MONTHLY VULNERABILITY INSIGHTS

Based on Data from Secunia Research

SEPTEMBER 2021

Flexera

Inform IT. Transform IT.™

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 be 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 a consistent and standard processes, which have been refined over the years.

Whenever a new vulnerability is reported, it is verified and a Secunia Advisory is published. A Secunia Advisory provides details including description, risk rating, impact, attack vector, recommended mitigation, credits, references and more for the vulnerability – 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

We've seen a minor increase again in vulnerabilities and threats for **September 2021**.
is something we also see in the total advisories : 461 ↑ (was: 459) .

Unfortunately the **Extreme Critical Vulnerabilities** are back (↑14) after none were reported last month.

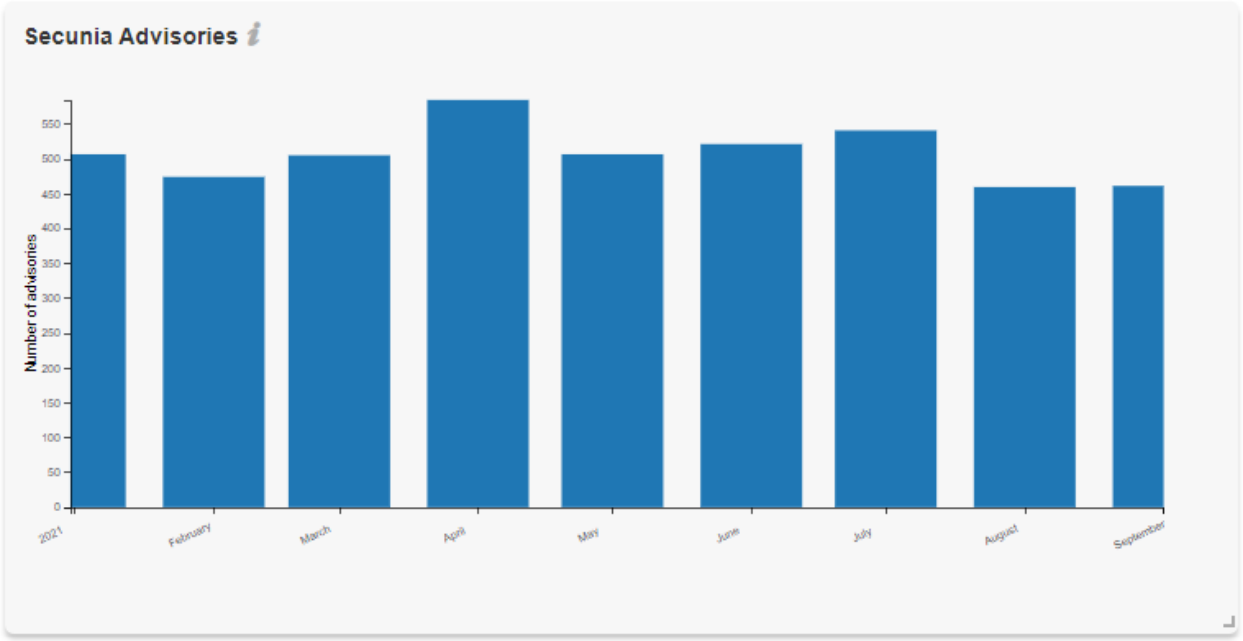
SAID	Release date	Modified date	Title	Criticality	Zero Day	Solution status	Where	CVSS Score	Threat Score
SA104329	2021-09-30	2021-09-30	Google Chrome Multiple Vulnerabilities		Yes	Vendor Patched	From remote	8.8 v3	3
SA104321	2021-09-27	2021-09-27	Microsoft Edge (Chromium-based) Multiple Vulnerabilities		Yes	Vendor Patched	From remote	8.8 v3	79
SA104204	2021-09-24	2021-09-24	Google Chrome Arbitrary Code Execution Vulnerability		Yes	Vendor Patched	From remote	8.8 v3	79
SA104302	2021-09-23	2021-09-23	Apple iOS Multiple Arbitrary Code Execution Vulnerabilities		Yes	Vendor Patched	From remote	8.8 v3	99
SA104124	2021-09-15	2021-09-15	Microsoft Windows Server 2012 / Windows RT 8.1 / 8.1 Multiple Vulnerabilities		Yes	Vendor Patched	From remote	8.8 v3	99
SA104125	2021-09-15	2021-09-15	Microsoft Windows Server 2008 / Windows 7 Multiple Vulnerabilities		Yes	Vendor Patched	From remote	8.8 v3	99
SA104120	2021-09-14	2021-09-21	Microsoft Windows Server 2019 / 2016 / Windows 10 Multiple Vulnerabilities		Yes	Vendor Patched	From remote	8.8 v3	99
SA104058	2021-09-14	2021-09-16	Microsoft Edge (Chromium-Based) Multiple Vulnerabilities		Yes	Vendor Patched	From remote	9.8 v3	99
SA102675	2021-09-14	2021-09-14	Google Chrome Multiple Vulnerabilities		Yes	Vendor Patched	From remote	9.8 v3	99
SA104057	2021-09-13	2021-09-15	Apple Safari Arbitrary Code Execution Vulnerability		Yes	Vendor Patched	From remote	8.8 v3	34
SA103448	2021-09-13	2021-09-22	Apple iOS Multiple Vulnerabilities		Yes	Vendor Patched	From remote	8.8 v3	99
SA103845	2021-09-13	2021-09-22	Apple macOS Big Sur Multiple Vulnerabilities		Yes	Vendor Patched	From remote	8.8 v3	99
SA103419	2021-09-13	2021-09-21	Apple macOS Catalina Multiple Vulnerabilities		Yes	Vendor Patched	From remote	8.8 v3	99
SA103992	2021-09-08	2021-09-16	Microsoft Windows Server 2022 Multiple Vulnerabilities		Yes	Vendor Patched	From remote	8.8 v3	99

More news:
Microsoft disclosed details of a targeted phishing campaign that leveraged a now-patched zero-day flaw in its MSHTML platform using specially crafted Office documents to deploy **Cobalt Strike Beacon** on compromised Windows systems. (CVE-2021-40444)
Cobalt Strike Beacon not only found on the Windows platform but also Linux platform, focusing on government, telco, IT and Finance organizations around the world.

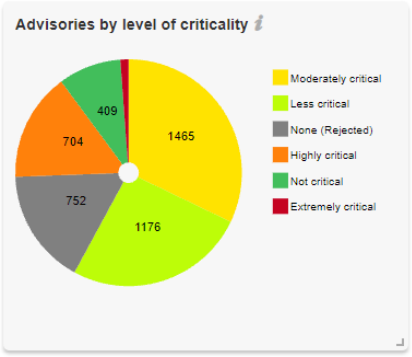
New **ATP Hacker Group** are actively attacking hotels and governments around the world , exploiting Vulnerabilities in **Sharepoint** and **Oracle Opera** in addition to the older ProxyLogon Vulnerability in MS Exchange (March'21)

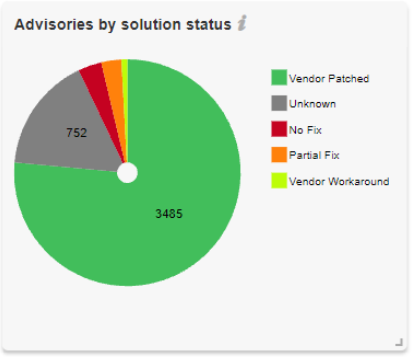
Year to Date Overview

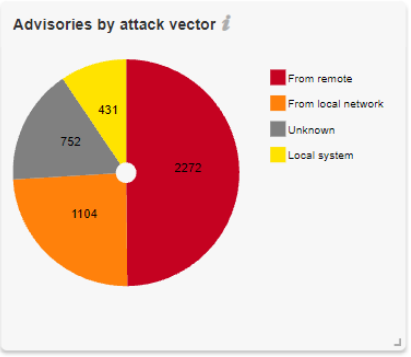
As of **September**, the year-to-date total is at **4556** Advisories ↓ which is lower than 2020 : **5265** YTD Advisories)



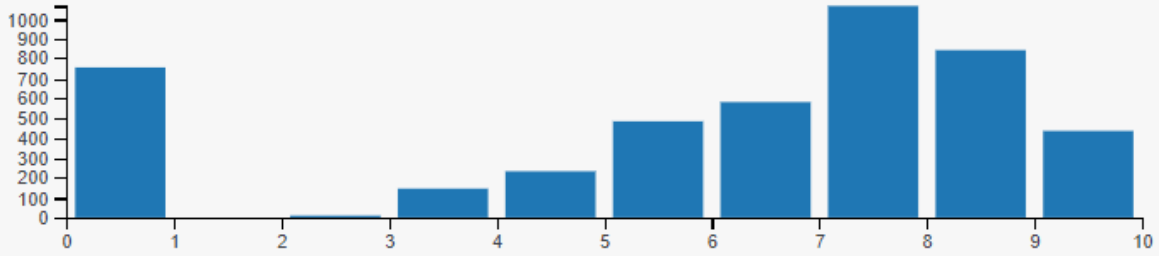
A relatively stable year compared with last year where we've seen spikes in April'20 and July'20.



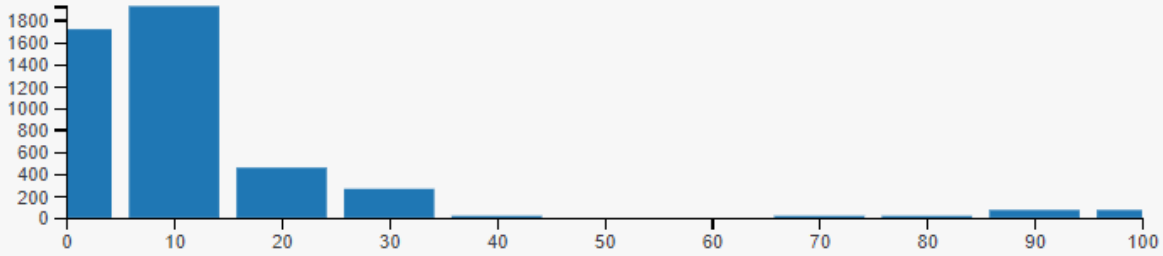




Advisories by CVSS score



Advisories by Threat score



Monthly Data

This month, a total of **461** ↑ advisories were reported by the Secunia Research Team.

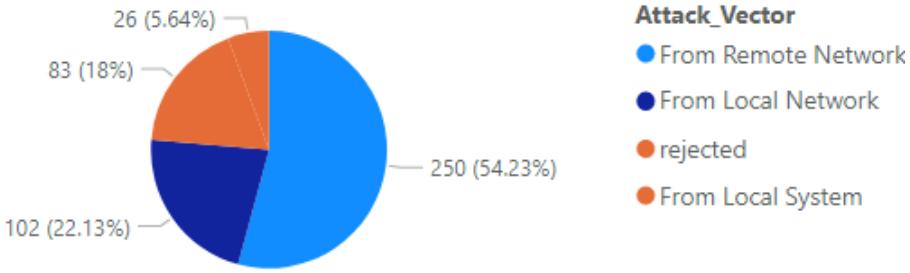
This Month:	#	Change *(last month):*
Total # of advisories	**461**	↑ *(559)*
Unique Vendors	**72**	↓ *(75)*
Unique Products	**307**	↑ *(268)*
Unique Versions	**414**	↑ *(338)*
Rejected Advisories *	**83**	↑ *(57)*

↑ increased ↓lower ↔ same

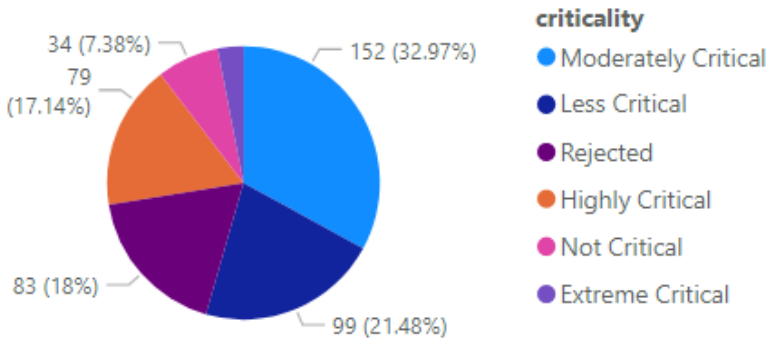
** **83** advisories have received the "rejected" status which means in general that leveraging it would require one or more violations of security best practices (e.g. product not securely configured or not used securely) or that it was "too weak of a gain" (e.g. administrative, local users already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



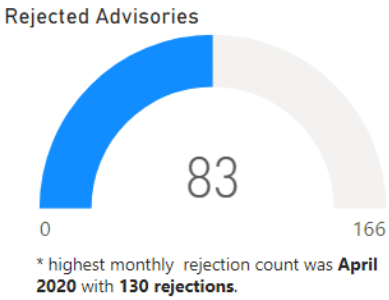
Advisories per Day

Below an overview of the daily advisory count.

Year	Month	Day	# of Advisories
2021	September	1	33
2021	September	2	23
2021	September	3	14
2021	September	6	4
2021	September	7	16
2021	September	8	38
2021	September	9	31
2021	September	10	16
2021	September	13	14
2021	September	14	32
2021	September	15	40
2021	September	16	15
2021	September	17	11
2021	September	20	14
2021	September	21	31
2021	September	22	26
2021	September	23	36
2021	September	24	15
2021	September	27	15
2021	September	28	18
2021	September	29	6
2021	September	30	13
Total			**461**

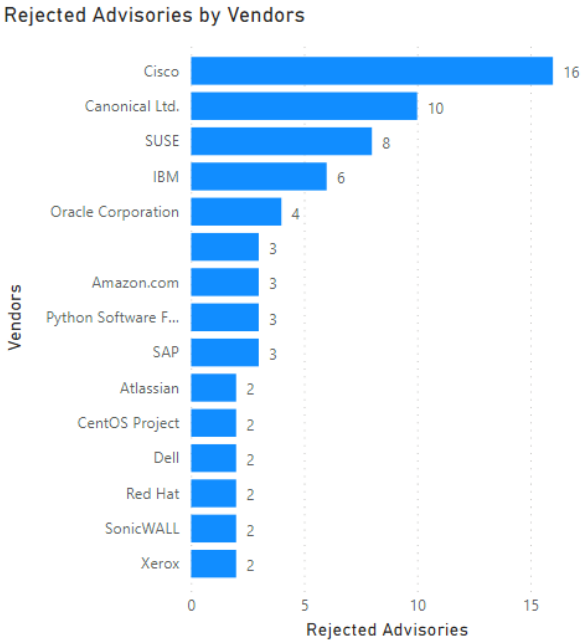
Rejected Advisories

There are a lot of vulnerabilities posted to the National Vulnerability Database (NVD), by a lot of people and companies. They are not always valid, they are not always 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 is depending 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:

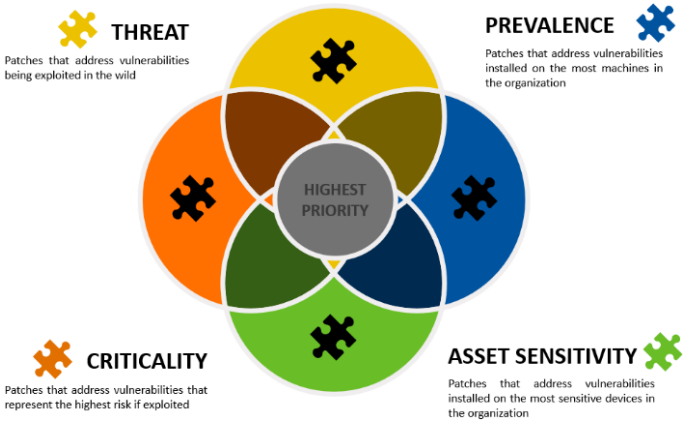
- What systems would result in the most risk if compromised?
- Is it a high-risk device? Patch!

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!



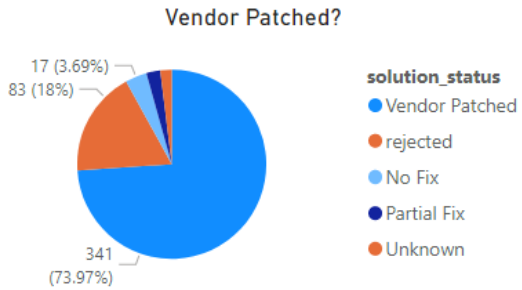
How do we know that more insights / data is needed?

Focusing on vulnerabilities with CVSS 7 or higher would address about 50% of exploits. Most exploits are CVSS scored between 4 and 7. Focusing on vulnerabilities for the top 20 vendors would address only about 20%

criticality	avg threat score x # of advisories
Moderately Critical	2,275.00
Extreme Critical	1,185.00
Highly Critical	1,133.00
Less Critical	663.00
Not Critical	120.00
Total	**5,376.00**

Take away 1:

Critical vulnerabilities do not necessarily those present the most risk.
Leverage Threat Intelligence to better prioritize what demands your most urgent attention.

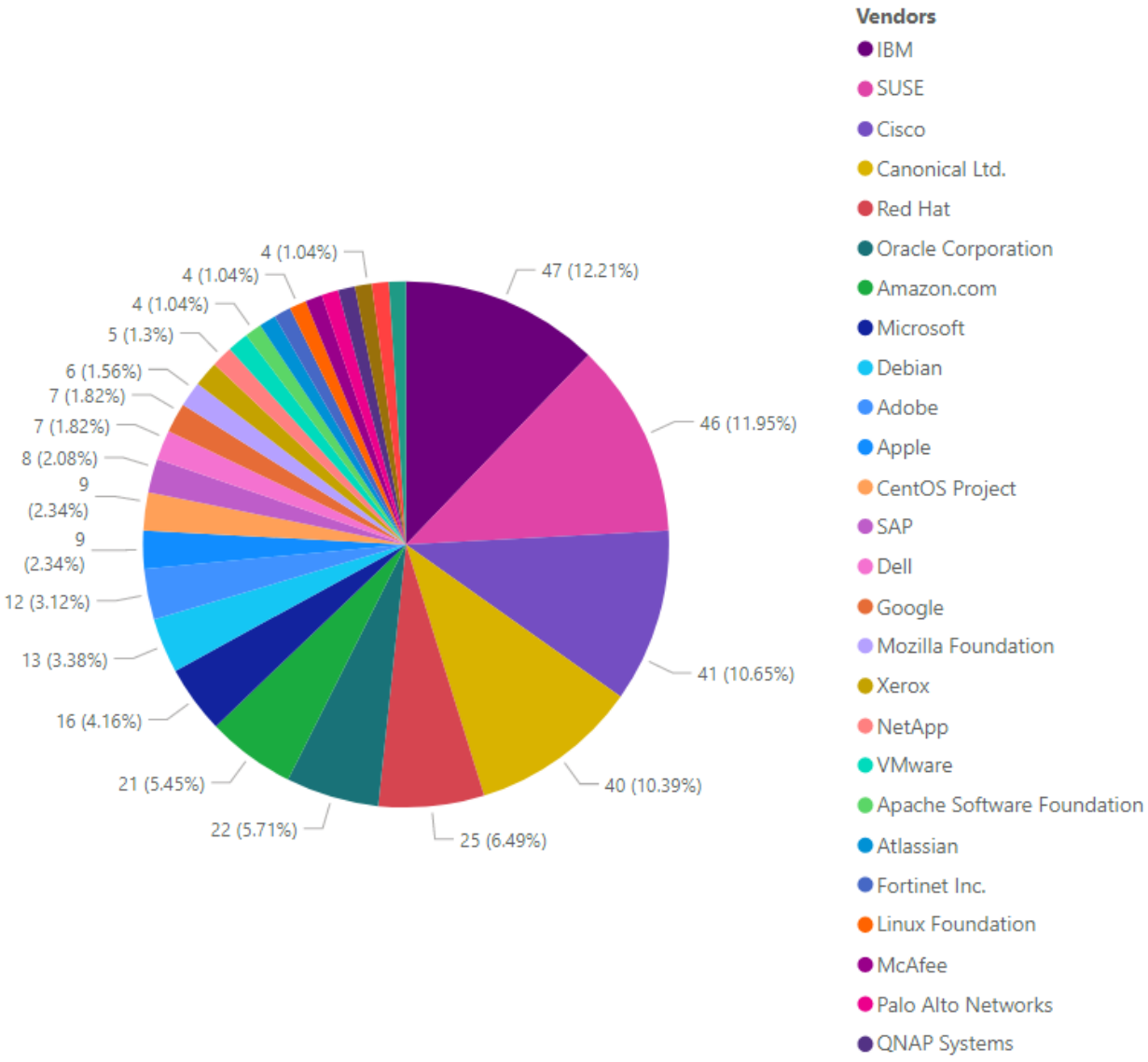


Take away 2:

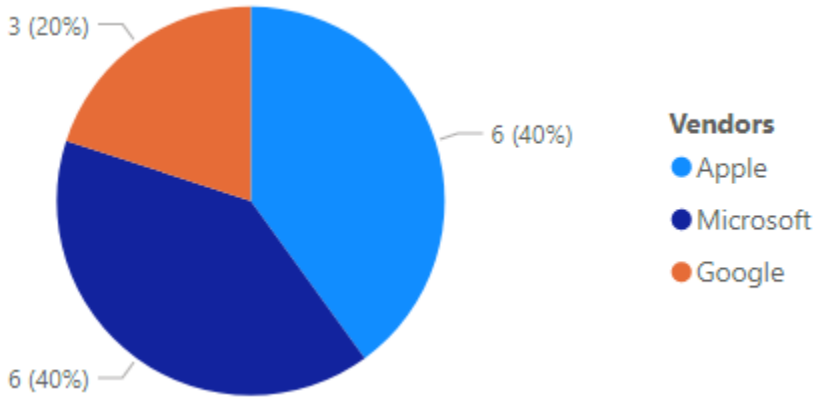
Most vulnerabilities have a Patch available (typically within 24h after disclosure).

Vendor View

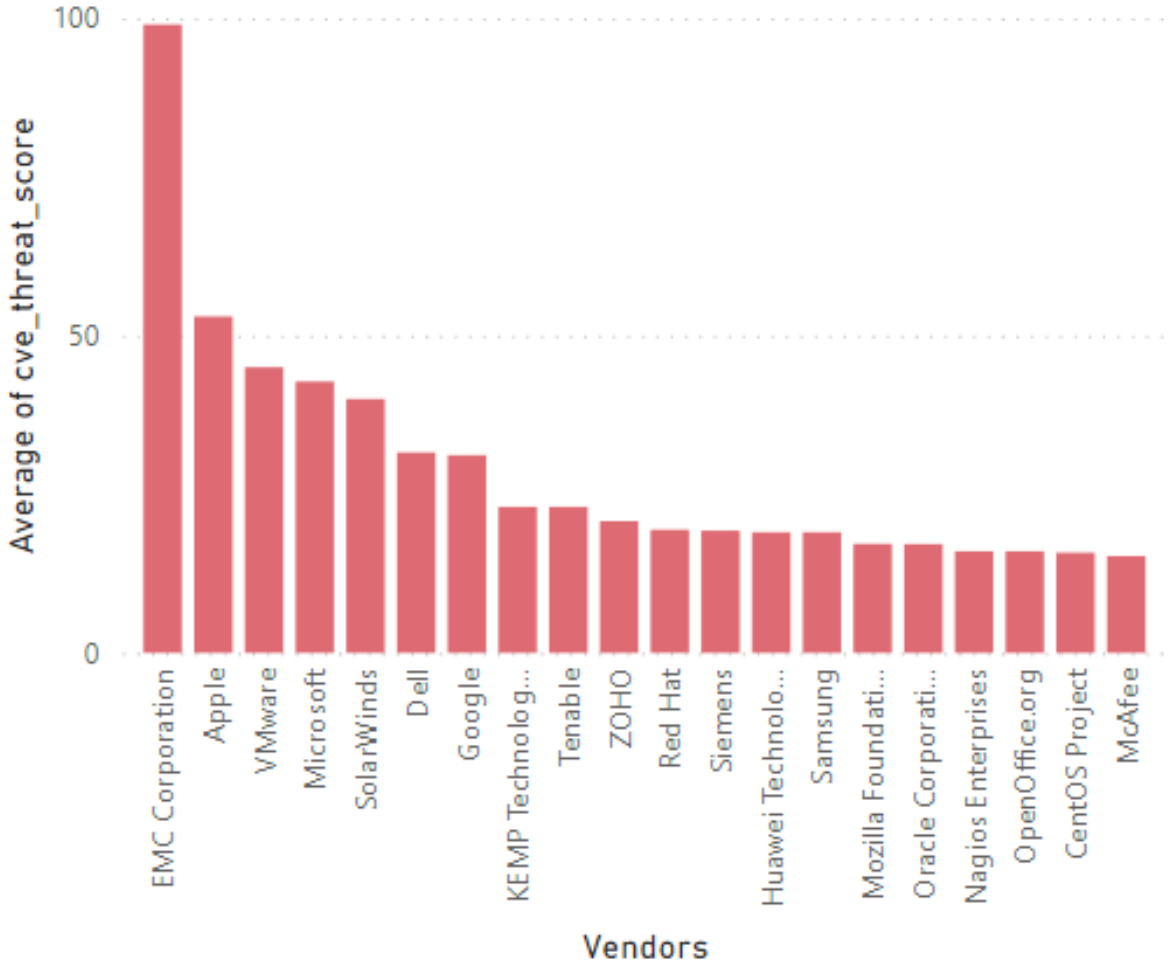
Top Vendors with most Advisories



Top Vendors with Zero-Day

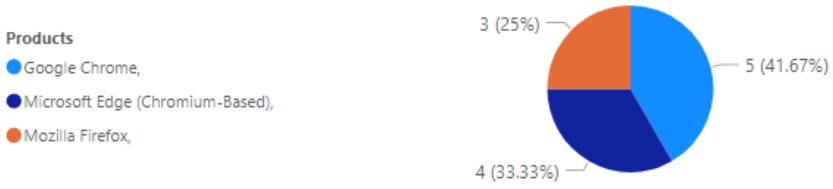


Top Vendors with highest average threat score



Browser Related Advisories

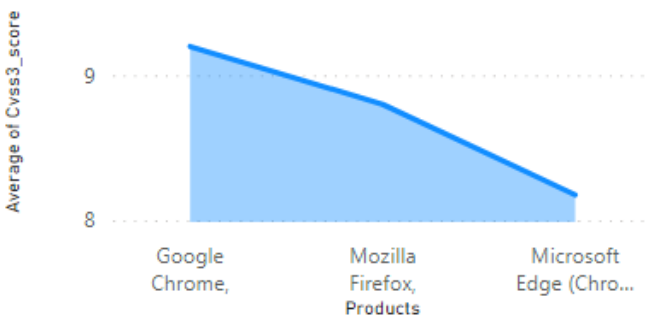
Advisories per browser



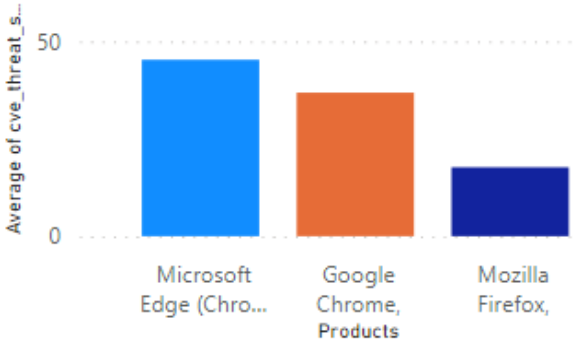
Browser Zero-Day vulnerabilities

Count of Advisories	Products	Advisories
1	Google Chrome,	SA102675
1	Google Chrome,	SA104204
1	Google Chrome,	SA104329
1	Microsoft Edge (Chromium-Based),	SA104058
1	Microsoft Edge (Chromium-Based),	SA104321
5		

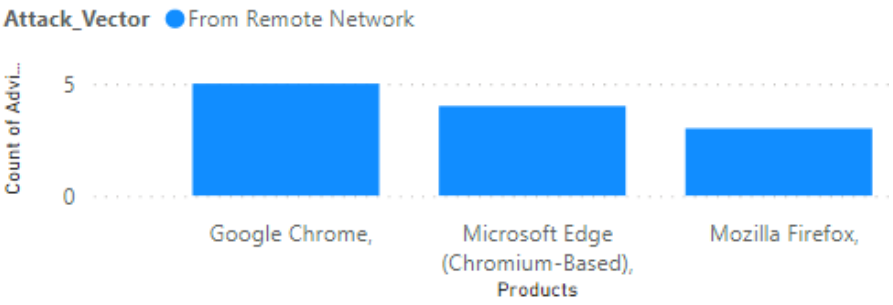
Average CVSS (Criticality) Score per Browser



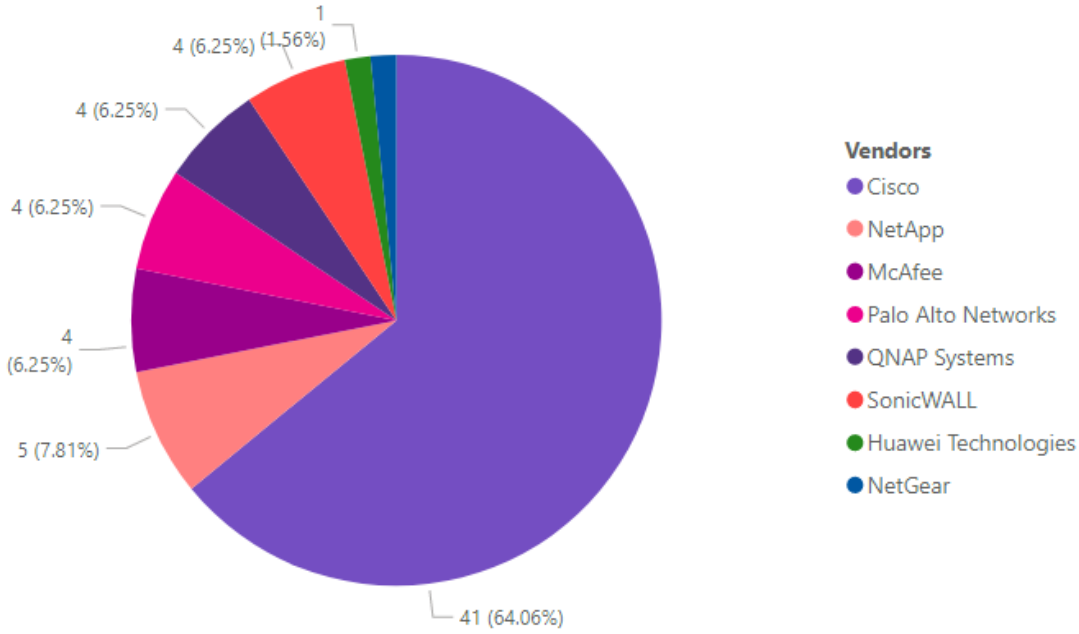
Average Threat Score per Browser



What's the Attack Vector ?



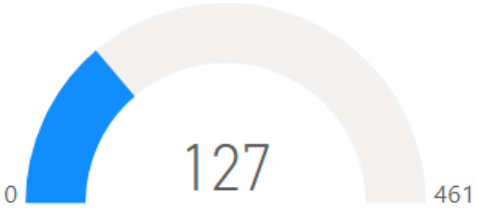
Networking Related Advisories



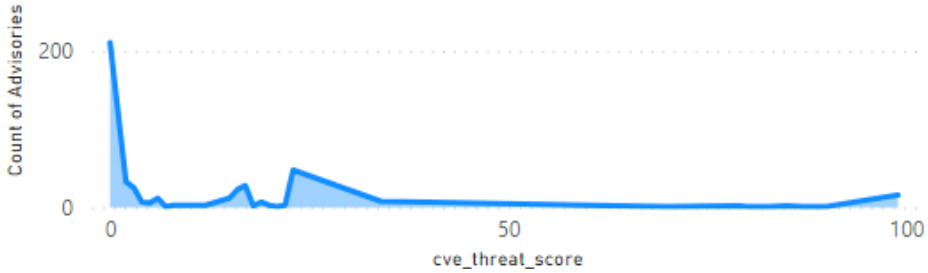
Threat Intelligence

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	250↓*(261)*	54.23%
SAIDs with no Threat Score	211↑*(198)*	45.77%

SAID: Secunia Advisory Identifier

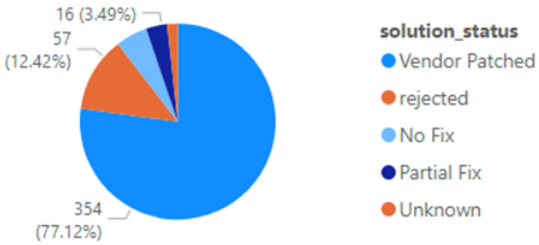
Range	Score	%
Medium-Range Threat Score SAIDs (13-23)	127 ↓	(27.55%)
Low-Range Threat Score SAIDs (1-12)	90 ↓	(19.52%)
High-Range Threat Score SAIDs (24-44)	8 ↓	(1.74%)
Very Critical Threat Score SAIDs (71-99)	24 ↑	(5.21%)
Critical-Range Threat Score SAIDs (45-70)	1 =	(0.22%)

Patching

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

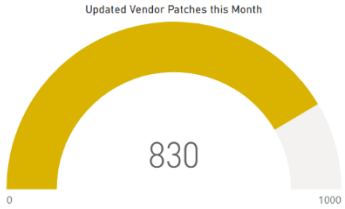
The challenge remains that organizations do not have full visibility or awareness when a vulnerability is disclosed (Time to Awareness) . Another big challenge is the time to Remediation (the time from having this information, correlating that with your environment and initiating the process to get the software updated to a secure version).

Vulnerabilities that are Vendor Patched



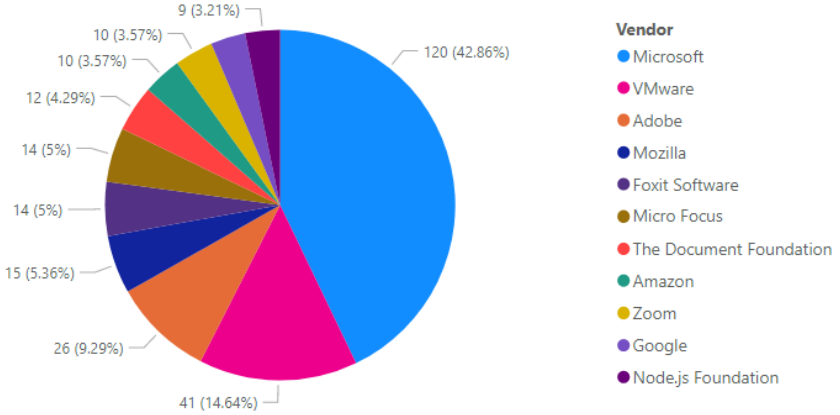
Flexera's Vendor Patch Module (VPM) statistics

Flexera has the largest third-party Patch Catalog **(~2500)** in the world. This helps customers to 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

(Patches per vendor)



About Flexera

Flexera delivers IT management solutions that enable Enterprises to accelerate and multiply the return on their technology investments. We help organizations ***inform their IT*** with total visibility into their complex hybrid ecosystems, providing the IT insights that fuel better-informed decisions. And we help them ***transform their IT*** with tools that allow IT leaders to rightsize across all platforms, reallocate spend, reduce risk and chart the most effective path to the cloud.

Our category-leading technology value optimization solutions are delivered by more than 1,300 passionate team members helping more than 50,000 customers achieve their business outcomes. To learn more, visit **flexera.com**