

MONTHLY VULNERABILITY INSIGHTS

Based on Data from Secunia Research

AUGUST 2022

flexera

Inform IT. Transform IT.™

Author: Jeroen Braak

Contents

Introduction.....	3
Secunia Research software vulnerability tracking process	3
Summary	3
Year-to-date overview	4
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
More information	16

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](#).

Summary

Total advisories : **591** ↑ (last month: **548**) .

August reported more advisories than July.

The **Log4j** vulnerability is still being detected / reported by vendors after almost **9 months** mostly by IBM:

- IBM Security identity Manager
- IBM Infosphere Master Data Management
- IBM Data Risk Manager
- CommVault

This month , the **trend** that we've seen for the last few months with hackers focusing on the Low and Medium Vulnerabilities has lowered again. We are seeing more focus this month on Highly Critical Vulnerabilities being exploited , but Moderately and Less Critical Vulnerabilities are still a target for hackers to create exploits for.

Please make sure you include Threat Intelligence in your Software Vulnerability Management Process to improve your prioritization .

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

- No extremely critical advisories were reported by the Secunia Research Team.
- **6 Zero-Day** Advisory reported (4x Apple (iOS,Safari,MacOS) , 1x Google Chrome , 1x Microsoft Edge)
- Over **1,982** CVE's were covered in the **591** Advisories
- Threat Intelligence indicates that more **Medium and Highly Critical Vulnerabilities** are targeted by hackers.
- More than half of all advisories are disclosed by **IBM, SUSE, Ubuntu (Canonical) , RedHat and Gentoo**.

Last month we reported that **64.23%** of all Secunia Advisories had a Threat (exploits, malware, ransomware , etc.) associated with them, this month the number has been slightly higher to **68.70%** , with an increase in the lower and medium criticality range.

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 Russia-Ukraine conflict , attacks on critical infrastructures in many countries are increasing.

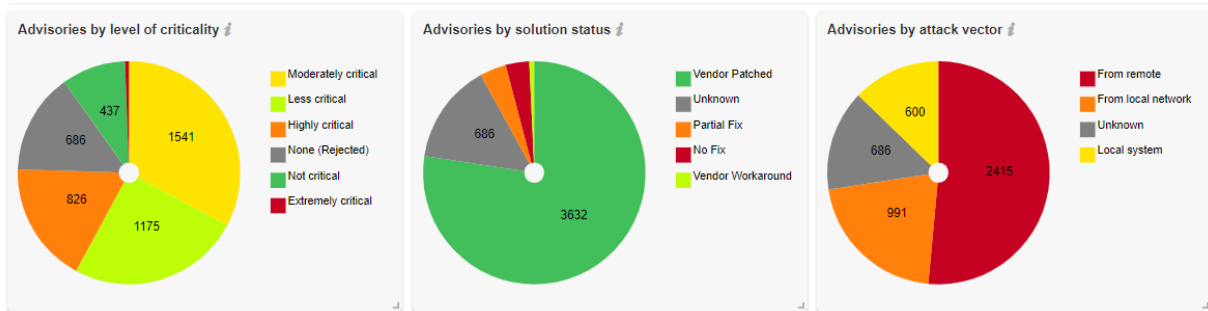
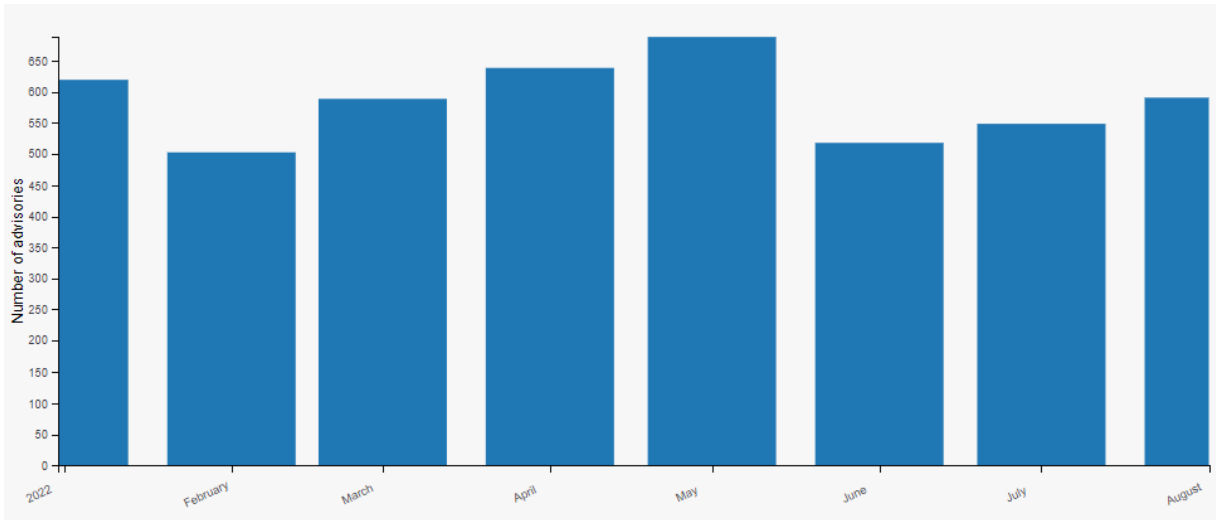
Back in 2019 (just before Covid) patching was recommended within 30 days (or 14 days for CVSS score 7 or higher)


Right now , hackers are able to deploy exploits within 1 week and even within **24 hours** . This means that organizations need

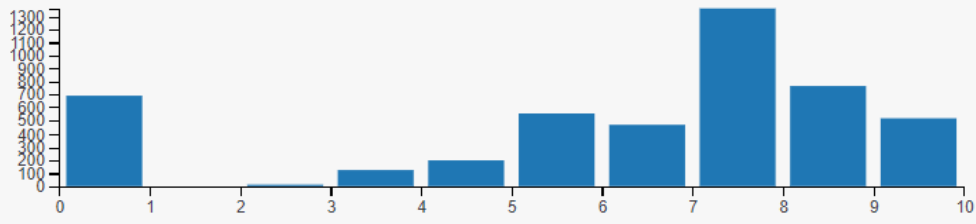
to prioritize even better to quickly patch vulnerabilities (especially the ones with threats associated with them)


Year-to-date overview

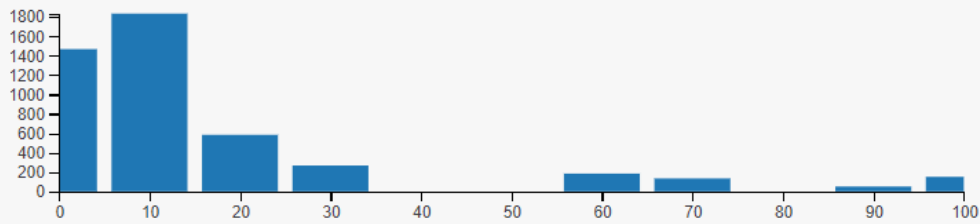
As of **August 31 2022**, the year-to-date total is at **4,692** Advisories **↑** which is higher than 2021 : **4,095** YTD Advisories)



Advisories by CVSS score 



Advisories by Threat score 



Monthly data

This month, a total of **591** ↑ (last month: **548**) advisories were reported by the Secunia Research Team.

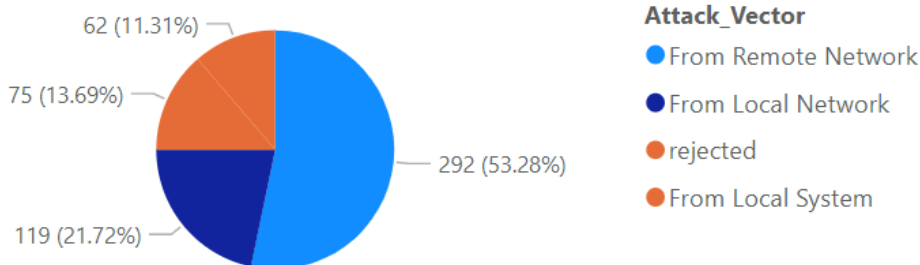
This month:	#	Change (last month):
Total # of advisories	591	↑ (548)
Unique Vendors	80	↓ (93)
Unique Products	322	= (322)
Unique Versions	404	↓ (413)
Rejected Advisories *	86	↑ (75)

↑ increased ↓ lower ↔ same

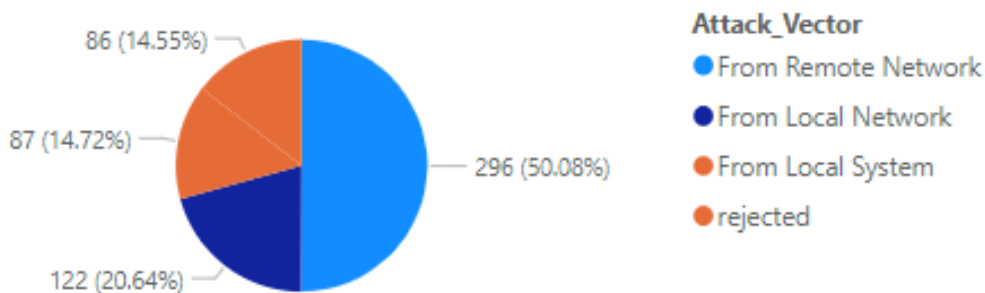
* **86** advisories have received the “rejected” status which means in general that leveraging it would require one or more violations of security best practices (e.g., product not securely configured or not used securely) or that it was “too weak of a gain” (e.g., administrative, local users already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



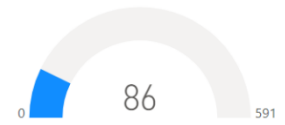
Advisories per day

Below an overview of the daily advisory count.

Year	Month	Day	# of Advisories
2022	August	1	27
2022	August	2	27
2022	August	3	64
2022	August	4	37
2022	August	5	19
2022	August	8	15
2022	August	9	35
2022	August	10	38
2022	August	11	38
2022	August	12	15
2022	August	15	29
2022	August	16	18
2022	August	17	23
2022	August	18	17
2022	August	19	11
2022	August	22	22
2022	August	23	18
2022	August	24	47
2022	August	25	17
2022	August	26	22
2022	August	29	10
2022	August	30	31
2022	August	31	11
Total			591

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.

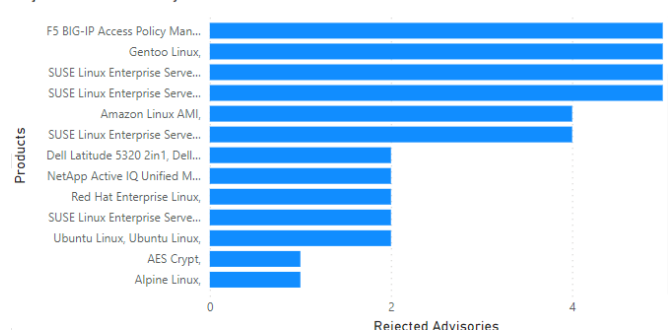


The Secunia Research team at Flexera evaluates vulnerabilities from hundreds of sources, rescores them when necessary and even rejects vulnerabilities not worth your attention. Rejection Advisories help you to reduce the volume of vulnerabilities to be mitigated by helping you focus only on those that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

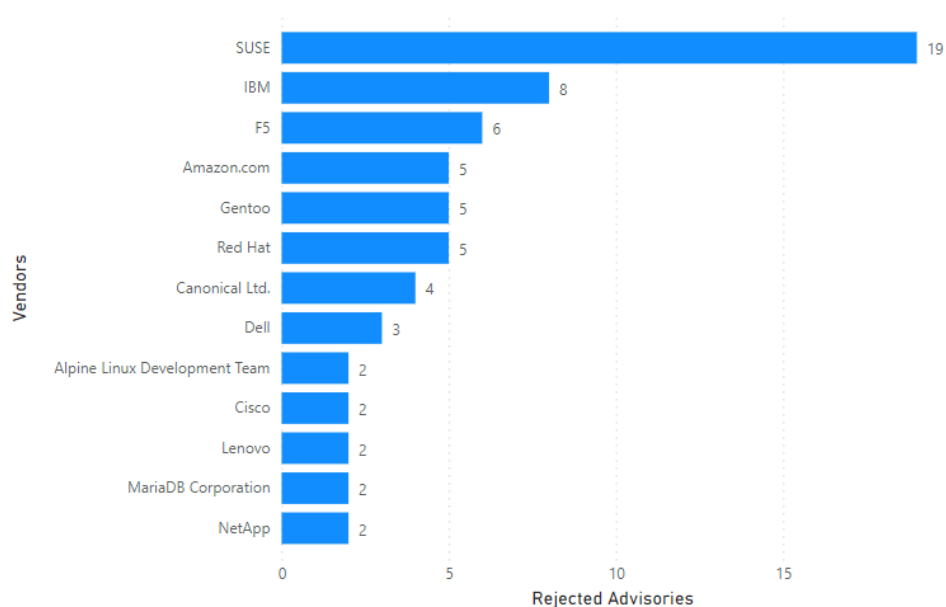
An advisory may be rejected many reasons. The most common are:

- 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.

Rejected Advisories by Products



Rejected Advisories by Vendors



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:

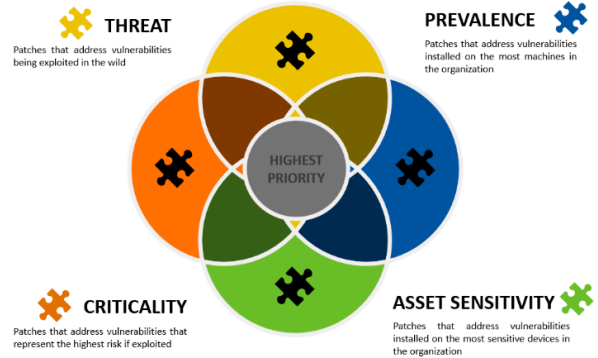
- What systems would result in the most risk if compromised?
- Is it a high-risk device? Patch.

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.

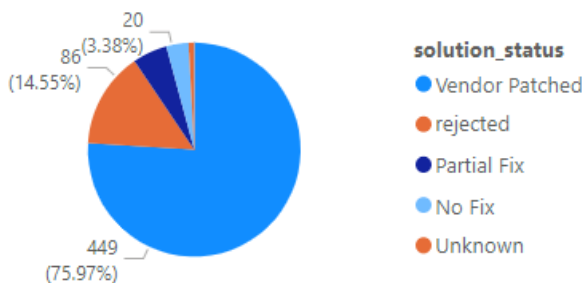
criticality	avg threat score x # of advisories
Highly Critical	2,972.00
Moderately Critical	2,298.00
Less Critical	1,677.00
Not Critical	623.00
Extreme Critical	372.00
Total	7,942.00

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:

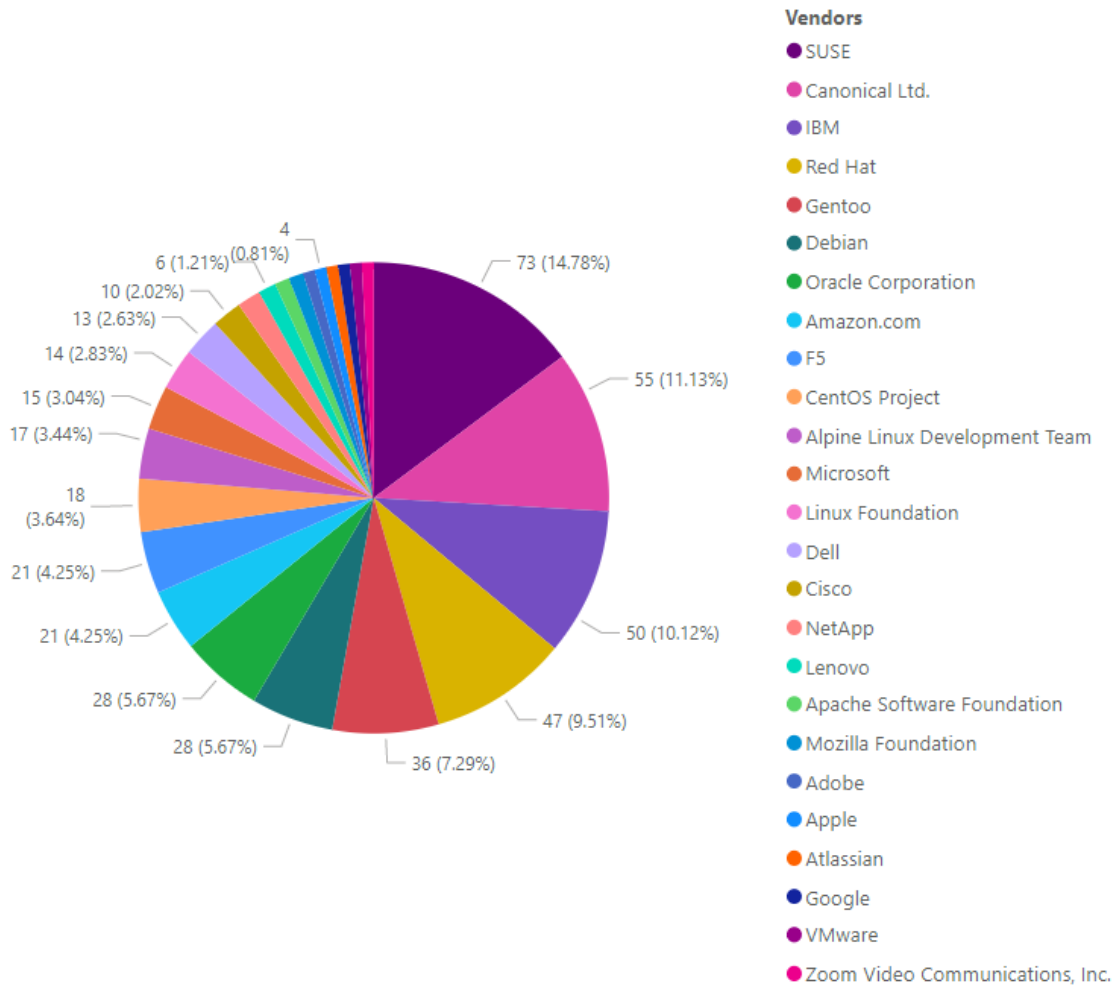
Most vulnerabilities have a patch available (typically within 24 hours after disclosure).



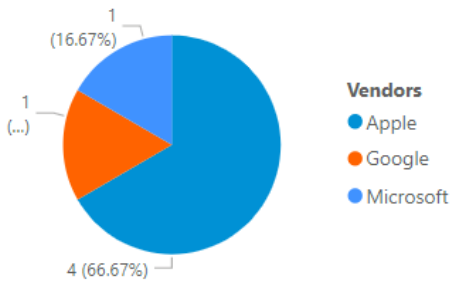
Previous month : 418 Vendor Patched (76.28%)
 This Month : 449 Vendor Patched (75.97%)

Vendor view

Top vendors with the most advisories

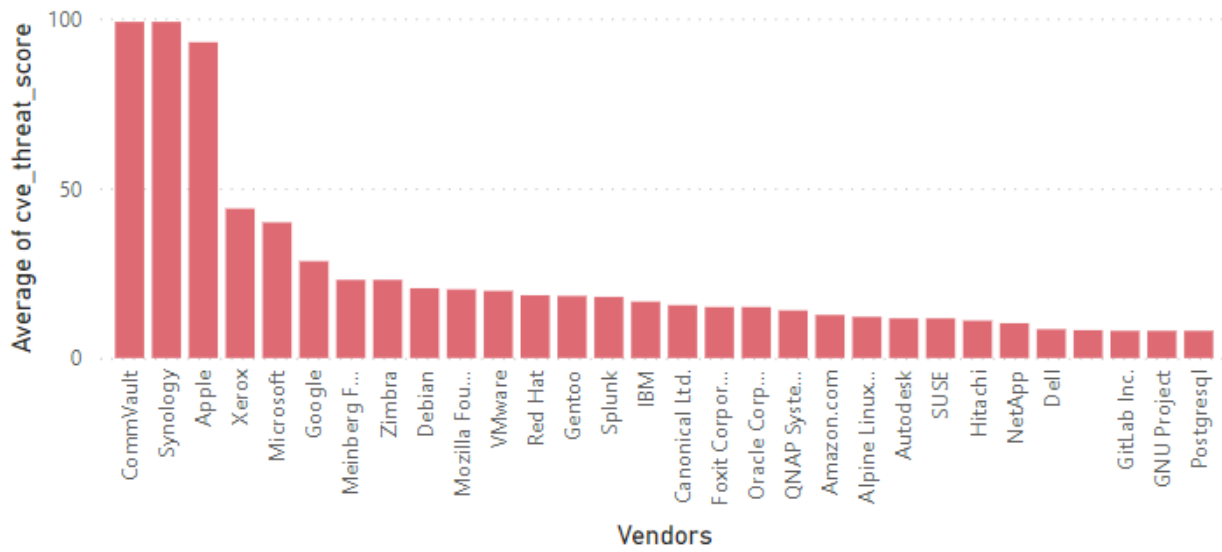


Top vendors with zero-day



Top Vendors with highest average threat score

Top Vendors with highest average Threat Score

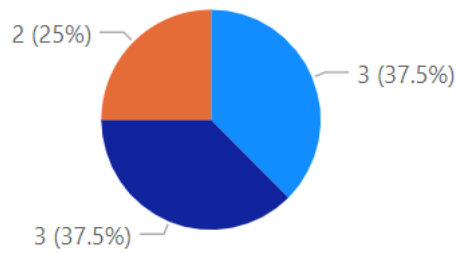


Browser-related advisories

Advisories per browser

Products

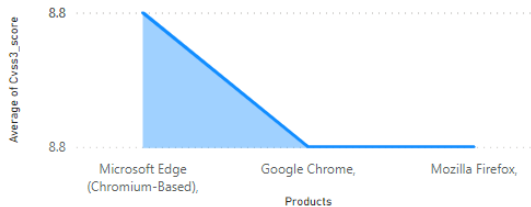
- Google Chrome,
- Mozilla Firefox,
- Microsoft Edge (Chromium-Based),



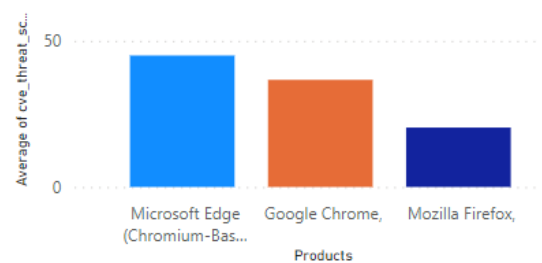
Browser zero-day vulnerabilities

Count of Advisories	Products	Advisories
1	Google Chrome,	SA110442
1	Microsoft Edge (Chromium-Based),	SA110452
2		
Count of Advisories	Products	Advisories

Average CVSS (criticality) score per browser



Average threat score per browser

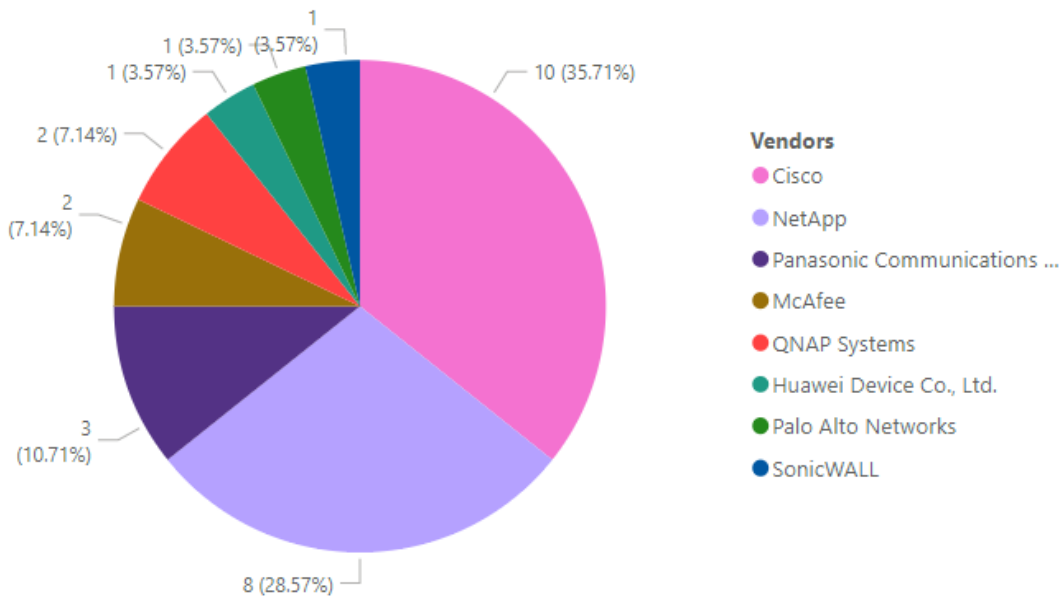


What's the Attack Vector ?

Attack_Vector ● From Remote Network



Networking related advisories



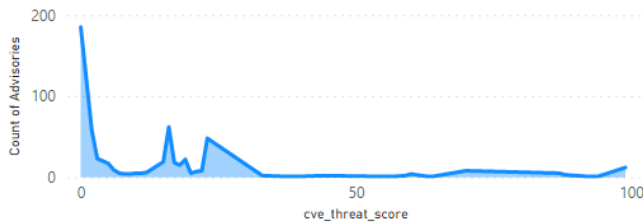
Threat intelligence

A look at threat intelligence related data for the month.

Count of malware-exploited CVEs



Count of advisories by CVE threat score



Threat intelligence advisory statistics:

SAIDs with a threat score (1+)	406 ↑ (352)	68.70%
SAIDs with no threat score (=0)	185 ↓ (196)	31.30%

SAID: Secunia Advisory Identifier

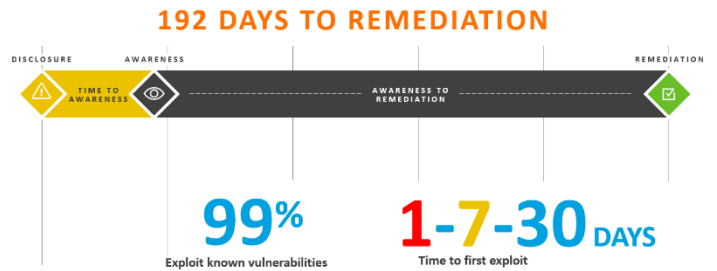
Range	Score	Last month
Medium-range threat score SAIDs (13-23)	204 ↑	(179)
Low-range threat score SAIDs (1-12)	156 ↑	(125)
Critical-range threat score SAIDs (45-70)	18 ↓	(32)
Very critical threat score SAIDs (71-99)	22 ↑	(14)
High-range threat score SAIDs (24-44)	6 ↑	(2)

Patching

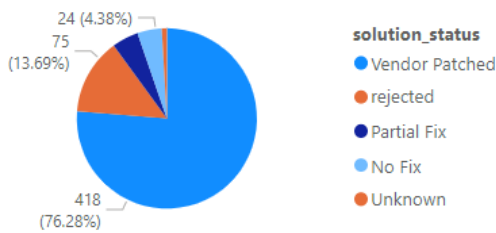
Most of this month's vulnerabilities are vendor patched. In fact, most vulnerabilities are patched within 24 hours after disclosure.

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

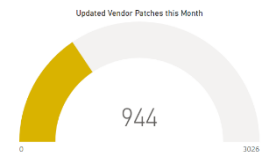


Vulnerabilities that are vendor patched



Flexera's Vendor Patch Module (VPM) statistics

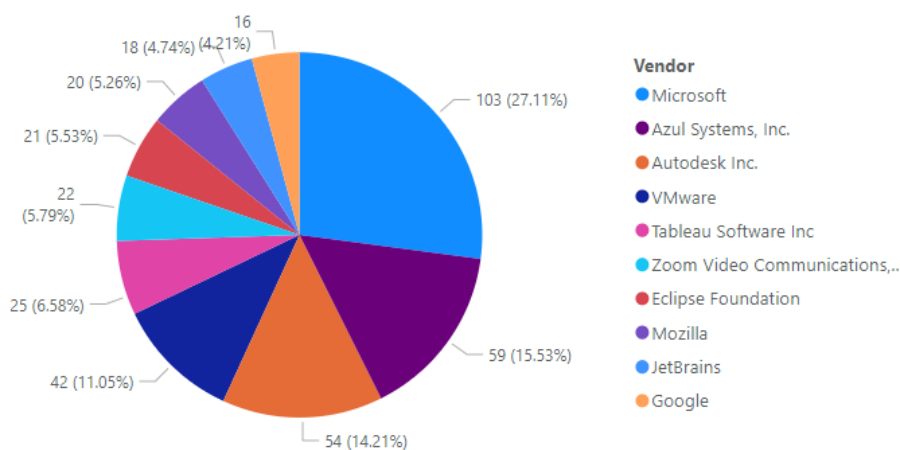
Flexera has the largest third-party patch catalog (3000+) in the world. This helps customers act quicker and save time by offering an integrated approach to effectively locate, prioritize threats and remediate them quickly to lower the risk to your organization.



This month's top vendor patches

(Updated Patches per vendor)

Patches per vendor



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