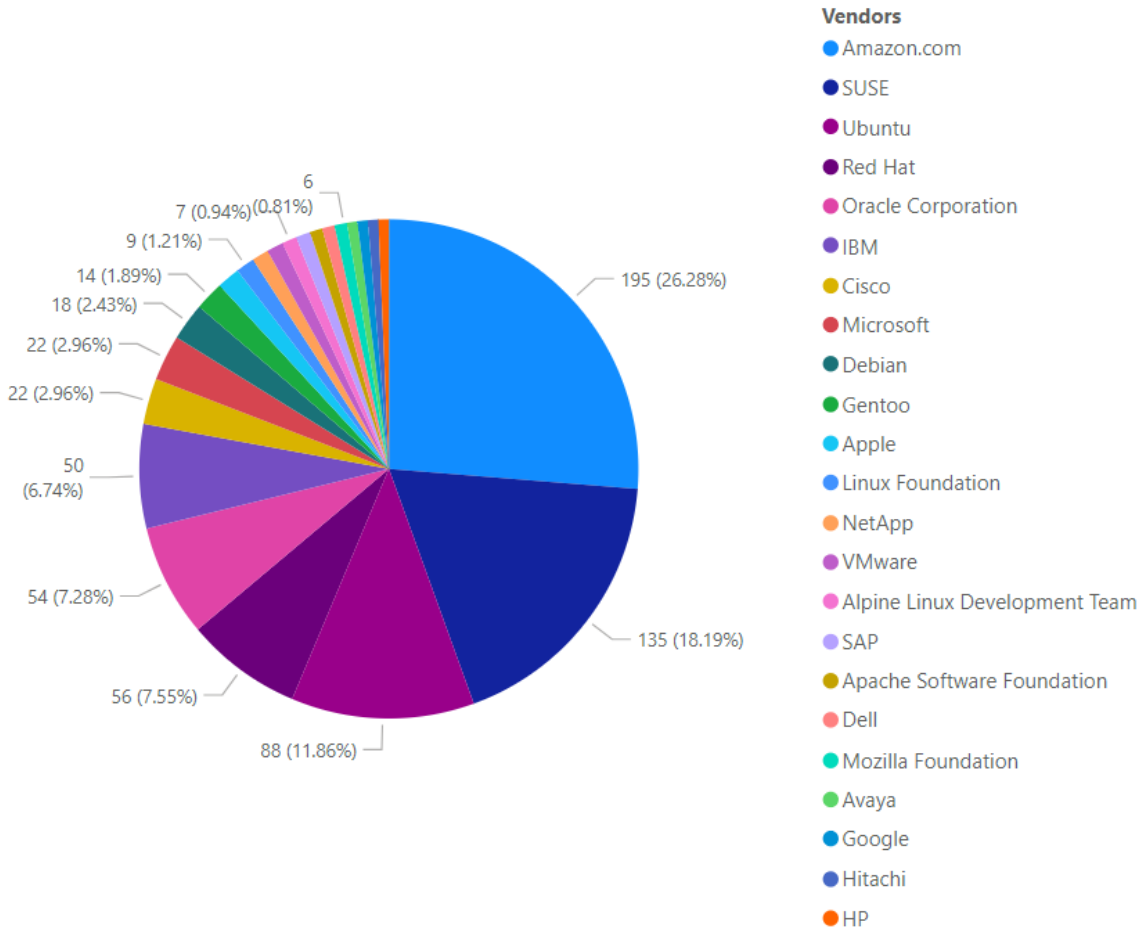
Take away 2:

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)

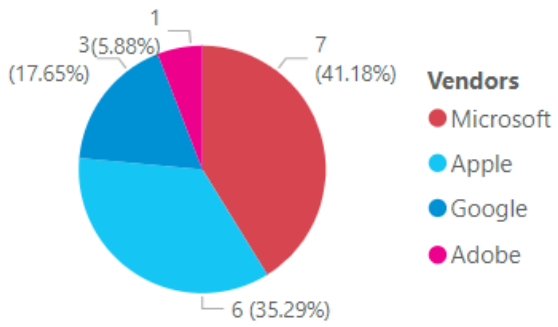


Vendor view

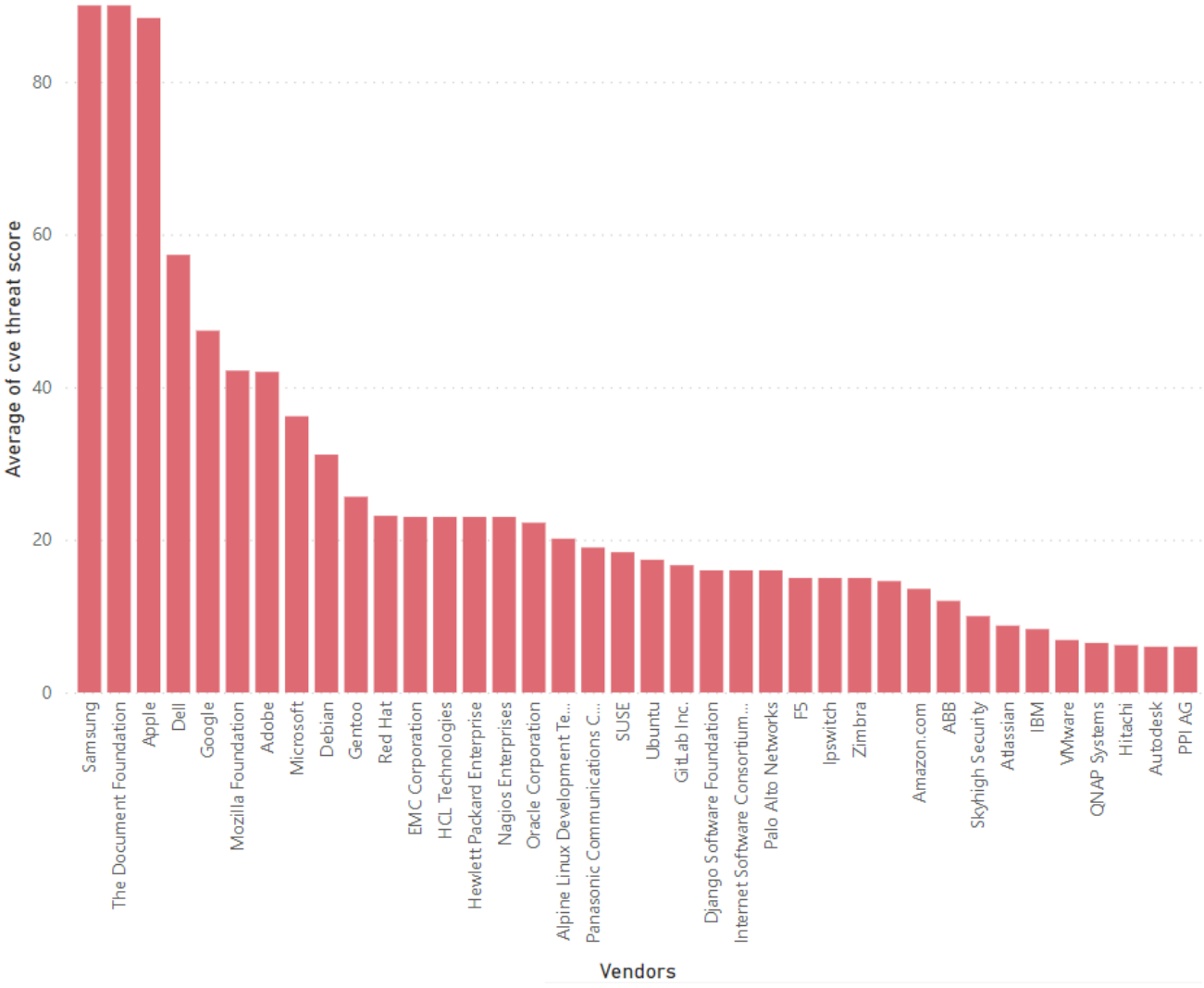
Top vendors with the most advisories



Top vendors with zero-day

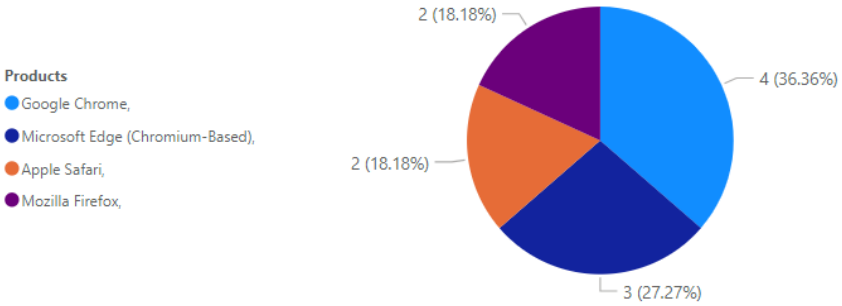


Top Vendors with highest average threat score



Browser-related advisories

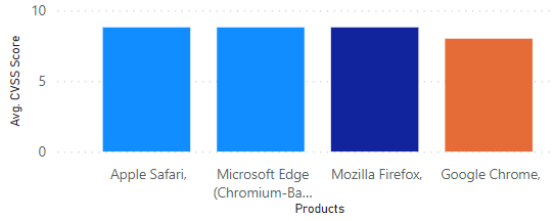
Advisories per browser



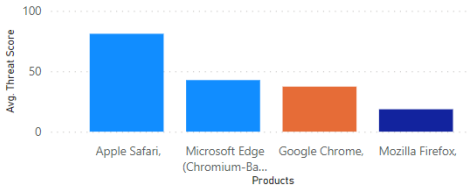
Browser zero-day vulnerabilities

Count of Advisories	Products	Advisories
1	Google Chrome,	SA119136
1	Google Chrome,	SA119598
1	Microsoft Edge (Chromium-Based),	SA119209
3		

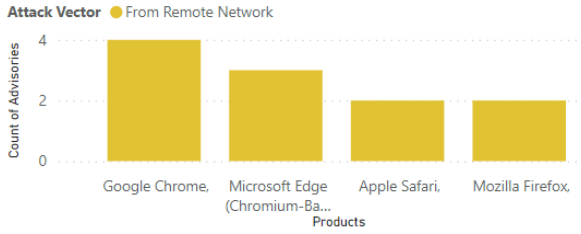
Average CVSS (criticality) score per browser



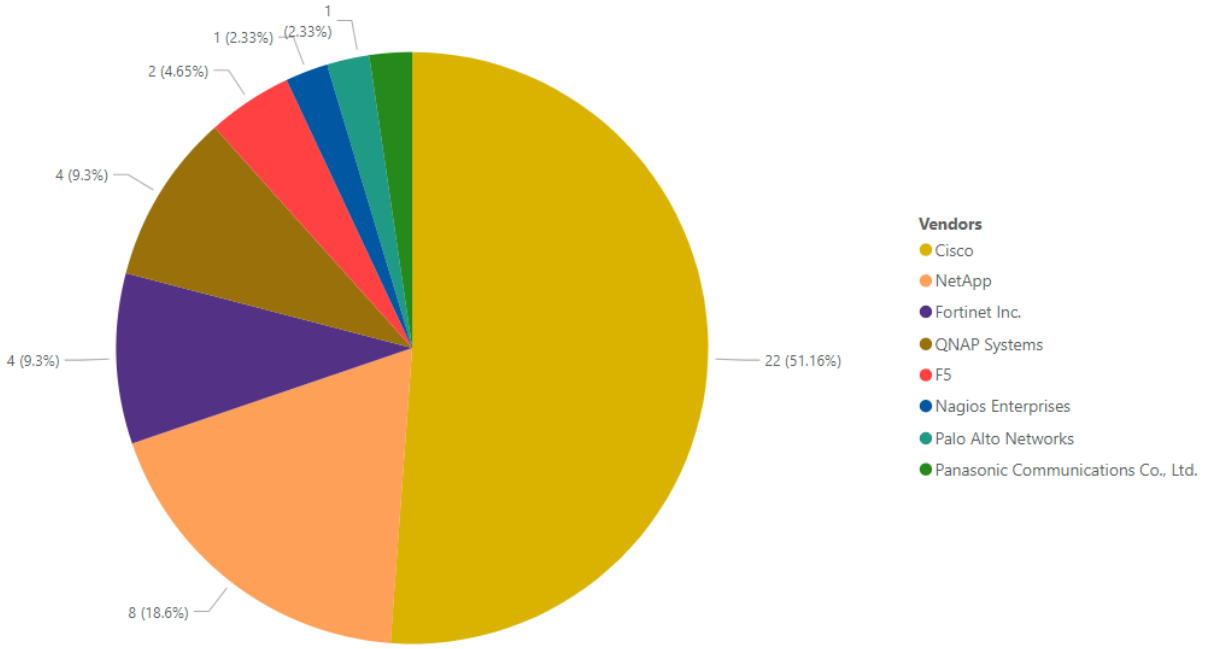
Average threat score per browser



What's the Attack Vector ?



Networking related advisories

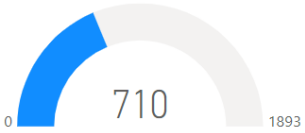


Threat intelligence

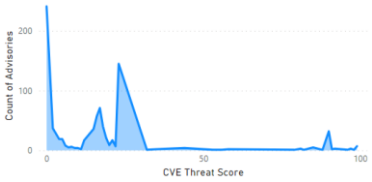
In a world where there are more than 18,000 new vulnerabilities every year, being smart about prioritizing remediation efforts is essential. Leveraging Threat Intelligence, another valuable layer of insight is provided to help you understand which of the vulnerabilities affecting your environment are 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+)	**623**↑(579)	72.11%
SAIDs with no threat score (=0)	**241**↓*(242)*	27.89%

SAID: Secunia Advisory Identifier

Range	# SAIDS	*Last month*
Medium-range threat score SAIDs (13-23)	**403** ↑	*(290)*
Low-range threat score SAIDs (1-12)	**149** ↓	*(222)*
Very critical threat score SAIDs (71-99)	60 ↑	*(16)*
High-range threat score SAIDs (24-44)	7 ↓	*(38)*
Critical-range threat score SAIDs (45-70)	4 ↓	*(13)*

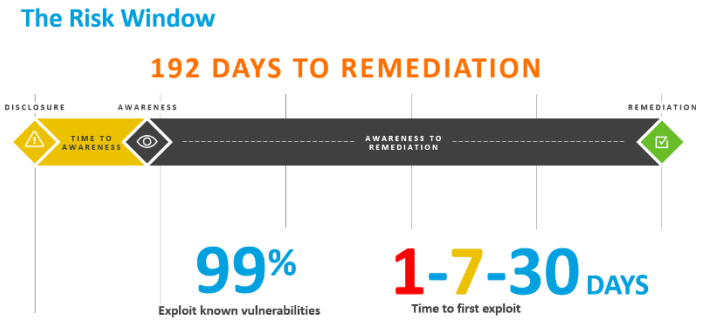
More information about how the Secunia team calculates the threat score :

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

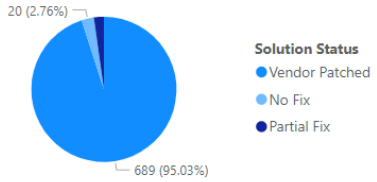
Patching

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

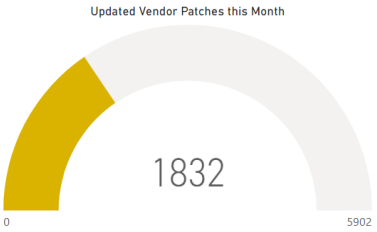


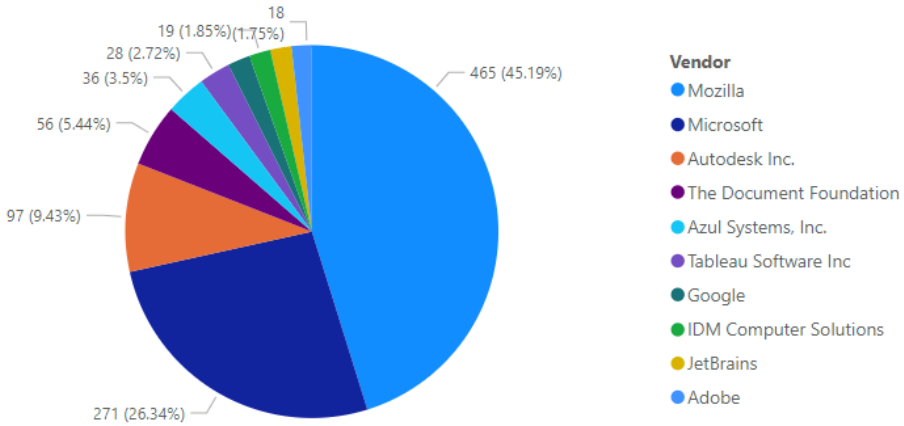
Flexera's Vendor Patch Module (VPM) statistics

Flexera has the largest third-party patch catalog **(More than 6,000)** 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)





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

First column "Day" is the date added to KEV Catalog.

Day	CVE	Vendor	Product	Due Date
6	CVE-2023-33246	Apache	RocketMQ	Wednesday, September 27, 2023
11	CVE-2023-41061	Apple	iOS, iPadOS, and watchOS	Monday, October 02, 2023
11	CVE-2023-41064	Apple	iOS, iPadOS, and macOS	Monday, October 02, 2023
12	CVE-2023-36761	Microsoft	Word	Tuesday, October 03, 2023
12	CVE-2023-36802	Microsoft	Streaming Service Proxy	Tuesday, October 03, 2023
13	CVE-2023-20269	Cisco	Adaptive Security Appliance and Firepower Threat Defense	Wednesday, October 04, 2023
13	CVE-2023-35674	Android	Framework	Wednesday, October 04, 2023
13	CVE-2023-4863	Google	Chromium WebP	Wednesday, October 04, 2023
14	CVE-2023-26369	Adobe	Acrobat and Reader	Thursday, October 05, 2023
18	CVE-2014-8361	Realtek	SDK	Monday, October 09, 2023
18	CVE-2017-6884	Zyxel	EMG2926 Routers	Monday, October 09, 2023
18	CVE-2021-3129	Laravel	Ignition	Monday, October 09, 2023
18	CVE-2022-22265	Samsung	Mobile Devices	Monday, October 09, 2023
18	CVE-2022-31459	Owl Labs	Meeting Owl	Monday, October 16, 2023
18	CVE-2022-31461	Owl Labs	Meeting Owl	Monday, October 16, 2023
18	CVE-2022-31462	Owl Labs	Meeting Owl	Monday, October 16, 2023
18	CVE-2022-31463	Owl Labs	Meeting Owl	Monday, October 16, 2023
19	CVE-2023-28434	MinIO	MinIO	Tuesday, October 10, 2023
21	CVE-2023-41179	Trend Micro	Apex One and Worry-Free Business Security	Thursday, October 12, 2023
25	CVE-2023-41991	Apple	Multiple Products	Monday, October 16, 2023
25	CVE-2023-41992	Apple	Multiple Products	Monday, October 16, 2023
25	CVE-2023-41993	Apple	Multiple Products	Monday, October 16, 2023
28	CVE-2018-14667	Red Hat	JBoss RichFaces Framework	Thursday, October 19, 2023

Top 15 of Vendors in the CISA KEV Catalog

Vendor	# of CVEs
QNAP	10
SAP	10
Trend Micro	10
Atlassian	9
SonicWall	9
Zoho	9
Zyxel	9
NETGEAR	8
Zimbra	8
Android	7
Arm	7
IBM	7
Red Hat	7
Exim	5
Owl Labs	5

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