



MONTHLY VULNERABILITY INSIGHTS

Based on Data from Secunia Research

AUGUST 2023

flexeraTM

Author: Jeroen Braak

Contents

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

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: **821** ↑ (last month: **725**).

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

- 2022 was a 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 **24.7%** Year-to-date. (Last month YTD was 22%)
- Advisories for **93** unique vendors, **381** unique products and **792** unique product versions reported this month.
- Almost **47.99%** of all vulnerabilities reported in this month have a "**Remote Attack Vector**" (last month 54.48%)
- The Secunia Research Team reported only **1 Extremely** critical advisory this month. (Last month: 16) which doesn't happen that often.
- **5 Zero-Day** Advisories reported. (last month :17)
- Over **1,491 unique** CVE's (last month: **1,731**) were covered in the **821** Advisories.
- Threat Intelligence indicates again that more **Moderately Critical Vulnerabilities** are targeted by hackers.
- More than half of all advisories are disclosed by 4 vendors (**SUSE** 16.94%, **Amazon** 13.62%, **Ubuntu** 11.04%, **RedHat** 11.04%)
- Interestingly some these vendors are also the ones with the most **rejected advisories**:
 - **SUSE**: 30 out of 151 advisories were rejected by the Secunia Research Team
 - **Amazon**: 23 out of 151 advisories were rejected.
- **Cisco and NetApp** are contributing to almost 63% of all Networking related Advisories this month.

Last month we reported that **80%** of all Secunia Advisories had a **Threat** (exploits, malware, ransomware, etc.) associated with them, **this month** the number has been **higher** to **70.52%**

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:

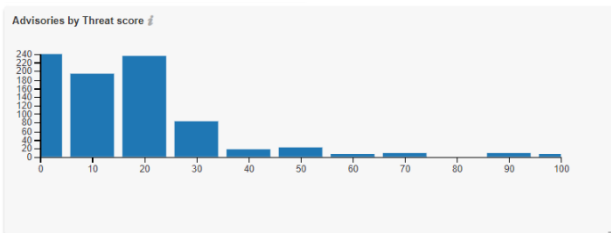
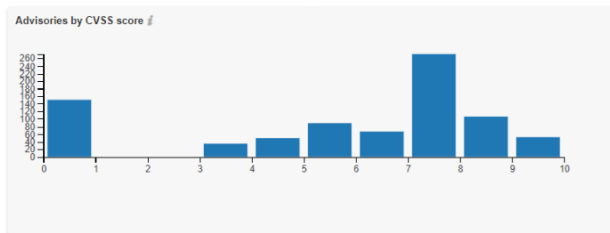
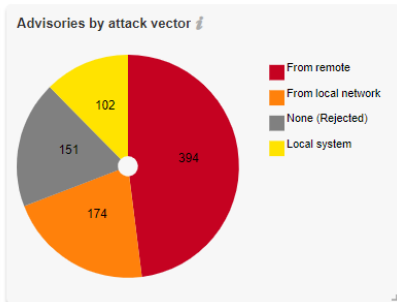
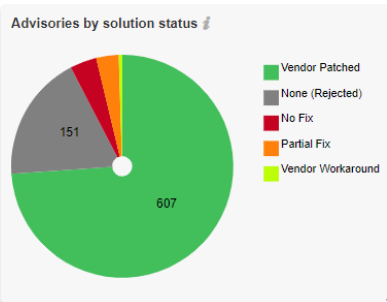
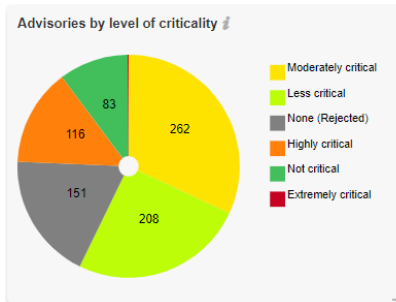
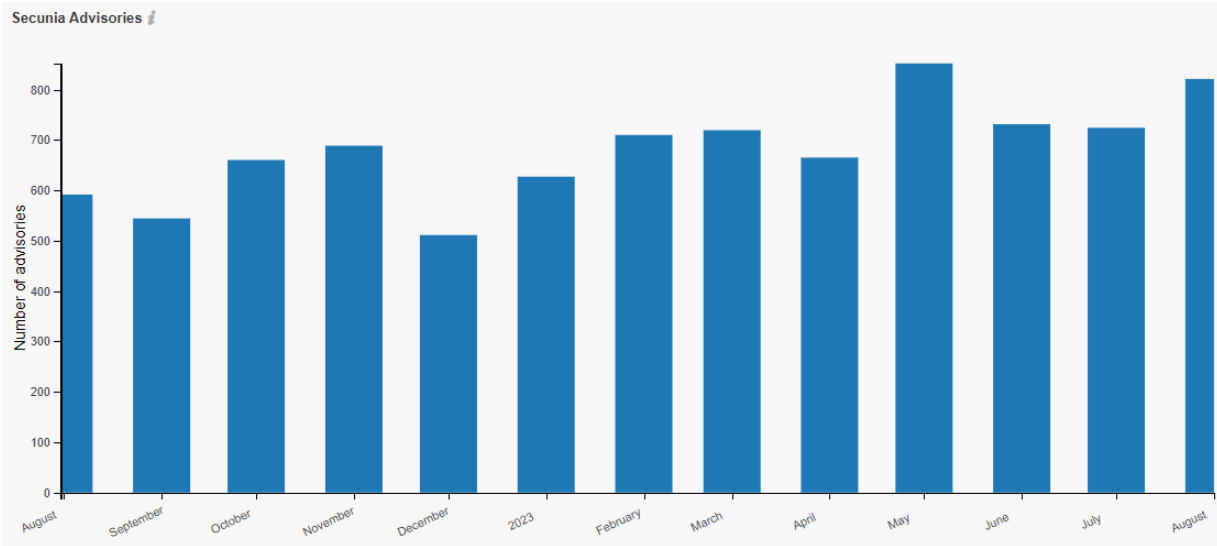
- [VMWare Aria](#) has disclosed multiple vulnerabilities(CVE-2023-34039, CVE-2023-20890) , **please patch now !**
- [WinRAR](#) disclosed a ZERO-DAY vulnerability associated with the following exploits:
 - REMCOS RAT (Remote Access Trojan)
 - ROMCOM RAT (Backdoor)
 - BURNTCIGAR
 - Cobalt Strike (Offensive Security Tools (OST))
 - Browlock (Ransomware)
- [Juniper](#) has released an "out-of-cycle" security update to address multiple vulnerabilities in the J-Web component of Junos OS. (actively being **exploited** by **ALPHV** Ransomware and **Raccoon** Stealer)
- [Microsoft](#) Releases Patches for 75 Vulnerabilities, Including 1 Zero-Day (CVE-2023-38180) and 1 advisory to stop the attack chain related to CVE-2023-36884
- [Apple](#) didn't release any security updates or rapid security responses this month.

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 **July 31, 2023**, the year-to-date total is at **5,850** Advisories **↑** which is higher than 2022 : **4,692** YTD Advisories)



Monthly data

This month, a total of **725** ↑ (last month: **725**) advisories were reported by the Secunia Research Team.

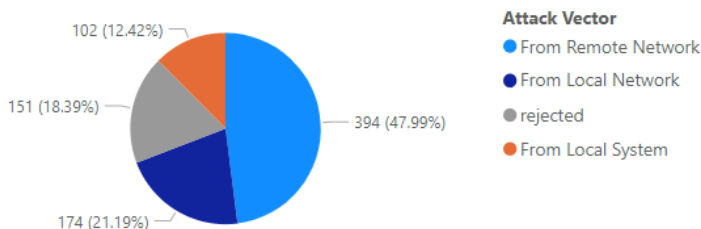
This month:	#	Change (last month):
Total # of advisories	821	↑ (725)
Unique Vendors	93	↑ (88)
Unique Products	381	↑ (337)
Unique Versions	492	↑ (410)
Rejected Advisories *	151	↑ (112)

↑ increased ↓ lower ↔ same

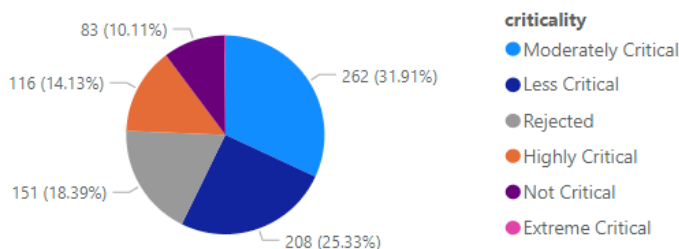
* **151** advisories have received the “rejected” status which means in general that leveraging it would require one or more violations of security best practices (e.g., product not securely configured or not used securely) or that it was “too weak of a gain” (e.g., administrative, local users already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



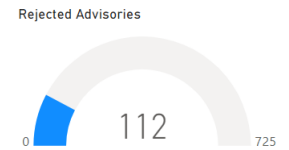
Advisories per day

Below an overview of the daily advisory count.

Year	Month	Day	# of Advisories
2023	August	1	38
2023	August	2	52
2023	August	3	33
2023	August	4	18
2023	August	7	19
2023	August	8	80
2023	August	9	45
2023	August	10	88
2023	August	11	26
2023	August	14	31
2023	August	15	19
2023	August	16	37
2023	August	17	35
2023	August	18	4
2023	August	19	23
2023	August	21	30
2023	August	22	13
2023	August	23	54
2023	August	24	41
2023	August	25	20
2023	August	28	22
2023	August	29	31
2023	August	30	22
2023	August	31	40
Total			821

Rejected advisories.

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

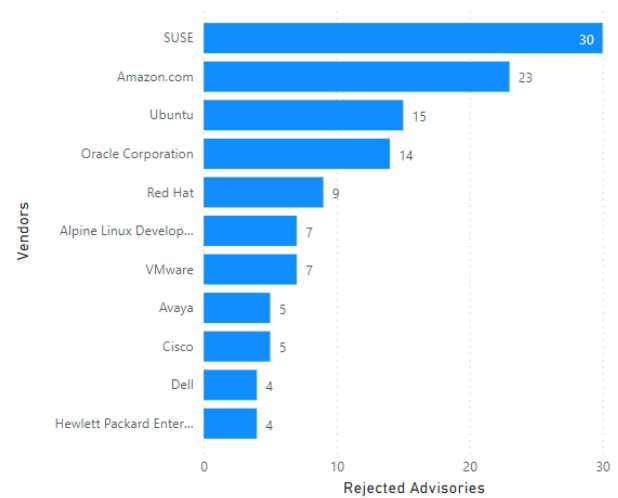


The Secunia Research team at Flexera evaluates vulnerabilities from hundreds of sources, rescors them when necessary and even rejects vulnerabilities not worth your attention. Rejection Advisories help you to reduce the volume of vulnerabilities to be mitigated by helping you focus only on those that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

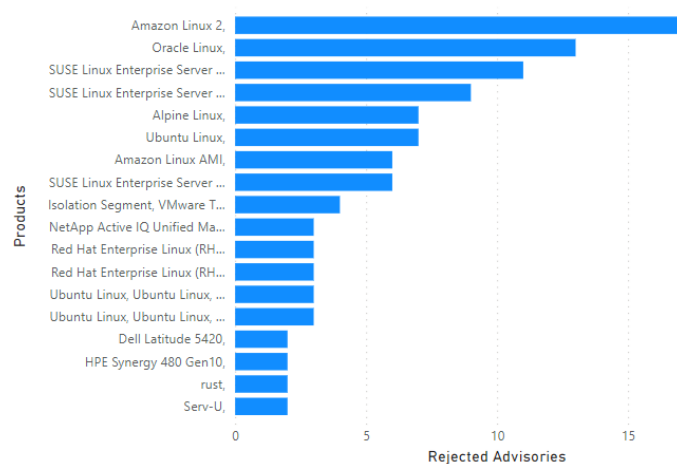
An advisory may be rejected many reasons. The most common are:

- No reachability**
 The vulnerability cannot be exploited because the affected systems cannot be reached by an attacker.
- No gain**
 The vulnerability may be reached, but without any gain for the attacker.
- No exploitability**
 The vulnerability cannot be exploited because, for example, policy forbids installation of the affected software.
- Dependent on other**
 The vulnerability cannot be exploited by itself, but depends on another vulnerability being present.

Rejected Advisories by Vendors



Rejected Advisories by Products



Addressing awareness with vulnerability insights

Prevalence:

- How many systems would benefit from any given security update?
- Does it pose a risk? It's on all systems? **Patch.**

Asset Sensitivity:

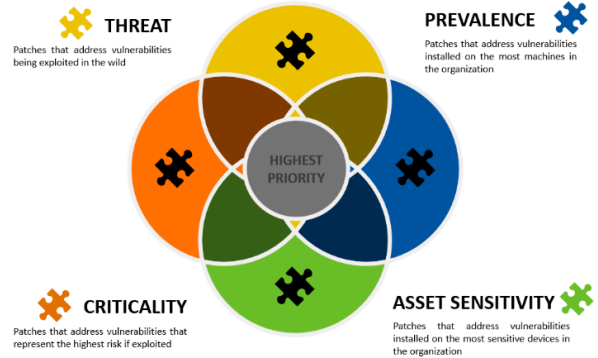
- What systems would result in the most risk if compromised?
- Is it a high-risk device? **Patch.**

Criticality:

- The most popular method of thoughtful prioritization.
- If exploited, how bad could it affect your security? Is it designated to be of a high criticality? **Patch.**

Threat Intelligence:

- The newest and most impactful method focuses on the likelihood of exploitation.
- Is it likely to be exploited? **Patch.**



How do we know that more insights/data is needed?

Focusing on vulnerabilities with CVSS 7 or higher would address about 50 percent of exploits. Most exploits are CVSS scored between 4 and 7.

Focusing

on vulnerabilities for the top 20 vendors would address only about 20 percent.

criticality	avg threat score x # of advisories
Moderately Critical	3,547.00
Less Critical	2,921.00
Highly Critical	2,733.00
Not Critical	1,067.00
Extreme Critical	67.00
Total	10,335.00

Take away 1:

Critical vulnerabilities do not necessarily present the most risk.

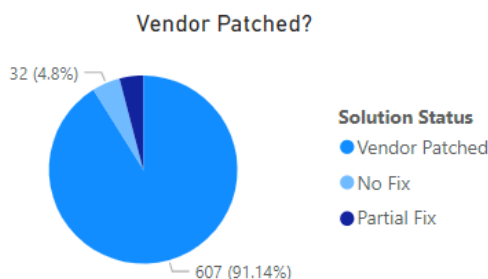
Leverage threat intelligence to better prioritize what demands your most urgent attention.

Organizations who do not have Threat Intelligence data should consider implementing this to ensure they have the complete picture.

Take away 2:

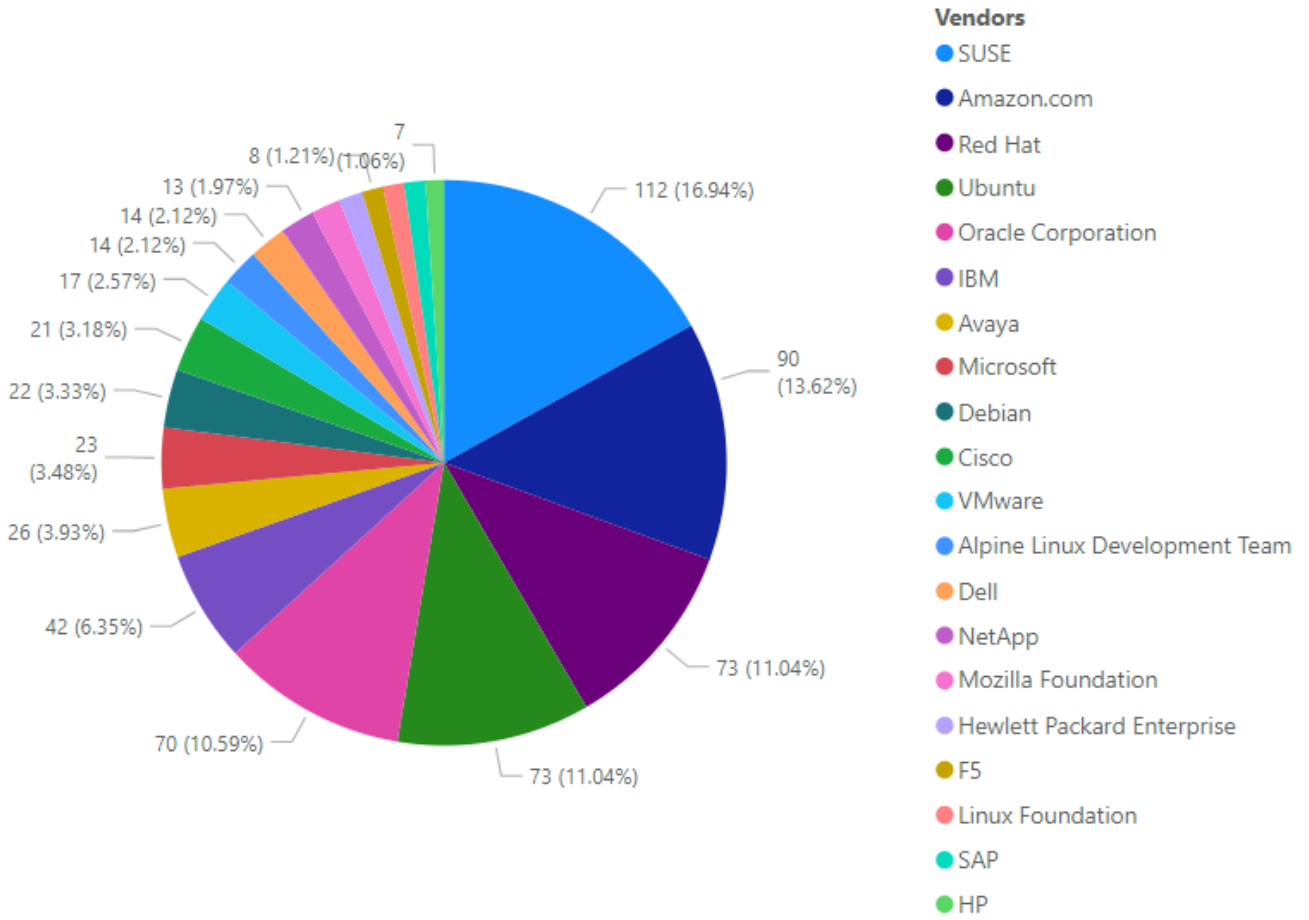
Most vulnerabilities have a patch available (typically within 24 hours after disclosure).

(No fix : no patch available for this insecure version, therefore need to upgrade)

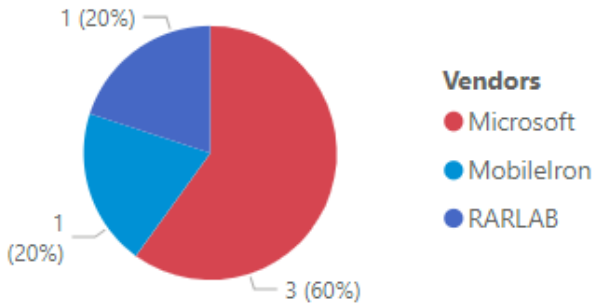


Vendor view

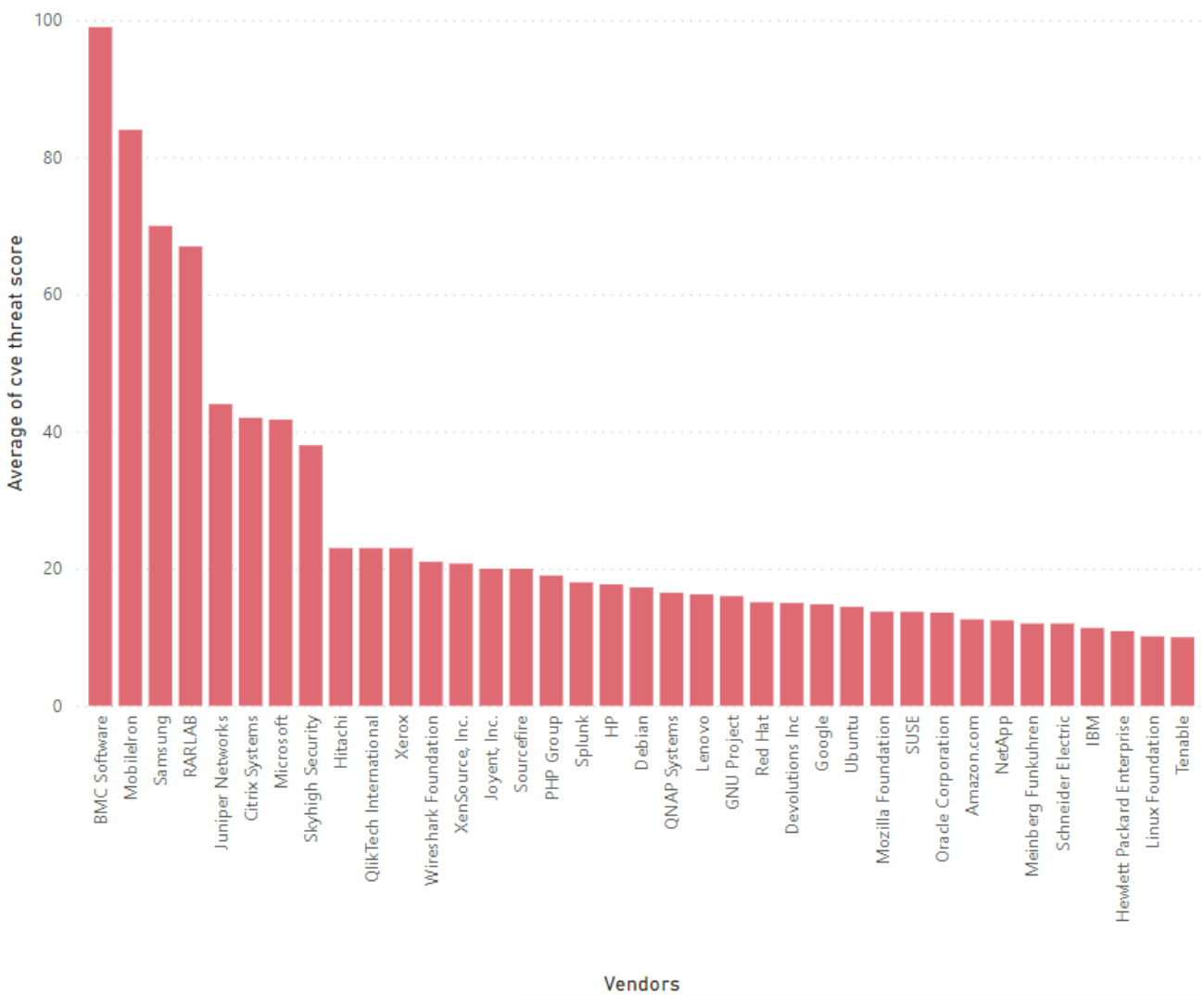
Top vendors with the most advisories



Top vendors with zero-day

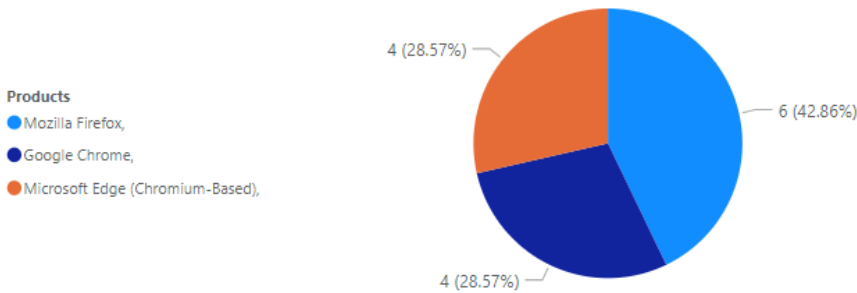


Top Vendors with highest average threat score



Browser-related advisories

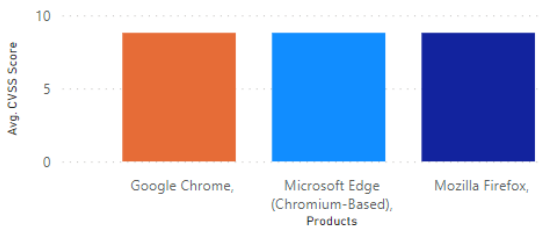
Advisories per browser



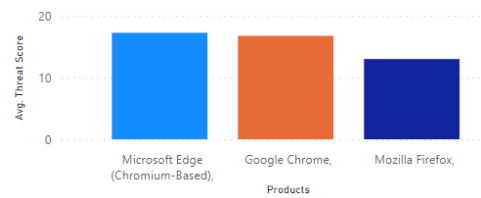
Browser zero-day vulnerabilities

No zero-day's reported for browsers

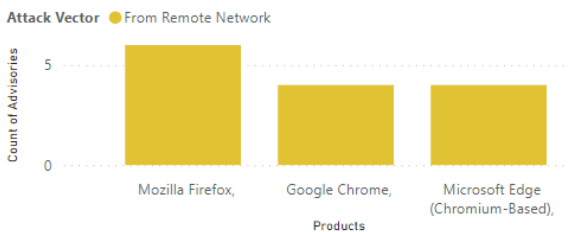
Average CVSS (criticality) score per browser



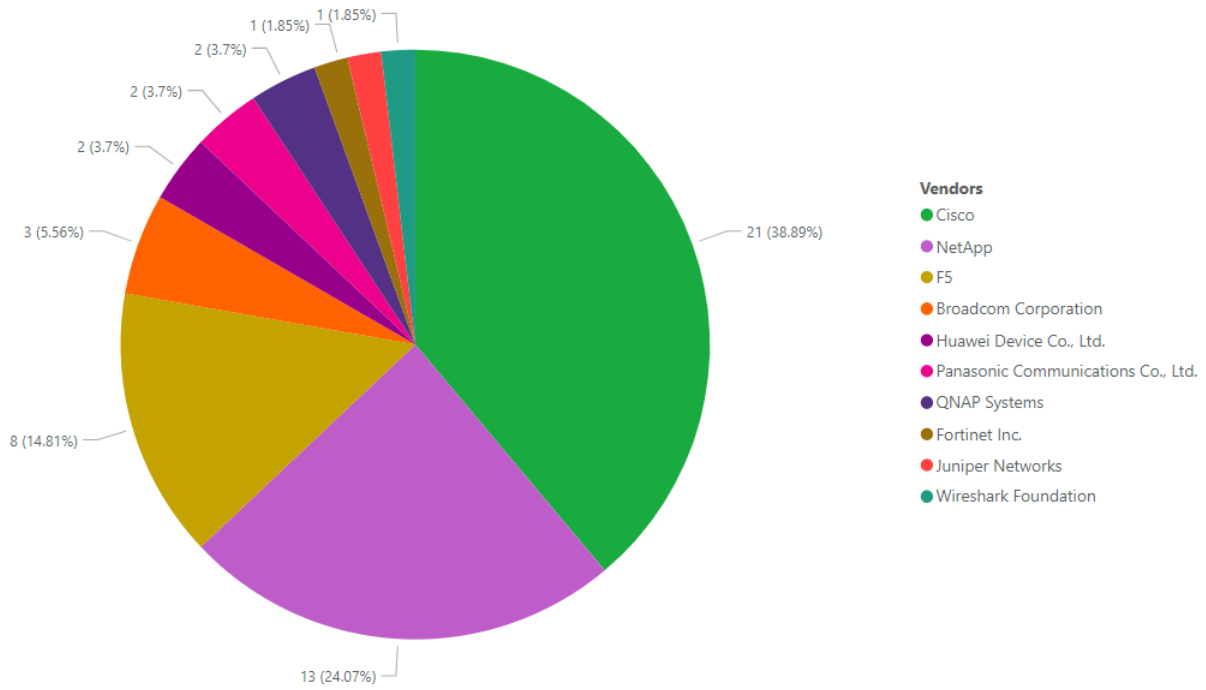
Average threat score per browser



What's the Attack Vector ?



Networking related advisories

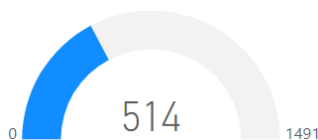


Threat intelligence

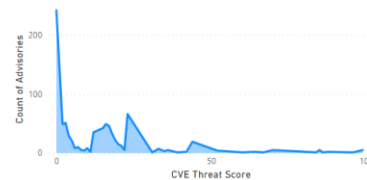
In a world where there are more than 18,000 new vulnerabilities every year, being smart about prioritizing remediation efforts is essential. Leveraging Threat Intelligence, another valuable layer of insight is provided to help you understand which of the vulnerabilities affecting your environment are 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+)	579 ↓ (580)	70.52%
SAIDs with no threat score (=0)	242 ↑ (145)	29.48%

SAID: Secunia Advisory Identifier

Range	# SAIDS	Last month
Medium-range threat score SAIDs (13-23)	290 ↓	(386)
Low-range threat score SAIDs (1-12)	222 ↑	(147)
High-range threat score SAIDs (24-44)	38 ↑	(4)
Very critical threat score SAIDs (71-99)	16 ↓	(34)
Critical-range threat score SAIDs (45-70)	13 ↑	(9)

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

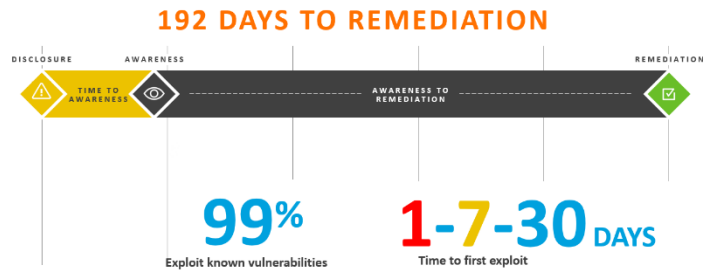
- [Evidence of exploitation](#)
- [Criteria for the threat Score Calculation](#)
- [Threat Score Calculation - Examples](#)

Patching

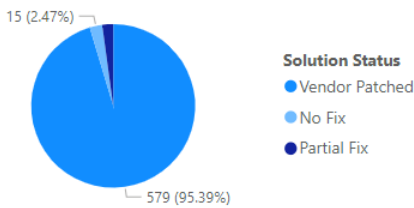
Most of this month's vulnerabilities are vendor patched. In fact, most vulnerabilities are patched within 24 hours after disclosure.

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

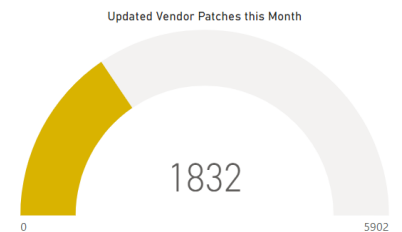
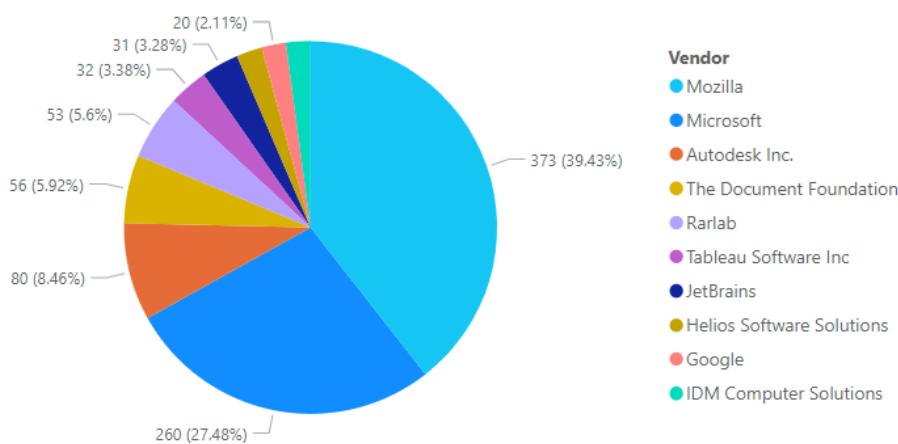


Flexera's Vendor Patch Module (VPM) statistics

Flexera has the largest third-party patch catalog (**More than 5,600**) 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 month's the additions to the KEV catalog

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

Day	CVE	Vendor	Product	Due Date
7	CVE-2021-29256	Arm	Mali Graphics Processing Unit (GPU)	Friday, July 28, 2023
11	CVE-2022-31199	Netwrix	Auditor	Tuesday, August 01, 2023
11	CVE-2023-32046	Microsoft	Windows	Tuesday, August 01, 2023
11	CVE-2023-32049	Microsoft	Windows	Tuesday, August 01, 2023
11	CVE-2023-35311	Microsoft	Outlook	Tuesday, August 01, 2023
11	CVE-2023-36874	Microsoft	Windows	Tuesday, August 01, 2023
13	CVE-2022-29303	SolarView	Compact	Thursday, August 03, 2023
13	CVE-2023-37450	Apple	Multiple Products	Thursday, August 03, 2023
19	CVE-2023-3519	Citrix	NetScaler ADC and NetScaler Gateway	Wednesday, August 09, 2023
20	CVE-2023-29298	Adobe	ColdFusion	Thursday, August 10, 2023
20	CVE-2023-38205	Adobe	ColdFusion	Thursday, August 10, 2023
25	CVE-2023-35078	Ivanti	Endpoint Manager Mobile (EPMM)	Tuesday, August 15, 2023
26	CVE-2023-38606	Apple	Multiple Products	Wednesday, August 16, 2023
27	CVE-2023-37580	Zimbra	Collaboration (ZCS)	Thursday, August 17, 2023
31	CVE-2023-35081	Ivanti	Endpoint Manager Mobile (EPMM)	Monday, August 21, 2023
17	CVE-2023-36884	Microsoft	Windows	Tuesday, August 29, 2023

Top 15 of Vendors in the CISA KEV Catalog

Vendor	# of CVEs
Microsoft	266
Cisco	64
Adobe	63
Apple	62
Google	48
Oracle	32
Apache	28
VMware	18
D-Link	15
Citrix	13
Ivanti	12
Linux	12
Fortinet	11
Mozilla	11
QNAP	10

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