MONTHLY VULNERABILITY INSIGHTS

Based on Data from Secunia Research

JULY 2022

Flexera

Inform IT. Transform IT.™

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.

Summary

Total advisories : **548** ↑ (last month: **517**) .

July reported more advisories than June's sudden dip . (first half year was a continued monthly increase until June)

The **Log4j** vulnerability is still being detected / reported by vendors after almost 8 months:

- IBM Operations Analytics
- IBM Tivoli Network IP Edition
- IBM Enterprise Content Management System Monitor

The **trend** that we've seen for the last few months with hackers focusing on the Low and Medium Vulnerabilities has increased again (with May being an exception) . These Moderate and Less Critical Vulnerabilities are normally not a priority for many organizations, but please make sure you include Threat Intelligence in your Software Vulnerability Management Process to improve your prioritization .

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

- 2 extreme critical advisories reported (Google Chrome and Microsoft Edge both also Zero-day)
- 8 **Zero-Day** Advisory reported (6x Microsoft OS , 1x Google Chrome , 1x Microsoft Edge)
- Over **2,645** CVE's were covered in the **548** Advisories which is more than double from last month. (**1,281**)
- Threat Intelligence indicates that more **Medium and Low Vulnerabilities** are targeted by hackers.
- Most vulnerabilities **(57.34%)** are disclosed by **IBM, SUSE, Ubuntu (Canonical) , Oracle and Amazon.**
  (Red Hat this month outside the top 5 / top +50%)

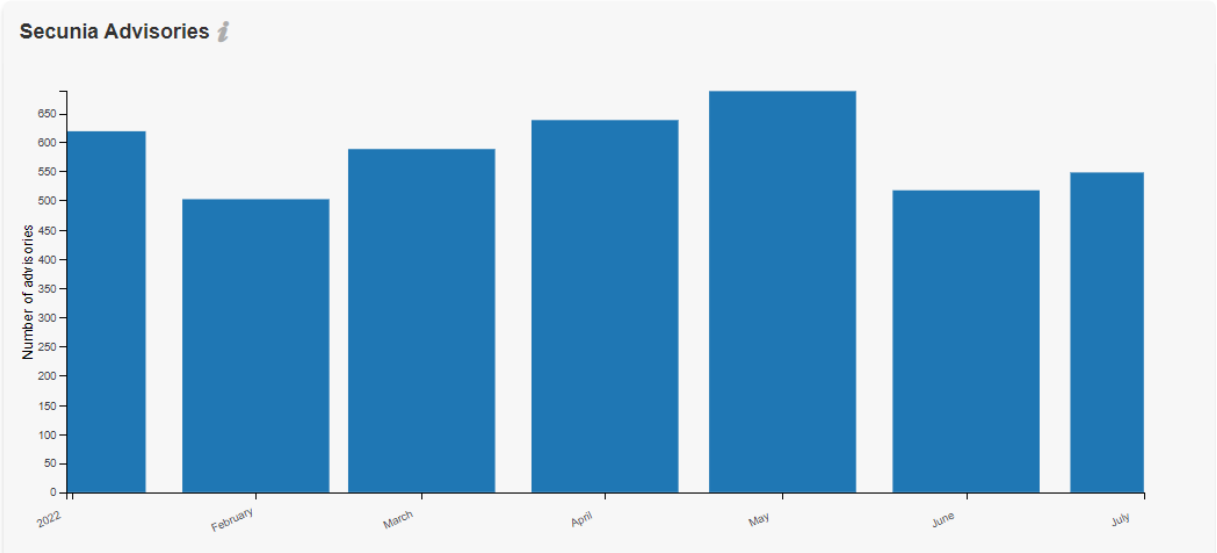
Last month we reported that **62.60%** of all Secunia Advisories had a Threat (exploits, malware, ransomware , etc.) associated with them, this month the number has been slightly lower to **64.23%**↓ , with an increase in the lower and medium criticality range.

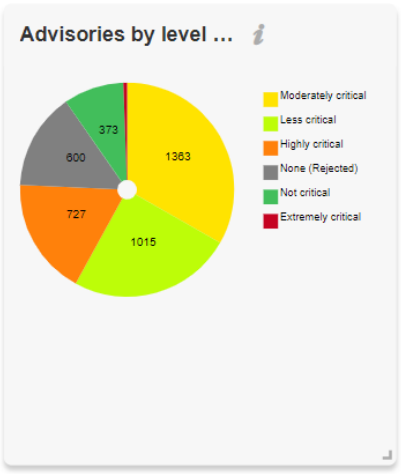
Using Threat Intelligence is going to help you with prioritizing what needs to be **patched** immediately.

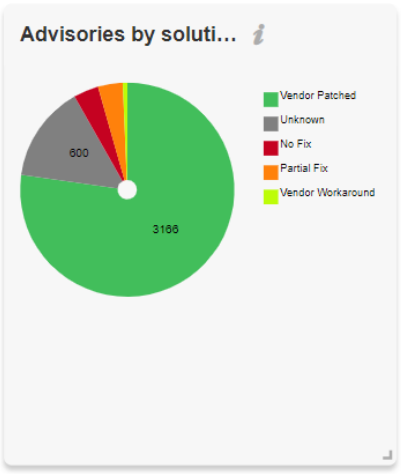
Software Vulnerability – and Patch Management is becoming more and more important.
Due to the ongoing Russia-Ukraine conflict , attacks on critical infrastructures in many countries are increasing.
Back in 2019 (just before Covid) patching was recommended within 30 days (or 14 days for CVSS score 7 or 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)

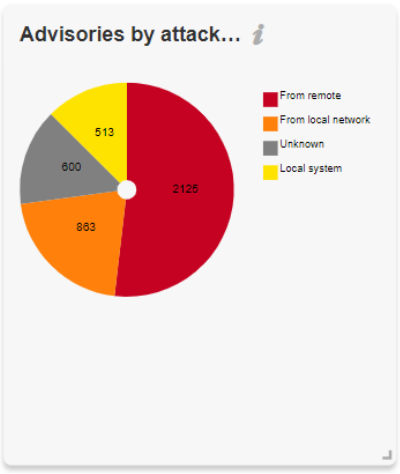
Year-to-date overview

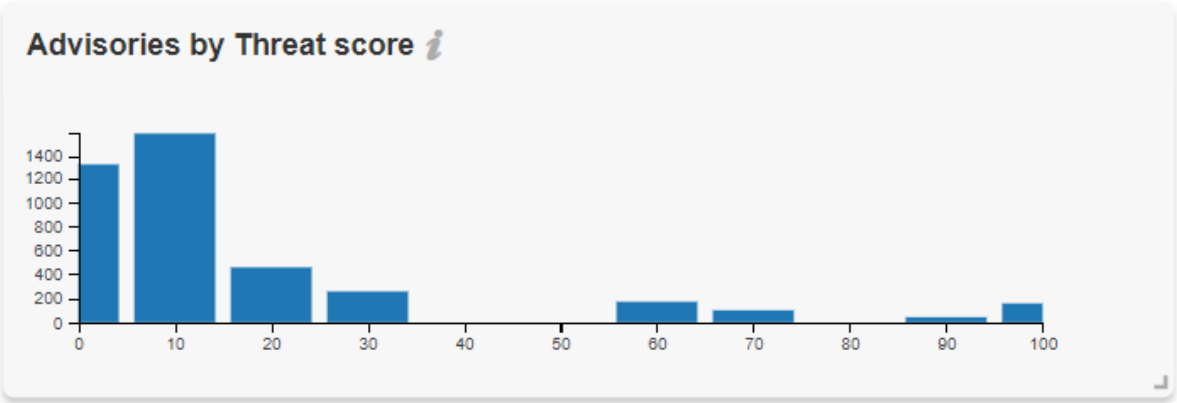
As of **July 31 2022**, the year-to-date total is at **4,101** Advisories ↑ which is higher than 2021 : **3,636** YTD Advisories)

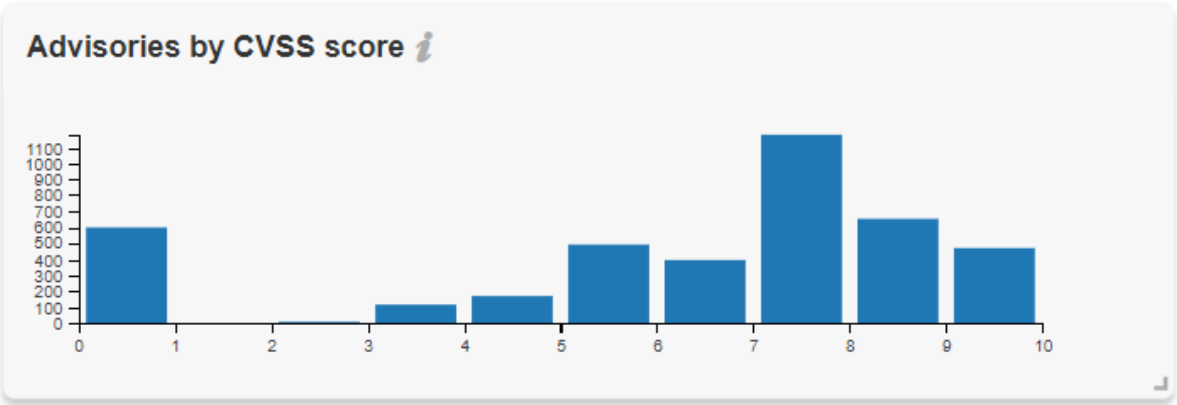












Monthly data

This month, a total of **517** ↓ (last month: **517**) advisories were reported by the Secunia Research Team.

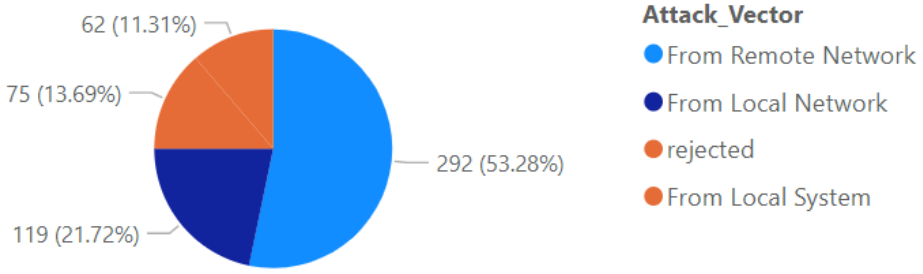
This month:	#	Change *(last month):*
Total # of advisories	**548**	↑ *(517)*
Unique Vendors	**93**	↑ *(76)*
Unique Products	**322**	↓ *(332)*
Unique Versions	**413**	↓ *(421)*
Rejected Advisories *	**75**	↓ *(77)*

↑ increased ↓ lower ↔ same

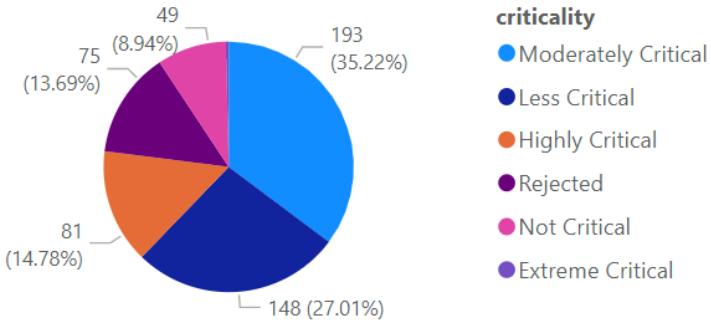
** **75** advisories have received the "rejected" status which means in general that leveraging it would require one or more violations of security best practices (e.g., product not securely configured or not used securely) or that it was "too weak of a gain" (e.g., administrative, local users already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



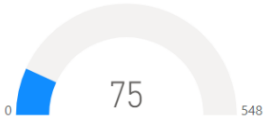
Advisories per day

Below an overview of the daily advisory count.

Year	Month	Day	# of Advisories
2022	July	1	28
2022	July	4	14
2022	July	5	11
2022	July	6	47
2022	July	7	31
2022	July	8	15
2022	July	11	16
2022	July	12	27
2022	July	13	42
2022	July	14	35
2022	July	15	31
2022	July	18	14
2022	July	19	13
2022	July	20	63
2022	July	21	33
2022	July	22	7
2022	July	25	26
2022	July	26	26
2022	July	27	26
2022	July	28	14
2022	July	29	29
Total			**548**

Rejected advisories

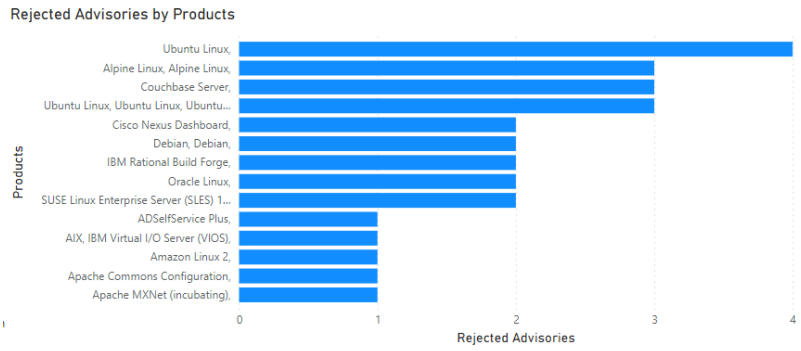
There are many vulnerabilities posted to the National Vulnerability Database (NVD) by a lot of people and companies. They are not always valid, assigned a proper criticality, and in some cases, a vulnerability may be legitimate but not afford the attacker any benefit.

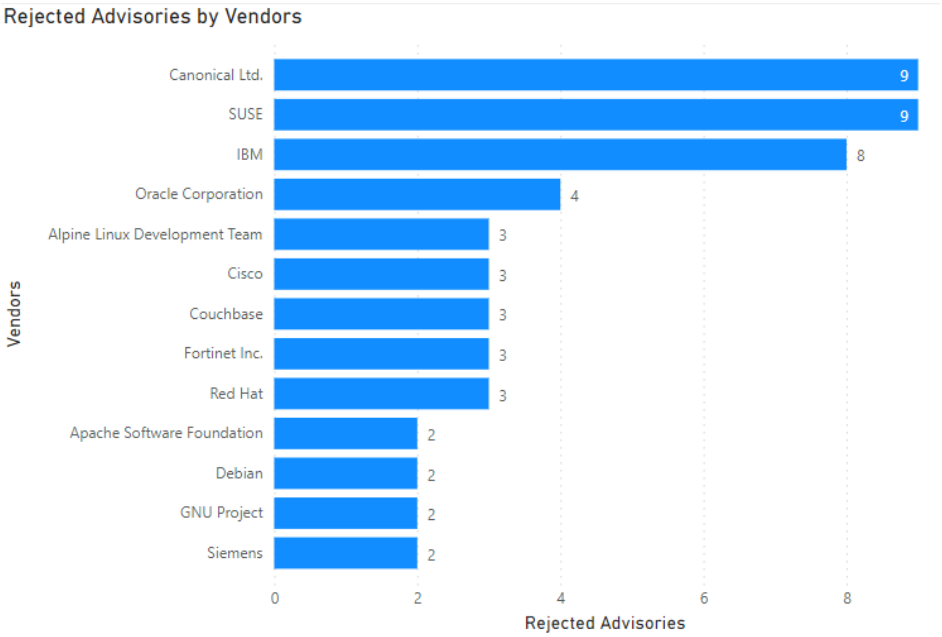


The Secunia Research team at Flexera evaluates vulnerabilities from hundreds of sources, rescores them when necessary and even rejects vulnerabilities not worth your attention. Rejection Advisories help you to reduce the volume of vulnerabilities to be mitigated by helping you focus only on those that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

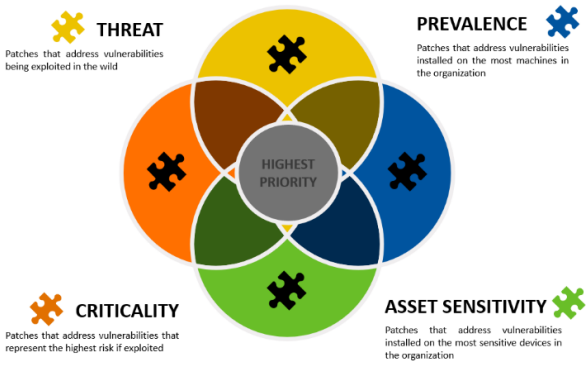
- What systems would result in the most risk if compromised?
- Is it a high-risk device? Patch.

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.

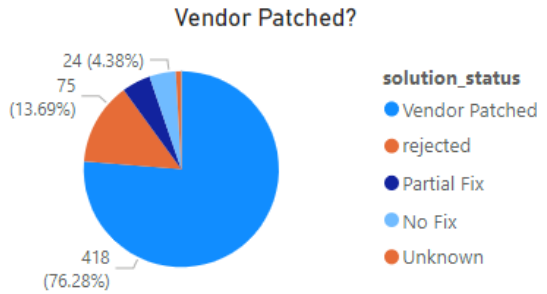
criticality	avg threat score x # of advisories
Moderately Critical	2,760.00
Highly Critical	2,240.00
Less Critical	1,690.00
Not Critical	517.00
Extreme Critical	124.00
Total	**7,331.00**

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).

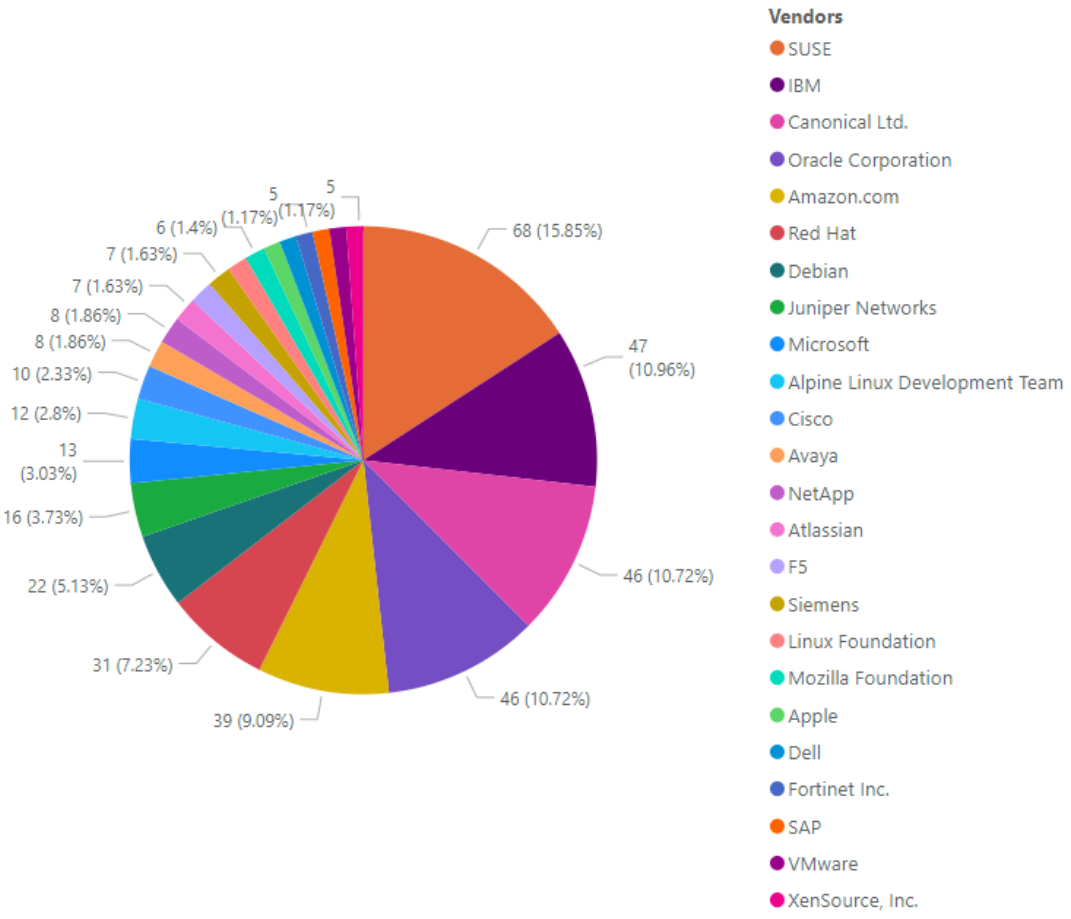


Previous month : 394 *Vendor Patched* (76.21%)
This Month : **418** Vendor Patched (**76.28%**)

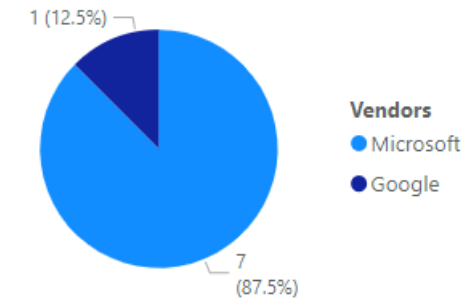
Vendor view

Top vendors with the most advisories

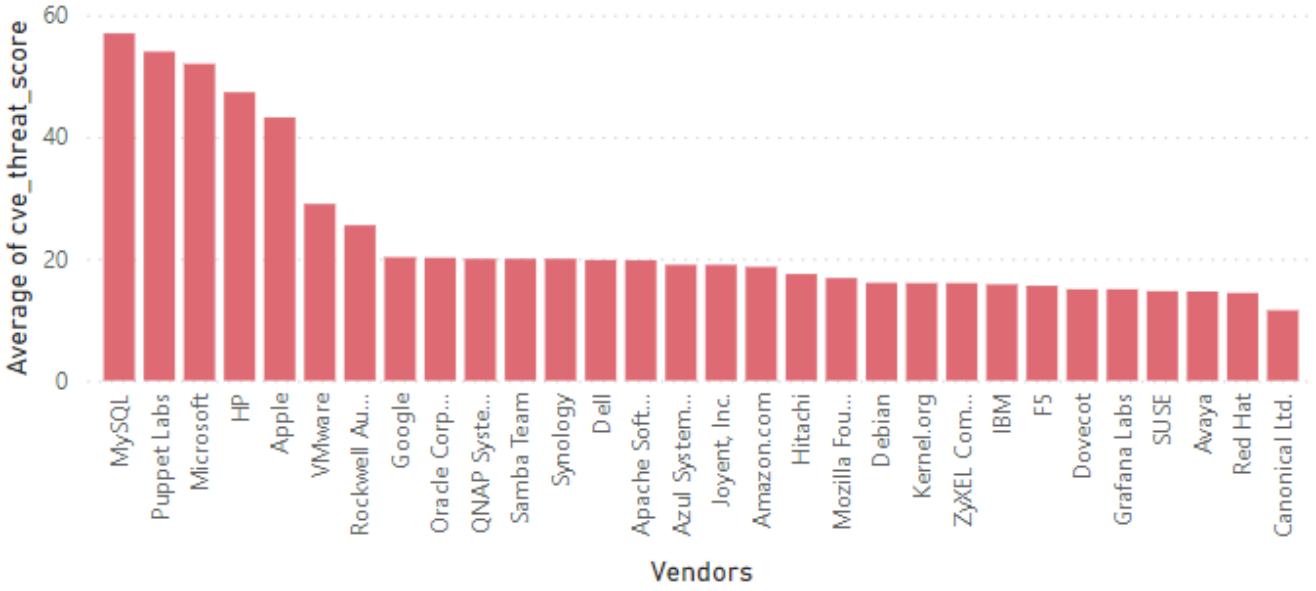
Top Vendors with most advisories



Top vendors with zero-day

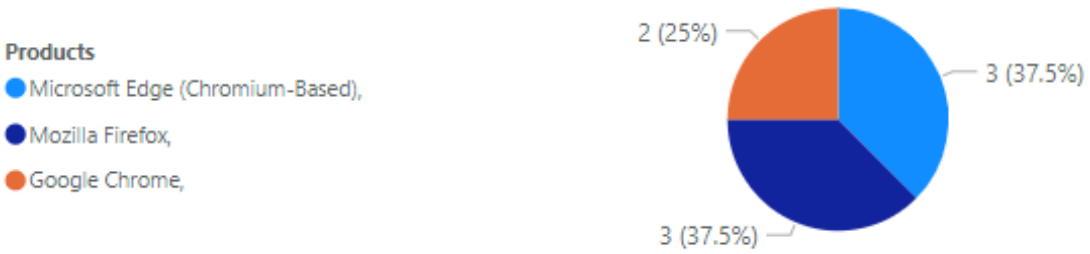


Top Vendors with highest average threat score



Browser-related advisories

Advisories per browser

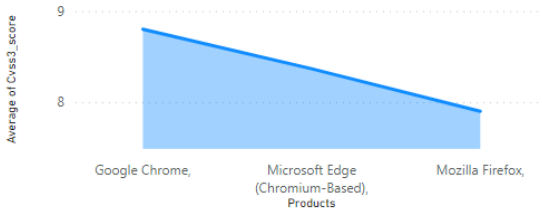


Browser zero-day vulnerabilities

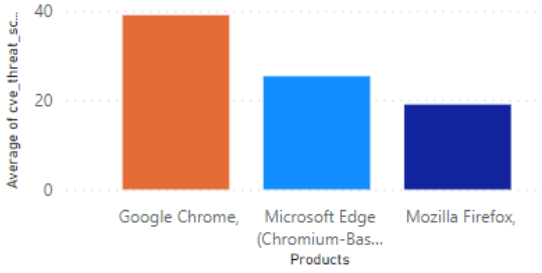
Count of Advisories	Products	Advisories

No Browser Zero-Day Advisories

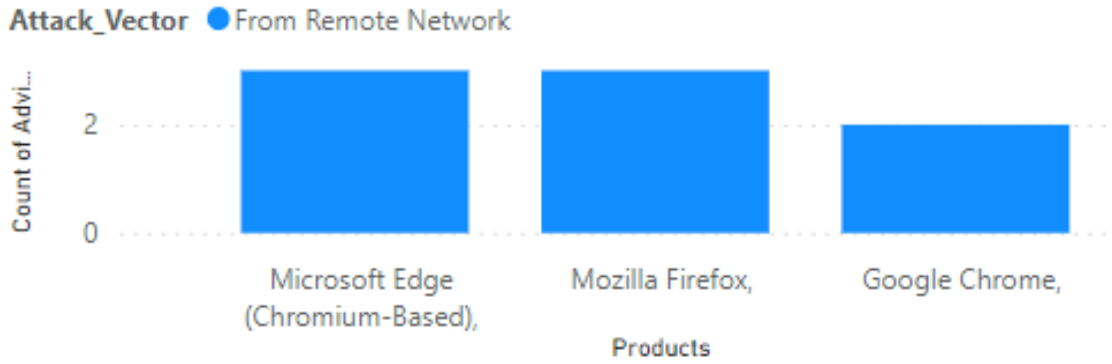
Average CVSS (criticality) score per browser



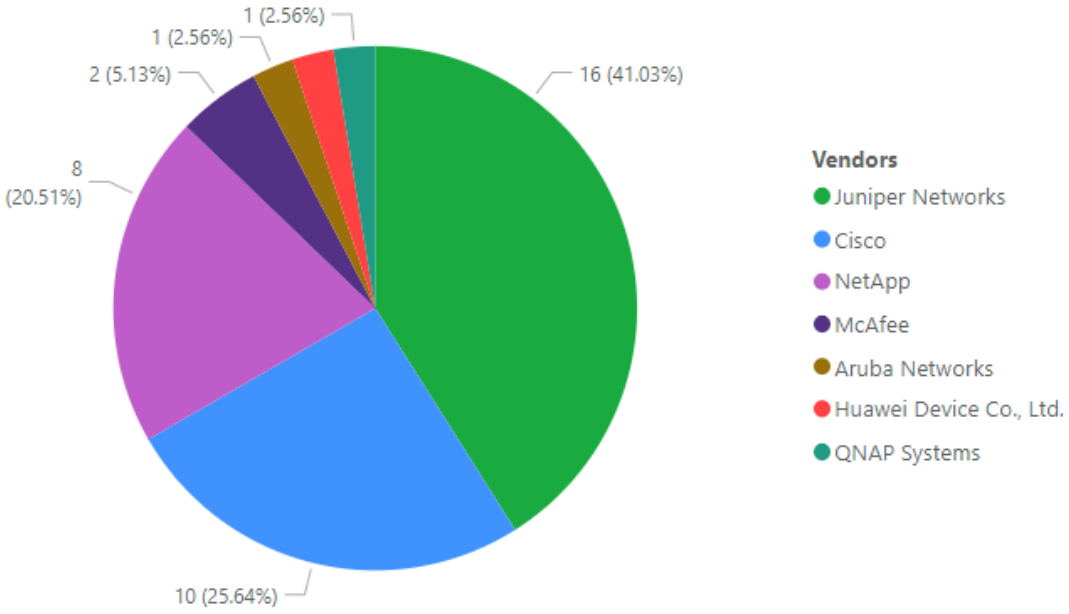
Average threat score per browser



What's the Attack Vector ?



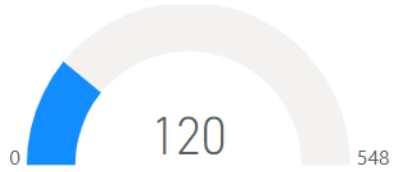
Networking related advisories



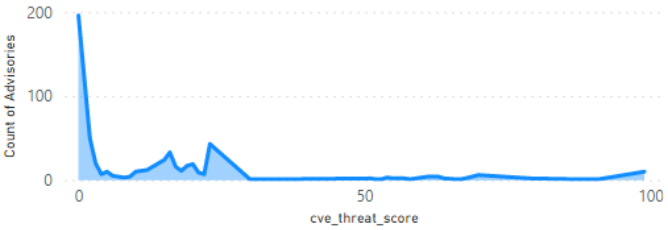
Threat intelligence

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+)	**352**↑(334*)*	64.23%
SAIDs with no threat score (=0)	**196**↑*(183)*	35.77%

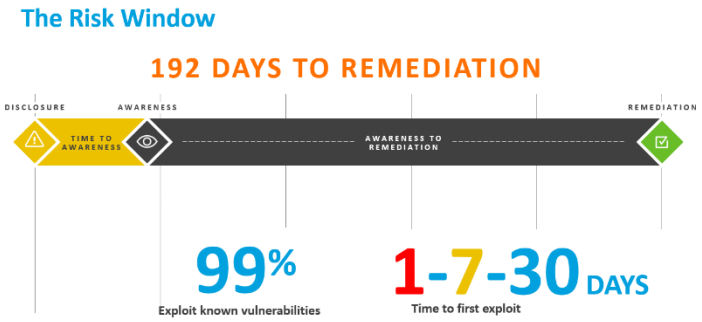
SAID: Secunia Advisory Identifier

Range	Score	*Last month*
Medium-range threat score SAIDs (13-23)	**179** ↑	***(163)***
Low-range threat score SAIDs (1-12)	**125** ↑	***(140)***
Critical-range threat score SAIDs (45-70)	32 ↑	*(20)*
Very critical threat score SAIDs (71-99)	14 ↑	*(11)*
High-range threat score SAIDs (24-44)	2 ↑	*(0)*

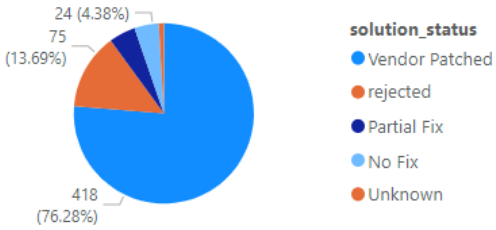
Patching

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).

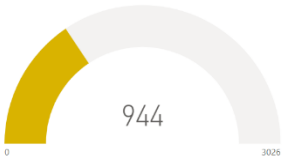


Vulnerabilities that are vendor patched



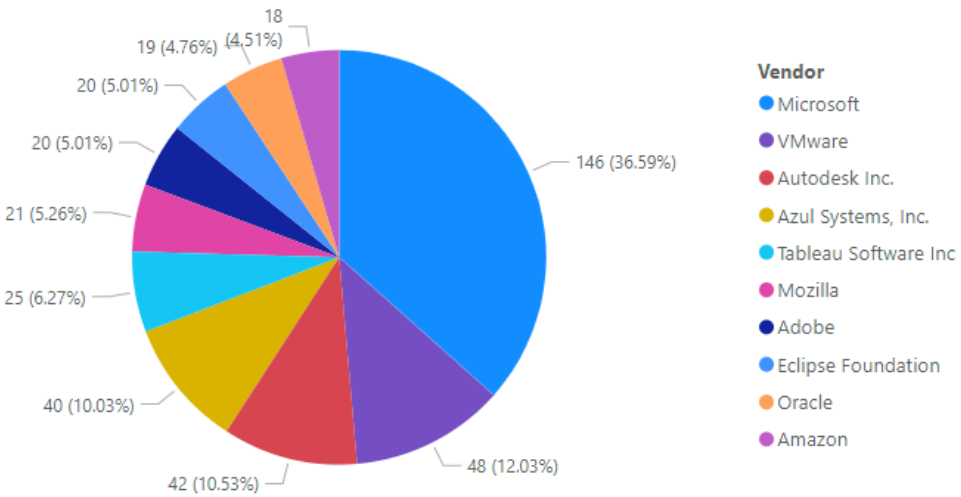
Flexera's Vendor Patch Module (VPM) statistics

Flexera has the largest third-party patch catalog **(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)



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