MONTHLY VULNERABILITY INSIGHTS

Based on Data from Secunia Research

JANUARY 2022

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

Total advisories: **620** ↑ (last month: **572**)

With an increase in advisories this month, we seen a decrease in the number of vendors with advisories.
Top 3 vendors with most vulnerabilities reported this month: **IBM** (72), **Oracle** (69) and **Amazon**(52)

It was a hectic holiday month, with the Log4j vulnerability haunting many organizations. However it didn't stop there and the Log4j vulnerabilities are still having an effect in the **January** report with continued attacks exploiting Apache Log4j vulnerabilities. You would think that software companies have a good grip on their components they use. But the truth is that almost 45 days later, vendors are disclosing that their products were not properly sanitized and vulnerabilities were still exploitable.(SolarWinds- Serv-U, VMWare Horizon, etc.)

Flexera's SVM customers have the ability to detect log4j-core*.jar files installed on host machines and can expect to see:

- the CVE associated with the vulnerability and its variants (as published by a trusted source)
- Threat Intelligence information associated with the vulnerability
- Patches you can publish to remediate this vulnerability and its variants.

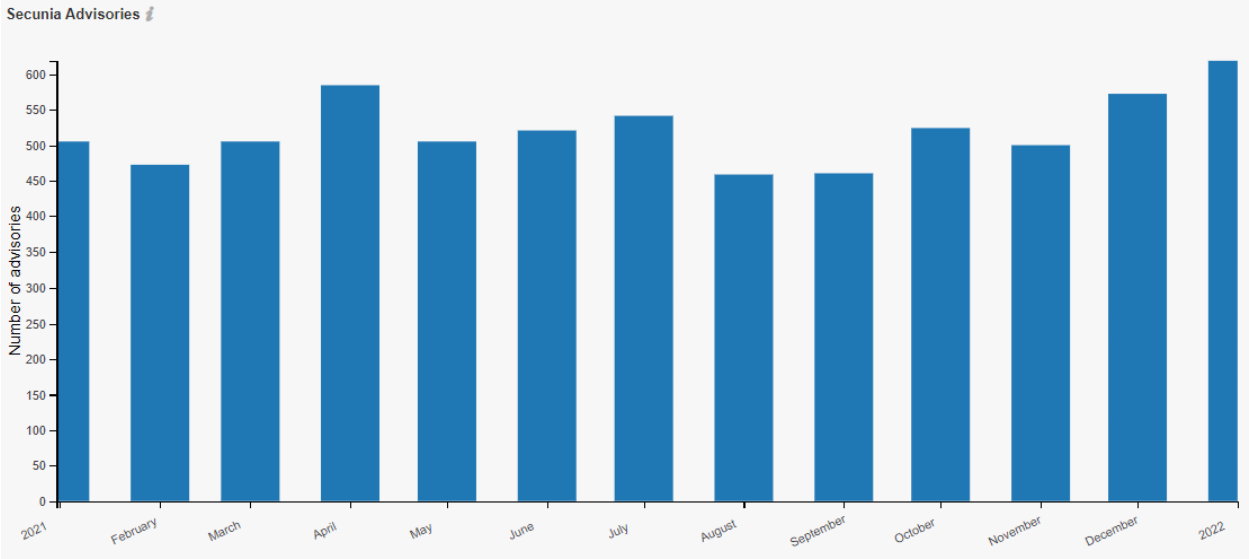
More information about identifying Apache Log4j using Flexera's SVM can be found here

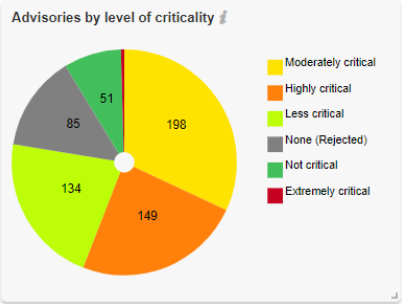
Other news:

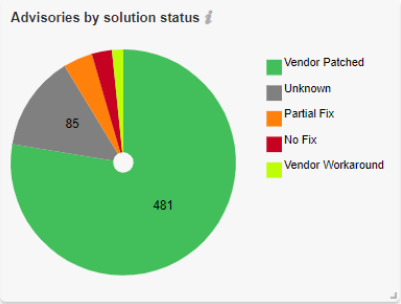
- **Apple** was in January the only vendor with a **Zero-Day** Vulnerability (**CVE-2022-22587)**
- **Cisco** has patched a pair of critical vulnerabilities for **StarOS**
- **CISA**'s known exploited vulnerabilities catalog reported 12 critical vulnerabilities that need to be fixed in February. The affected vendors are : **October CMS, Nagios, Aviatrix, Microsoft, F5, VMWare, SolarWinds, Apple, SonicWall**

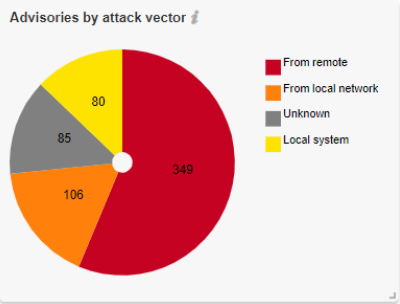
Year to Date Overview

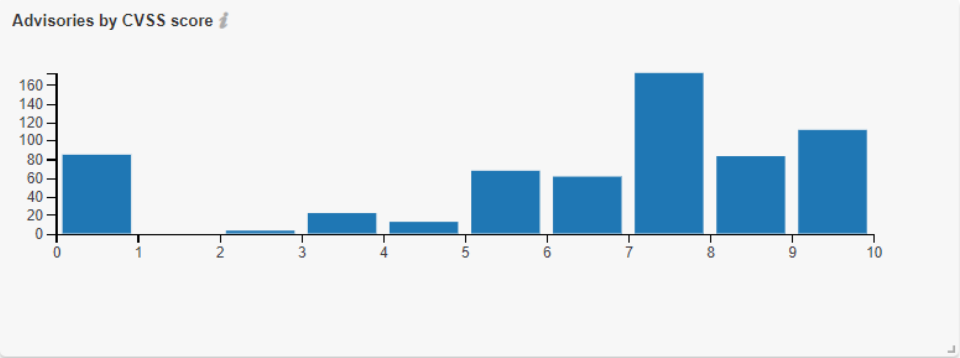
As of **February 1. 2022** , the year-to-date total is at **620** Advisories ↑ which is higher than in 2021 : **506** YTD Advisories)
620 advisories is the highest monthly count since October 2020. **The trend is upwards.**

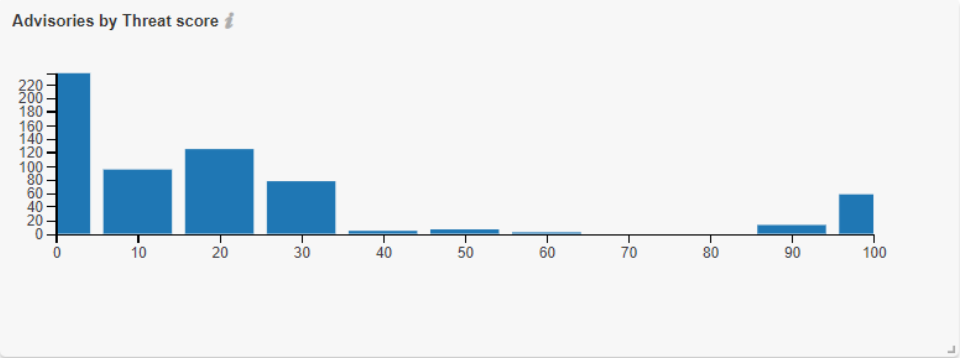












Monthly Data

This month, a total of **620** ↑ advisories were reported by the Secunia Research Team.

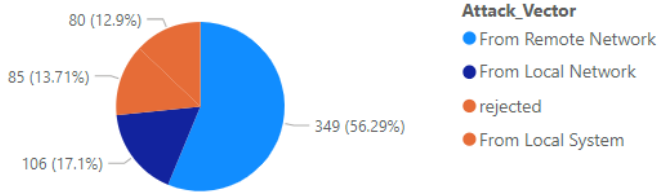
This Month:	#	Change *(last month):*
Total # of advisories	**620**	↑ *(572)*
Unique Vendors	**80**	↓ *(102)*
Unique Products	**383**	↓ *(387)*
Unique Versions	**471**	↑ *(467)*
Rejected Advisories *	**85**	↓ *(89)*

↑ increased ↓ lower ↔ same

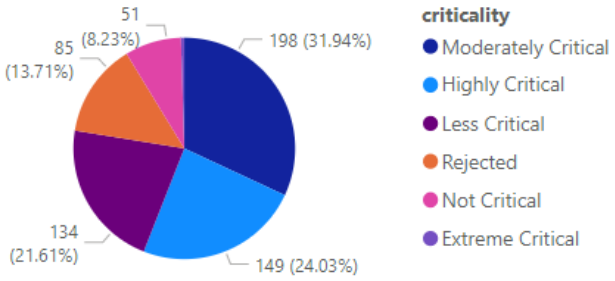
** **85** advisories have received the "rejected" status which means in general that leveraging it would require one or more violations of security best practices (e.g. product not securely configured or not used securely) or that it was "too weak of a gain" (e.g. administrative, local users already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



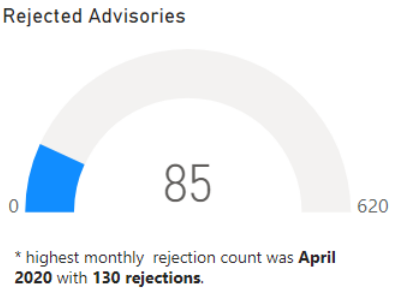
Advisories per Day

Below an overview of the daily advisory count.

Year	Month	Day	# of Advisories
2022	January	4	23
2022	January	5	15
2022	January	6	29
2022	January	7	6
2022	January	10	22
2022	January	11	35
2022	January	12	61
2022	January	13	43
2022	January	14	14
2022	January	17	11
2022	January	18	35
2022	January	19	96
2022	January	20	27
2022	January	21	17
2022	January	22	4
2022	January	24	24
2022	January	25	21
2022	January	26	32
2022	January	27	36
2022	January	28	18
2022	January	31	51
Total			**620**

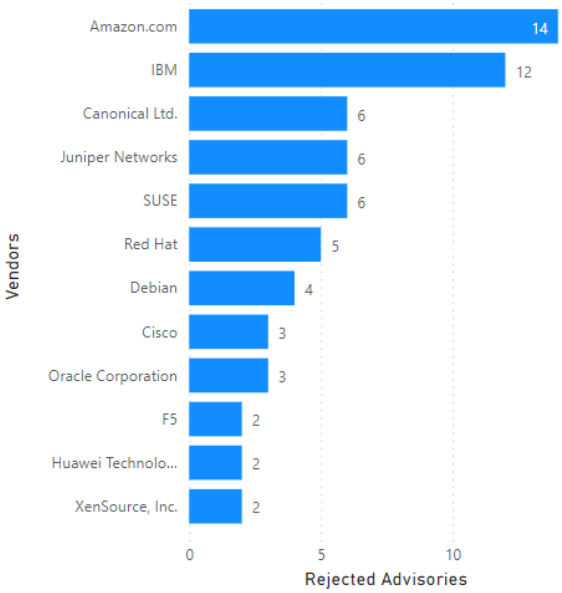
Rejected Advisories

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:

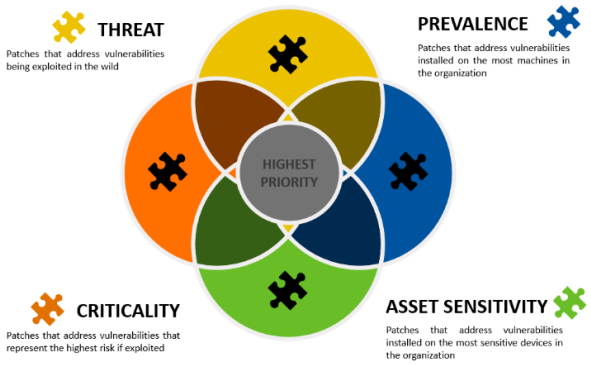
- What systems would result in the most risk if compromised?
- Is it a high-risk device? Patch!

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%

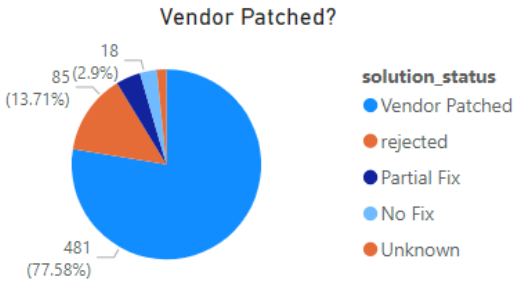
criticality	avg threat score x # of advisories
Highly Critical	7,162.00
Moderately Critical	2,004.00
Less Critical	1,923.00
Not Critical	341.00
Extreme Critical	67.00
Total	**11,497.00**

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.

[Exception this month: Like last month , the Log4j vulnerability is still impacting the scoring with Highly Critical Vulnerabilities *(where normally Moderately Critical Vulnerabilities would be present the most risk)*



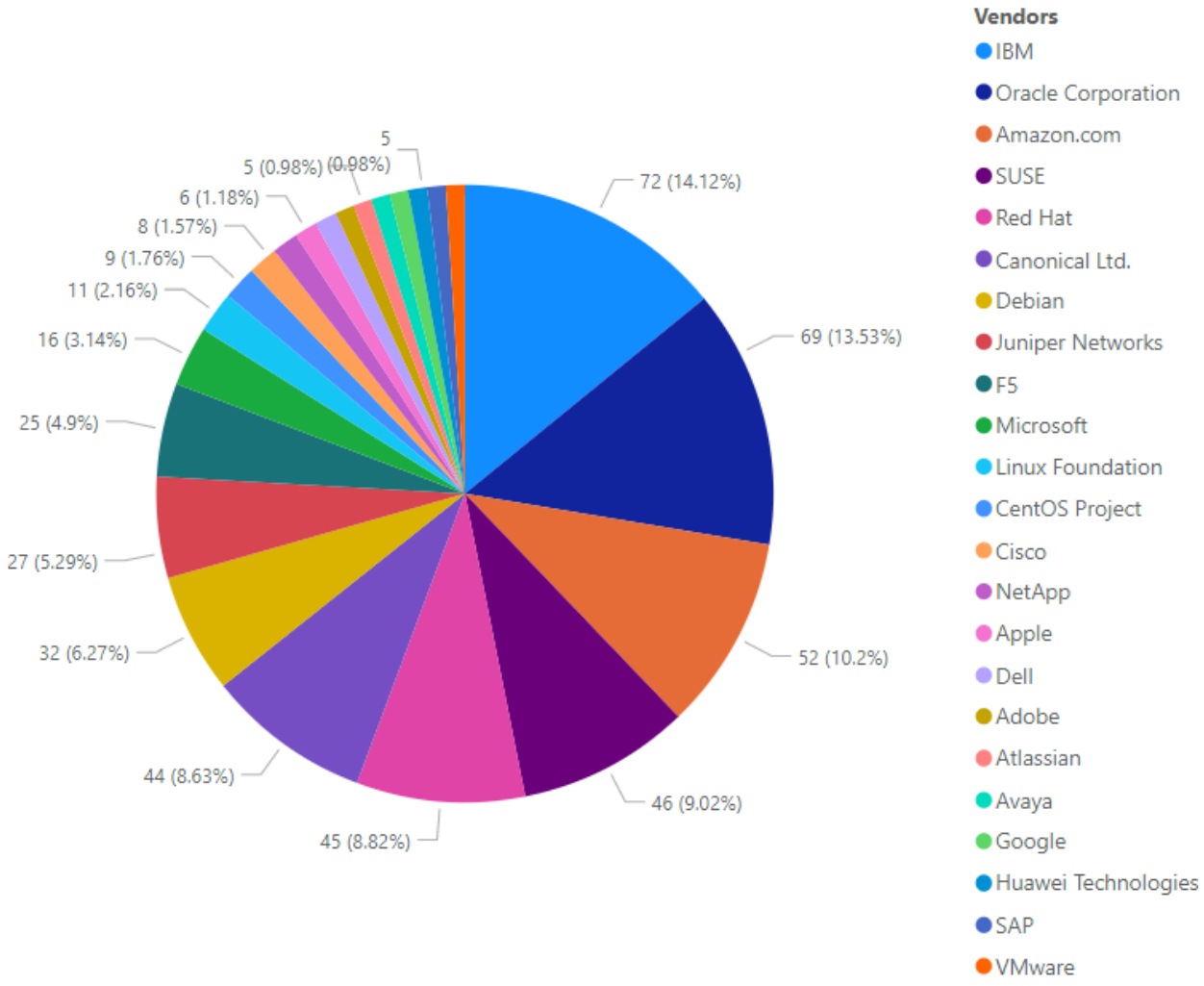
Take away 2:

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

Previous month : 424 Vendor Patched (74.13%)
This Month : **481** Vendor Patched (**77.58%)**

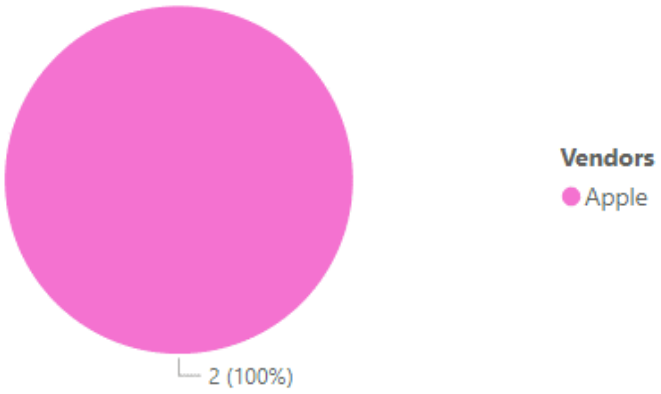
Vendor View

Top Vendors with most Advisories

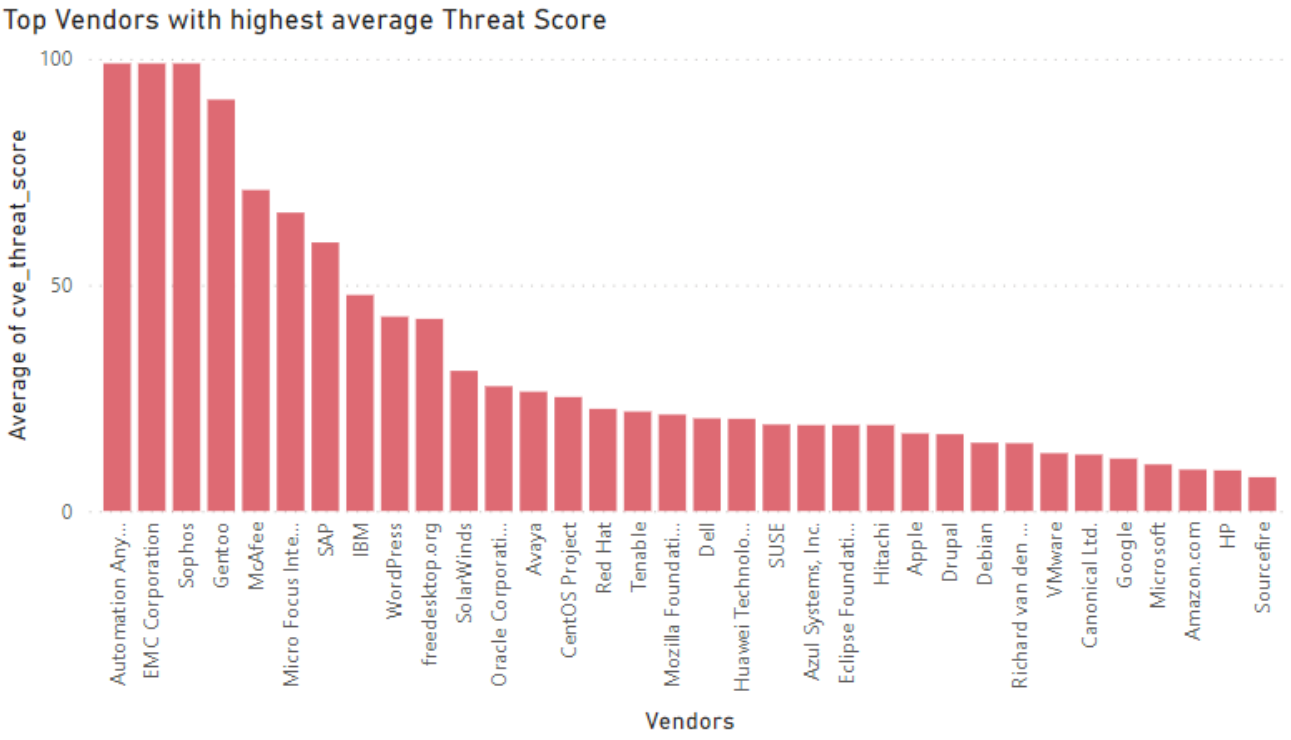


Take away:
IBM reported the most vulnerabilities in this month (again) , mostly due to Log4j disclosures.

Top Vendors with Zero-Day

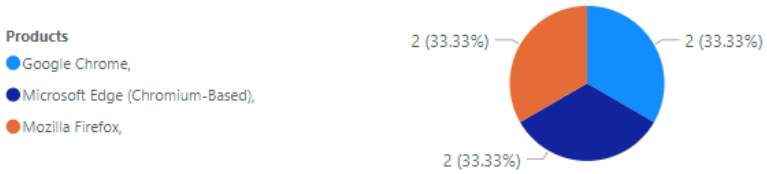


Top Vendors with highest average threat score



Browser Related Advisories

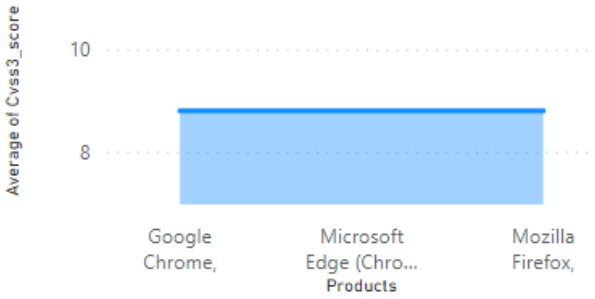
Advisories per browser



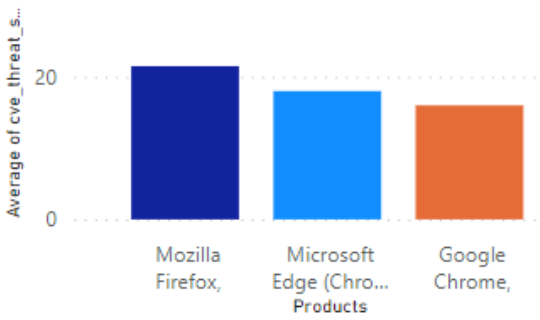
Browser Zero-Day vulnerabilities

No Browser Zero-Day vulnerabilities to report. (This doesn't happen often)

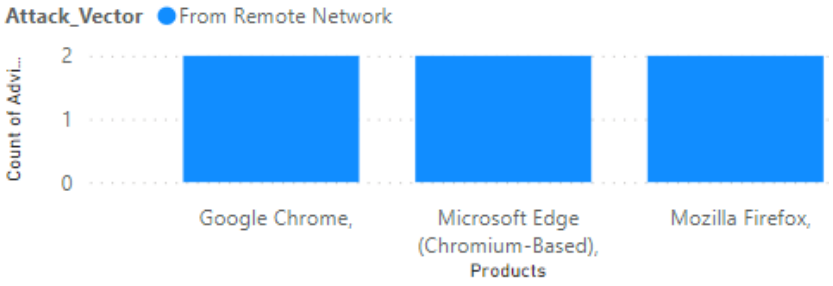
Average CVSS (Criticality) Score per Browser



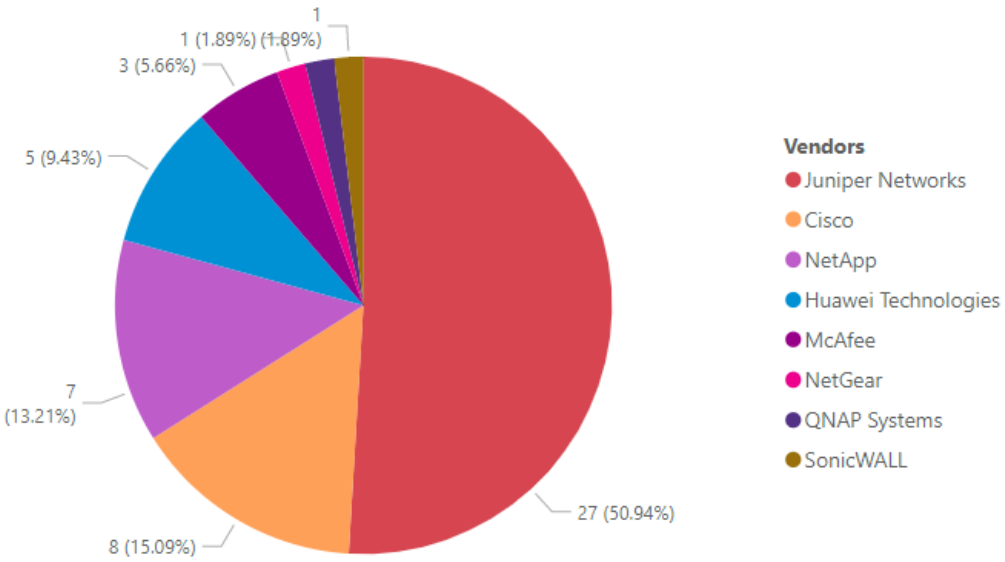
Average Threat Score per Browser



What's the Attack Vector ?



Networking Related Advisories



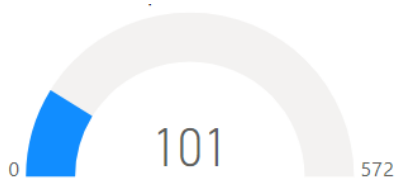
Juniper Networks, one of the world's largest network equipment suppliers, has provided updates to patch numerous security vulnerabilities in device operating systems and network services.

The vulnerabilities range from the ability to inject and execute scripts, through escalating the rights of registered users, to denial-of-service vulnerabilities that attackers could use to paralyze devices. In some cases remote attackers could have triggered this with manipulated packets, for example, in other cases users have to be logged on locally to provoke the errors. Furthermore, Juniper cloud solutions apparently contain Log4j and thus inherit the security vulnerabilities therein..

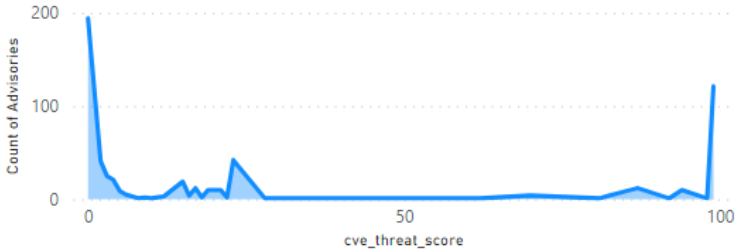
Threat Intelligence

A look at threat intelligence related data for the month.

Count of Malware Exploited CVEs



Count of Advisories by CVE Threat Score



Top 10 Exploits

#	Count	Exploit
1	46	Mirai XMRig Miner CoinMiner Metasploit Conti Ransomware ; CVE-2021-45105
2	43	Khonsari Ransomware Hive Ransomware Mirai Uroburos Rootkit Conti Ransomware ; CVE-2021-45046
3	26	Conti Ransomware Nightsky Ransomware Mirai Cobalt Strike Tellyouthepass ; CVE-2021-44228
4	14	CoinMiner XMRig Miner ; CVE-2021-44832
5	12	DELoader ; CVE-2021-44790
6	10	Crowbar Metasploit RefleXXion ; CVE-2021-4034
7	8	Mirai Xorddos ; CVE-2021-4155
8	6	Metasploit ; CVE-2022-21836
9	6	Metasploit ; CVE-2022-21857
10	6	Metasploit ; CVE-2022-21850

Threat Intelligence Advisory Statistics:

SAIDs with a Threat Score (1+)	383↑*(378)*	61.77%
SAIDs with no Threat Score (=0)	237↑*(194)*	38.23%

SAID: Secunia Advisory Identifier

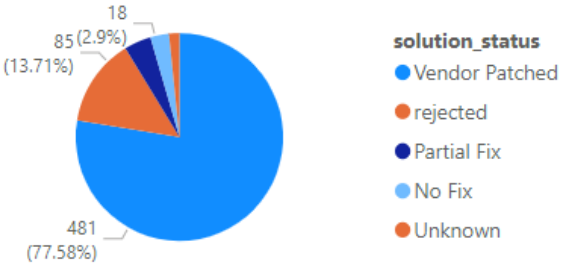
Range	Score	*Last month*	%
Medium-Range Threat Score SAIDs (13-23)	193↑	*(111)*	(31.13%)
Low-Range Threat Score SAIDs (1-12)	105 ↓	*(111)*	(16.77%)
Very Critical Threat Score SAIDs (71-99)	71 ↓	*(149)*	(11.45%)
High-Range Threat Score SAIDs (24-44)	11 ↑	*(2)*	(1.77%)
Critical-Range Threat Score SAIDs (45-70)	3 ↓	*(5)*	(0.48%)

Patching

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

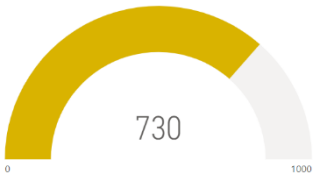
The challenge remains that organizations do not have full visibility or awareness when a vulnerability is disclosed (Time to Awareness) . Another big challenge is the time to Remediation (the time from having this information, correlating that with your environment and initiating the process to get the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

Vulnerabilities that are Vendor Patched



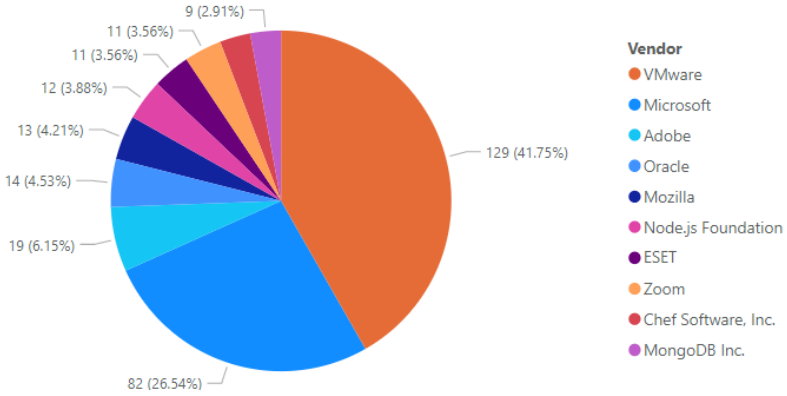
Flexera's Vendor Patch Module (VPM) statistics

Flexera has the largest third-party Patch Catalog **(+2700)** 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**