MONTHLY VULNERABILITY INSIGHTS

Based on Data from Secunia Research

NOVEMBER 2021

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.

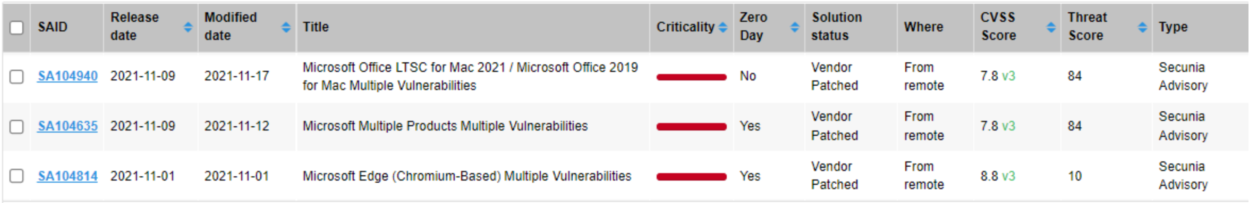
Click here to learn more about Secunia Advisories and their contents.

Summary

We've seen a decrease in vulnerabilities for **November 2021**.
However, seeing an increase in the number of threats associated with vulnerabilities.

total advisories : **500** ↓ (was: **526**) .

Slight increase of **Extreme Critical Vulnerabilities** : **3** ↑ after 2 were reported last month.



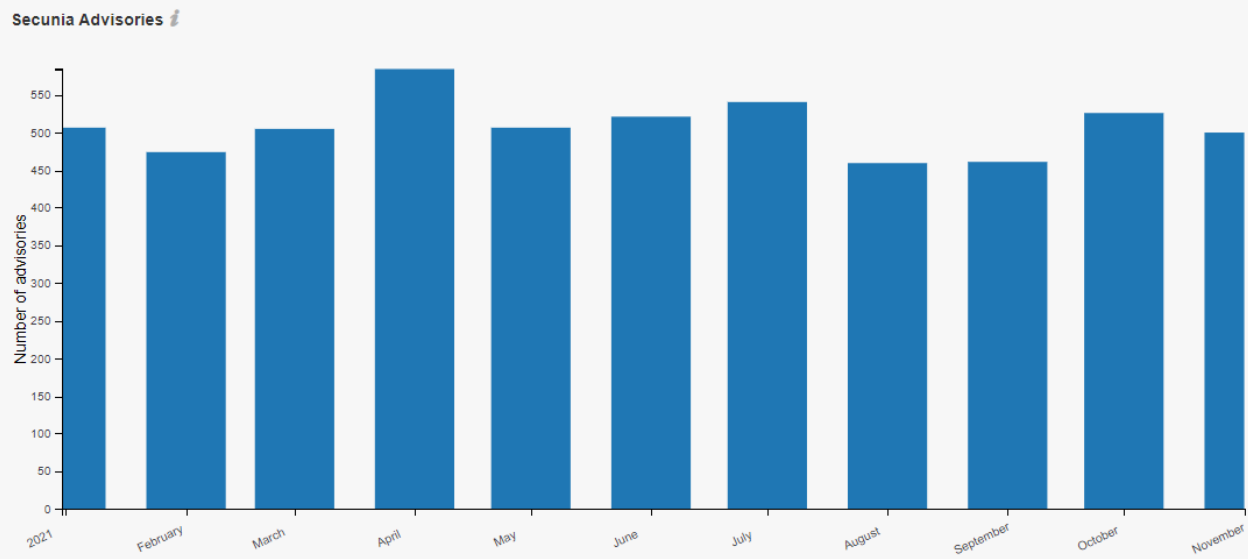
☐	SAID	Release date	Modified date	Title	Criticality	Zero Day	Solution status	Where	CVSS Score	Threat Score	Type
☐	SA104940	2021-11-09	2021-11-17	Microsoft Office LTSC for Mac 2021 / Microsoft Office 2019 for Mac Multiple Vulnerabilities	🟥	No	Vendor Patched	From remote	7.8 v3	84	Secunia Advisory
☐	SA104635	2021-11-09	2021-11-12	Microsoft Multiple Products Multiple Vulnerabilities	🟥	Yes	Vendor Patched	From remote	7.8 v3	84	Secunia Advisory
☐	SA104814	2021-11-01	2021-11-01	Microsoft Edge (Chromium-Based) Multiple Vulnerabilities	🟥	Yes	Vendor Patched	From remote	8.8 v3	10	Secunia Advisory

Note:

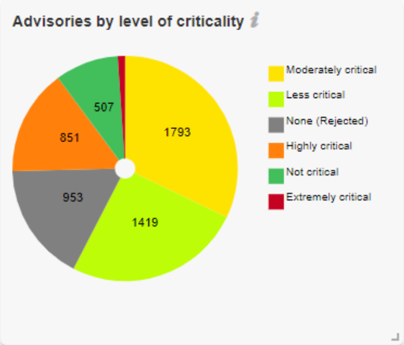
Advisory SA104814 (initial release Oct. 31) was released in the CET twilight of Oct.31 and Nov 01. During the run of the report (CET) the advisory was not included in the October report , therefore adding it to the November report.

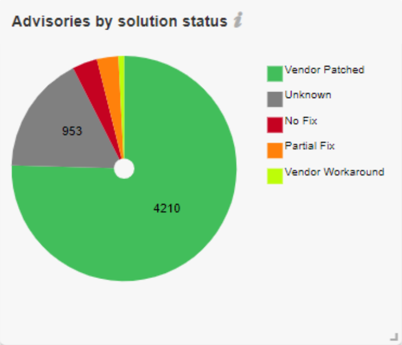
Year to Date Overview

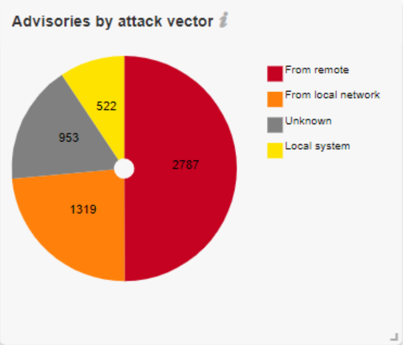
As of **November**, the year-to-date total is at **5581** Advisories ↓ which is lower than 2020 : **6529** YTD Advisories)

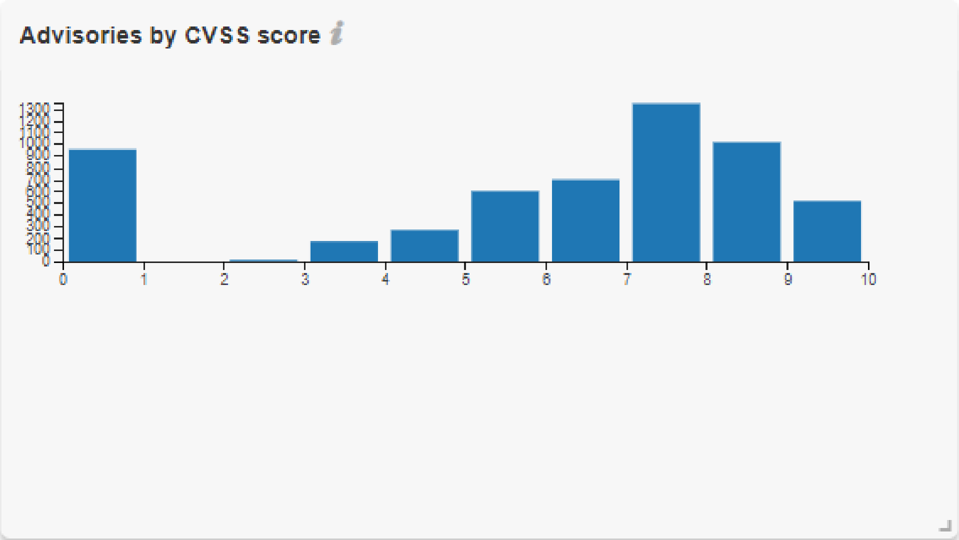

Secunia Advisories

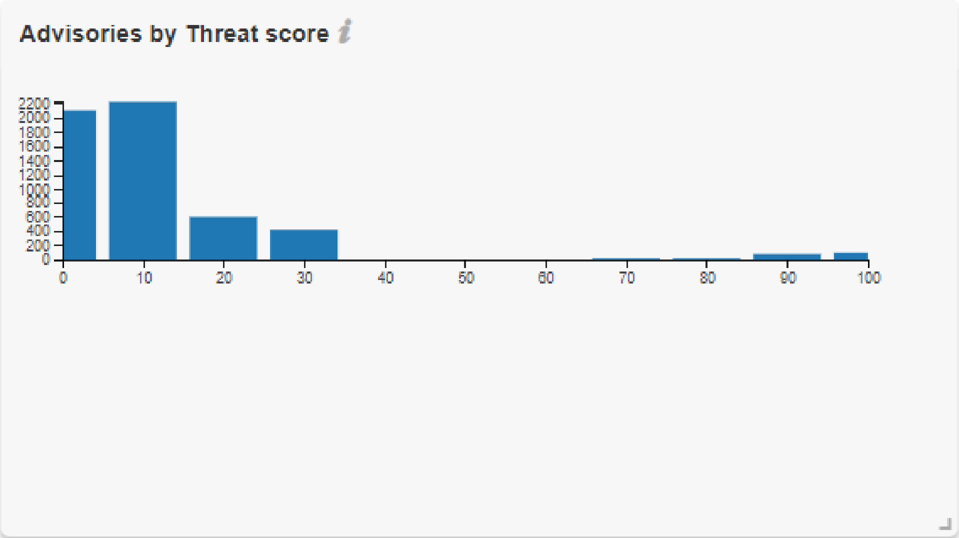
A relatively stable year compared with last year where we've seen spikes in April'20 and July'20.


Advisories by level of criticality


Advisories by solution status


Advisories by attack vector


Advisories by CVSS score
1300
1200
1100
1000
900
800
700
600
500
400
300
200
100
0
0
1
2
3
4
5
6
7
8
9
10


Advisories by Threat score
2200
2000
1800
1600
1400
1200
1000
800
600
400
200
0
0
10
20
30
40
50
60
70
80
90
100

Monthly Data

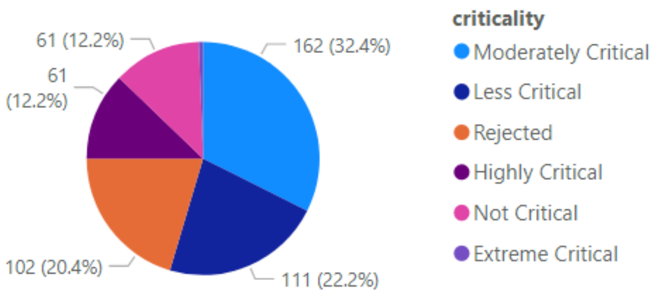
This month, a total of **500** ↑ advisories were reported by the Secunia Research Team.

This Month:	#	Change *(last month):*
Total # of advisories	**500**	↓ *(526)*
Unique Vendors	**75**	↓ *(80)*
Unique Products	**312**	↓ *(328)*
Unique Versions	**390**	↓ *(410)*
Rejected Advisories *	**102**	↑ *(99)*
		↑ increased ↓lower ↔ same

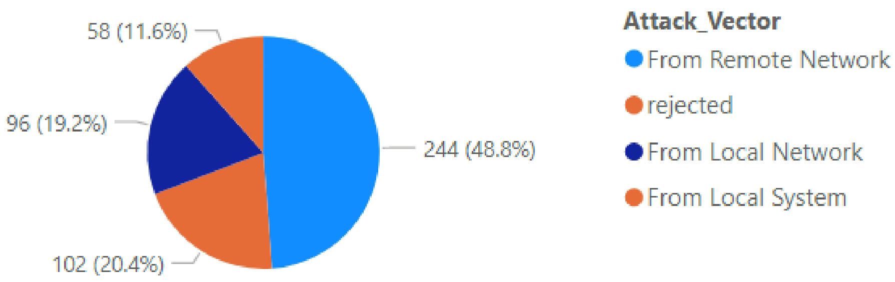
** **102** advisories have received the “rejected” status which means in general that leveraging it would require one or more violations of security best practices (e.g. product not securely configured or not used securely) or that it was “too weak of a gain” (e.g. administrative, local users already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

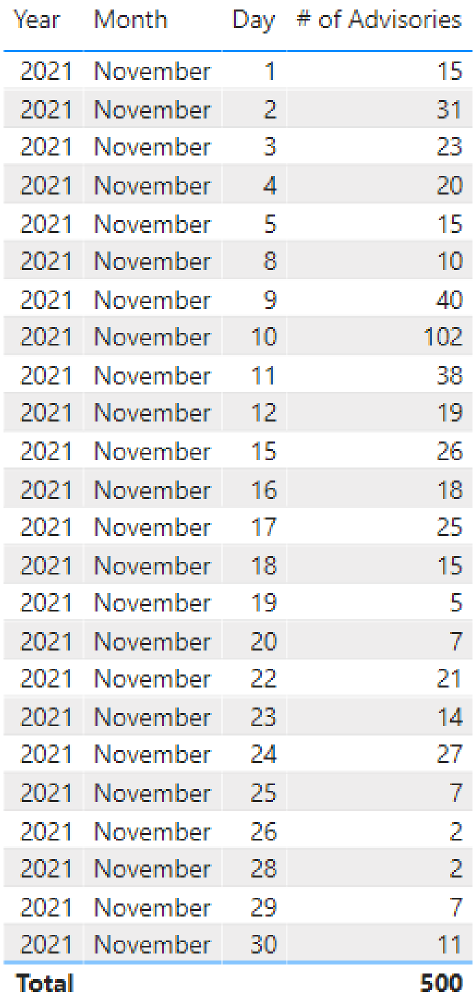


Advisories by Criticality



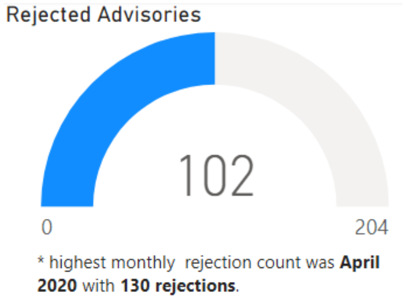
Advisories per Day

Below an overview of the daily advisory count.



Year	Month	Day	# of Advisories
2021	November	1	15
2021	November	2	31
2021	November	3	23
2021	November	4	20
2021	November	5	15
2021	November	8	10
2021	November	9	40
2021	November	10	102
2021	November	11	38
2021	November	12	19
2021	November	15	26
2021	November	16	18
2021	November	17	25
2021	November	18	15
2021	November	19	5
2021	November	20	7
2021	November	22	21
2021	November	23	14
2021	November	24	27
2021	November	25	7
2021	November	26	2
2021	November	28	2
2021	November	29	7
2021	November	30	11
Total			**500**

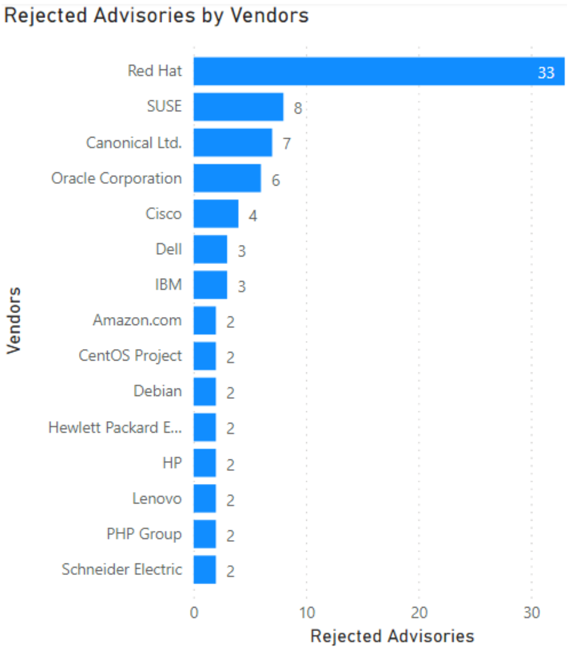
Rejected Advisories



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.



Monthly Vulnerability Review

November 2021

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:

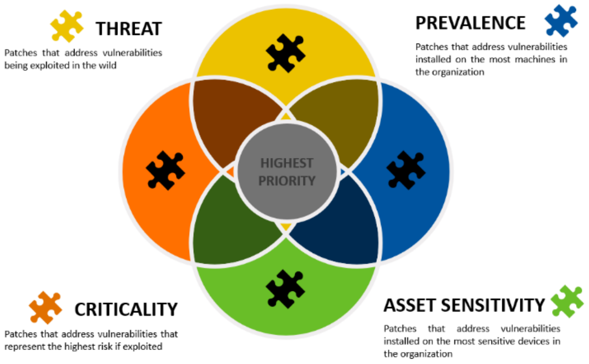
- What systems would result in the most risk if compromised?
- Is it a high-risk device? Patch!

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!

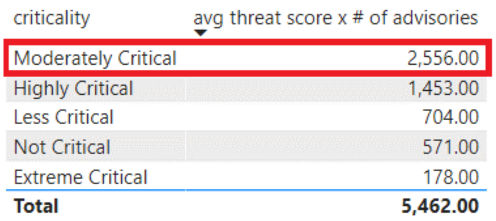
Threat Intelligence:

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


THREAT
Patches that address vulnerabilities being exploited in the wild
PREVALENCE
Patches that address vulnerabilities installed on the most machines in the organization
HIGHEST PRIORITY
CRITICALITY
Patches that address vulnerabilities that represent the highest risk if exploited
ASSET SENSITIVITY
Patches that address vulnerabilities installed on the most sensitive devices in the organization

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%

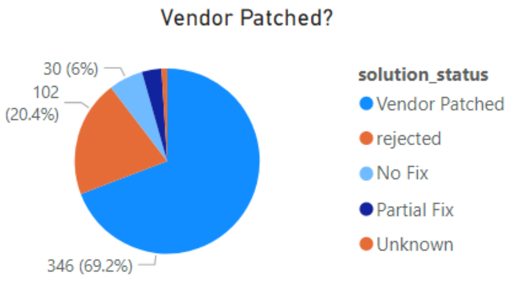


criticality	avg threat score x # of advisories
Moderately Critical	2,556.00
Highly Critical	1,453.00
Less Critical	704.00
Not Critical	571.00
Extreme Critical	178.00
Total	**5,462.00**

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.

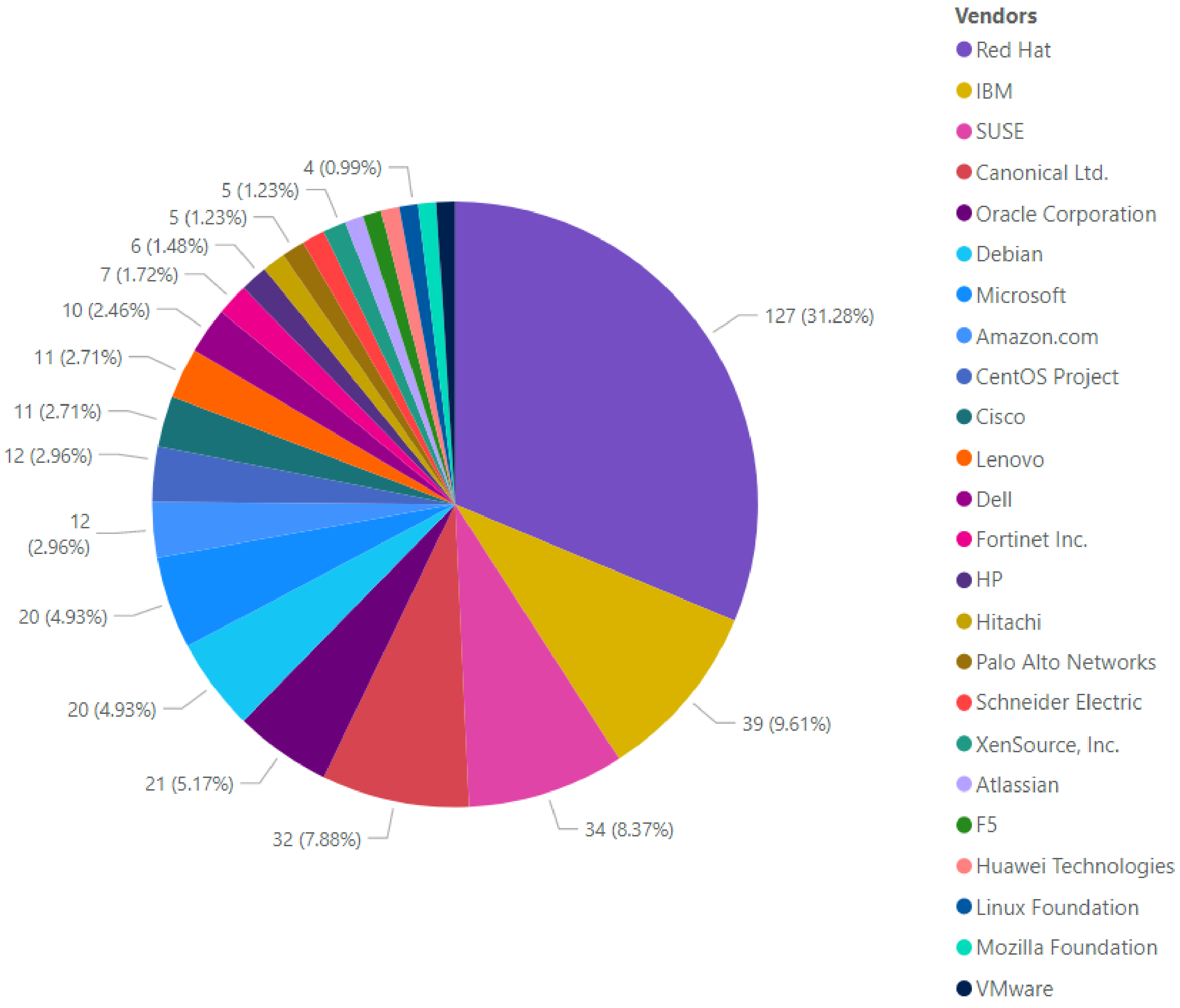


Take away 2:

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

Vendor View

Top Vendors with most Advisories

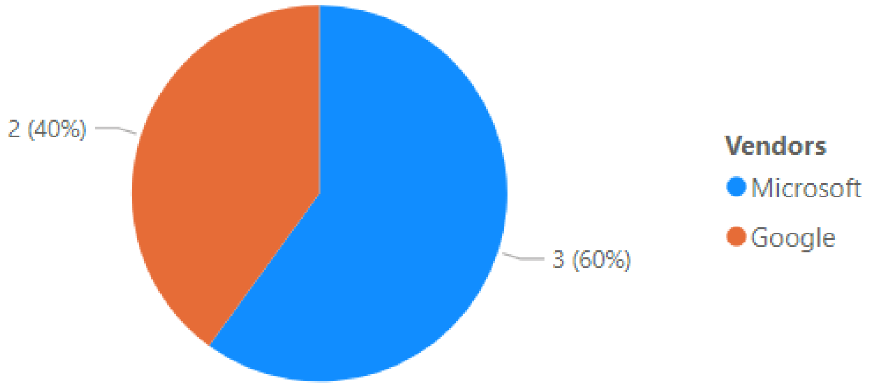


Take away:
Red Hat is not only the vendor with the most vulnerabilities, but also rejected vulnerabilities.
(127 vulnerabilities – 33 rejections = 96 actual vulnerabilities (still number 1 on the list)

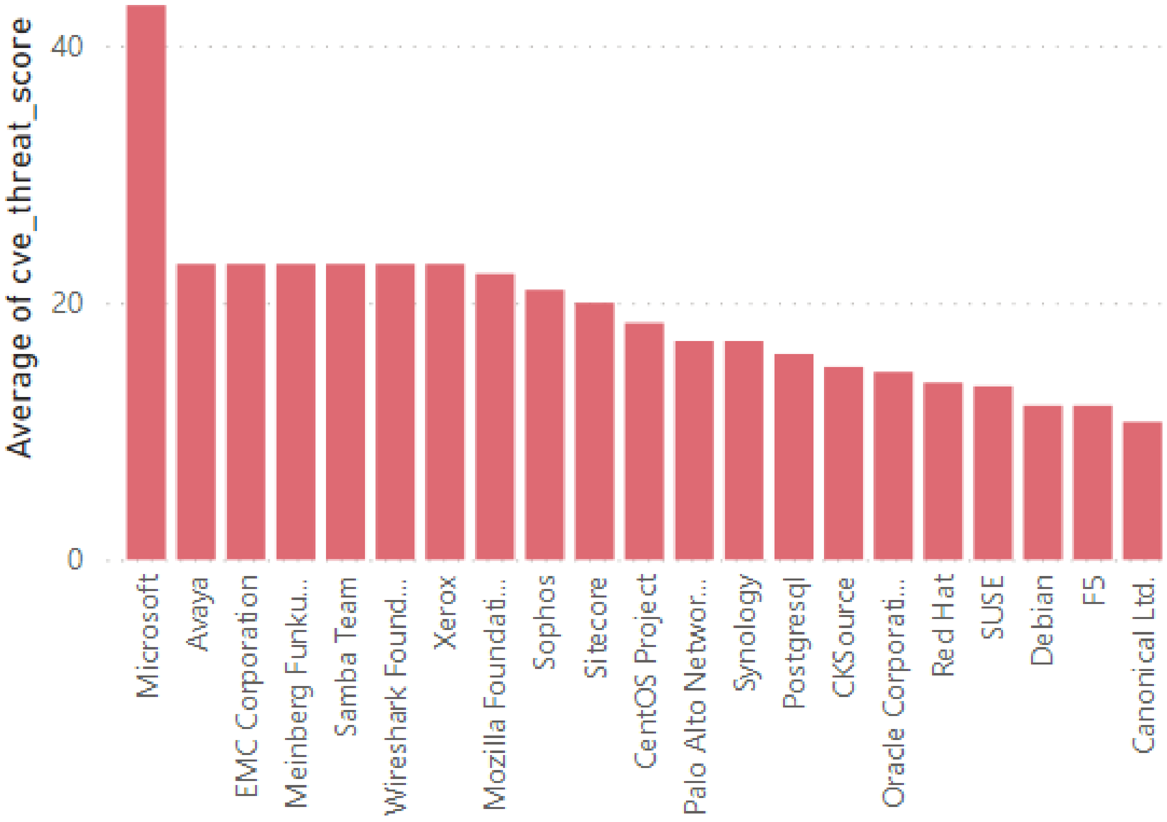
Top 5 if excluding rejections:

Vendor	Total
Red Hat	94
IBM	36
SUSE	26
Canonical	25
Microsoft	20

Top Vendors with Zero-Day

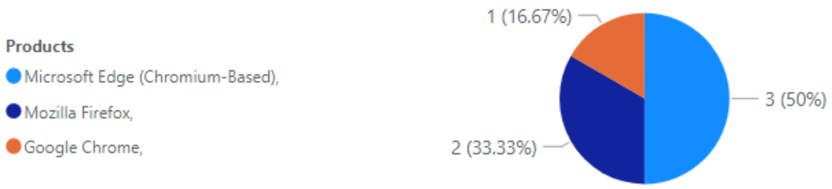


Top Vendors with highest average threat score



Browser Related Advisories

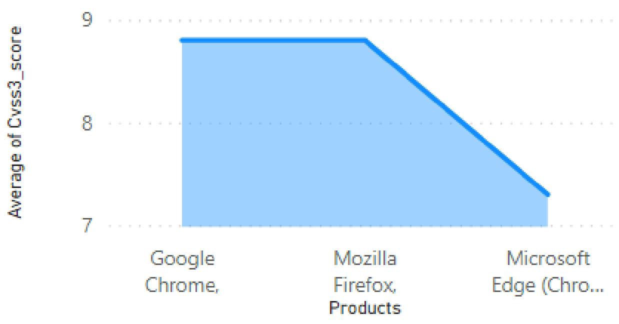
Advisories per browser



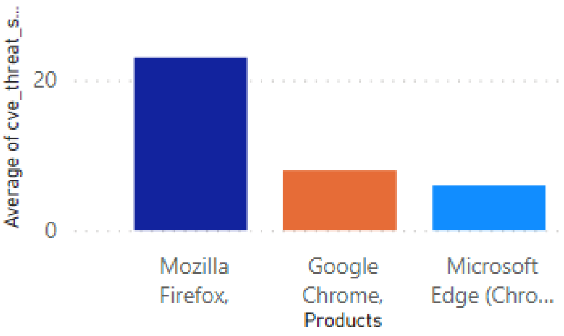
Browser Zero-Day vulnerabilities

Count of Advisories	Products	Advisories
1	Microsoft Edge (Chromium-Based),	SA104814
1		

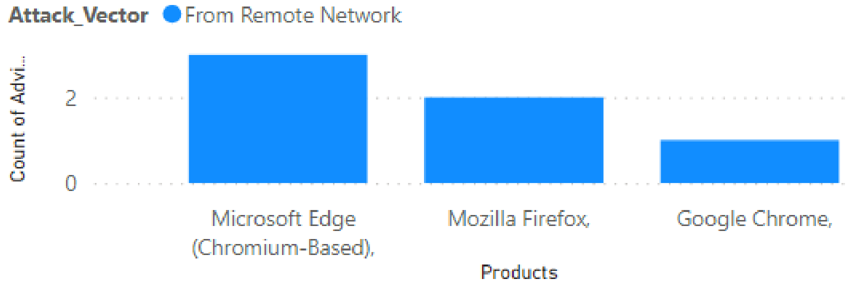
Average CVSS (Criticality) Score per Browser



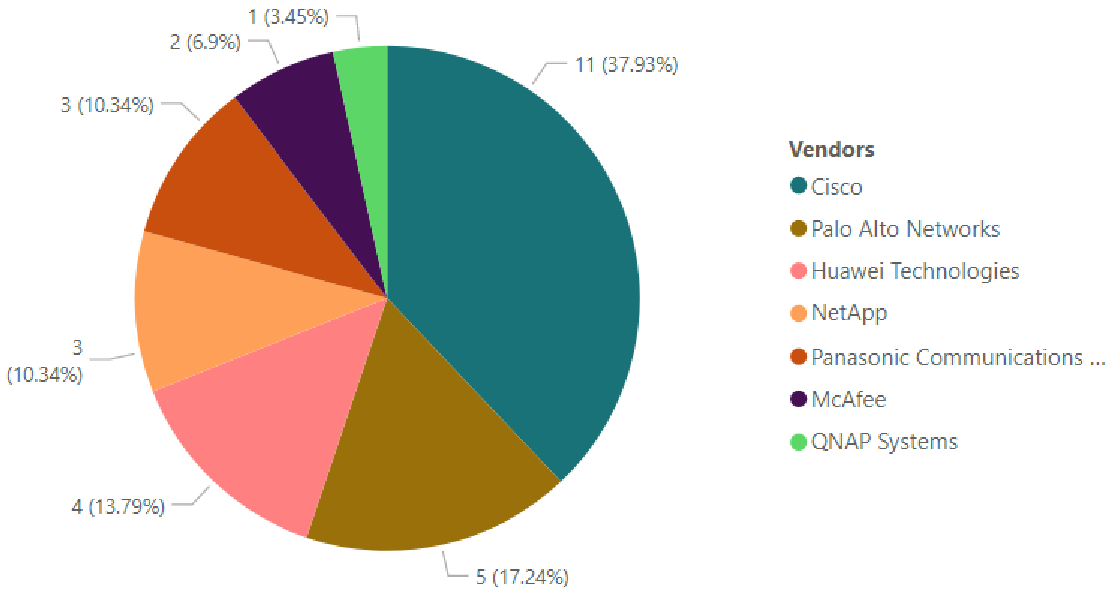
Average Threat Score per Browser



What's the Attack Vector ?



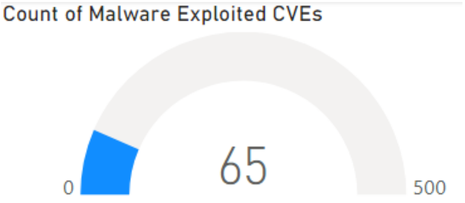
Networking Related Advisories



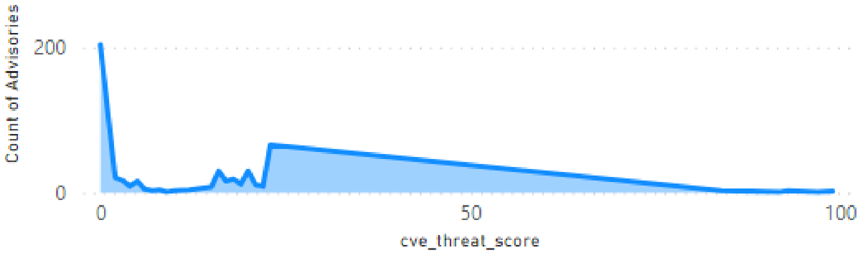
Threat Intelligence

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	295↑*(270)*	59.12%
SAIDs with no Threat Score	204↓*(256)*	40.88%

SAID: Secunia Advisory Identifier

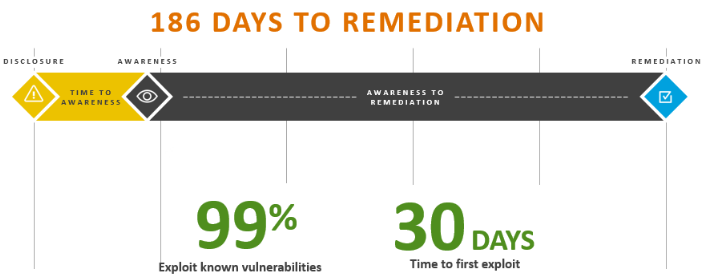
Range	**Score**	***change***	**%**
Medium-Range Threat Score SAIDs (13-23)	201↑	*(157)*	(40.28%)
Low-Range Threat Score SAIDs (1-12)	82 ↓	*(88)*	(16.43%)
Very Critical Threat Score SAIDs (71-99)	12 ↓	*(20)*	(2.4%)
High-Range Threat Score SAIDs (24-44)	0 ↓	*(5)*	(0.0%)
Critical-Range Threat Score SAIDs (45-70)	0 =	*(0)*	(0.0%)

Patching

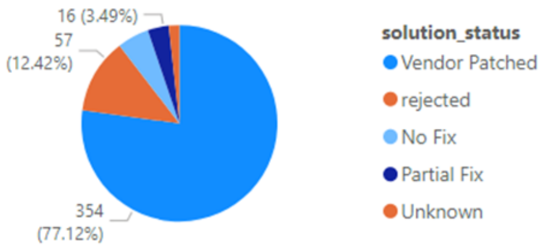
Most of this month’s vulnerabilities are vendor patched, in fact most vulnerabilities are patched within 24 hours after disclosure.

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).

The Risk Window

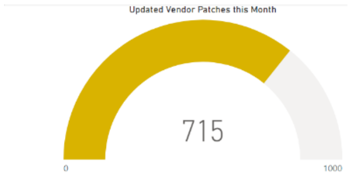


Vulnerabilities that are Vendor Patched



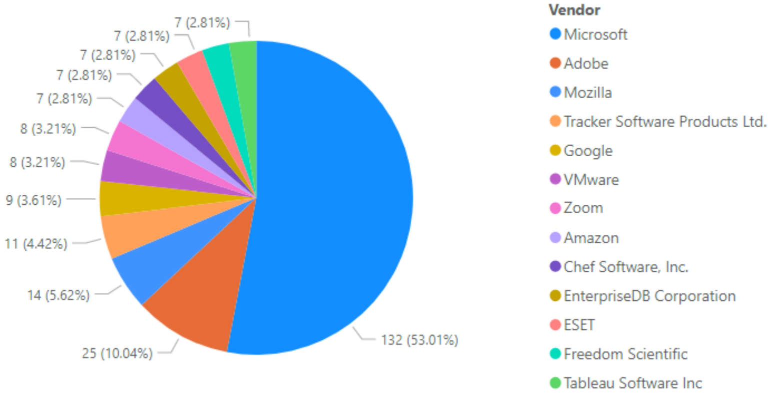
Flexera’s Vendor Patch Module (VPM) statistics

Flexera has the largest third-party Patch Catalog **(+2600)** 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)



Top Advisory of the month

Oracle Solaris Multiple Third Party Components Multiple Vulnerabilities

Secunia Advisory ID	SA105245
Creation Date	2021-11-17
Criticality	- Highly critical
Zero Day	No
Impact	System access, DoS, Exposure of sensitive information, Manipulation of data, Spoofing, Cross Site Scripting, Security Bypass, Unknown
Where	From remote
Solution Status	Vendor Patched
Secunia CVSS Scores	CVSS3 Base: 9.8, Overall: 8.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
CVE references	CVE-2021-20254 CVE-2021-1825 CVE-2021-22960 CVE-2021-22947 CVE-2021-28662 CVE-2021-21806 CVE-2021-1826 CVE-2021-30797 CVE-2018-19492 CVE-2008-2711 CVE-2021-35588 CVE-2021-35517 CVE-2021-35586 CVE-2020-36318 CVE-2021-22898 CVE-2021-3522 CVE-2021-30661 CVE-2021-30795 CVE-2021-30761 CVE-2021-28877 CVE-2021-35603 CVE-2021-36090 CVE-2021-31808 CVE-2021-28879 CVE-2021-30689 CVE-2021-30858 CVE-2021-22117 CVE-2021-35564 CVE-2021-35556 CVE-2018-19490 CVE-2021-3497 CVE-2021-30720 CVE-2021-21775 CVE-2021-30666 CVE-2021-30682 CVE-2021-31807 CVE-2021-22959 CVE-2021-23960 CVE-2021-3498 CVE-2021-28116 CVE-2020-7595 CVE-2021-28875 CVE-2021-35560 CVE-2021-21779 CVE-2021-1817 CVE-2021-35550 CVE-2021-30744 CVE-2021-35559 CVE-2021-22925 CVE-2021-28876 CVE-2020-26968 CVE-2021-23437 CVE-2021-28878 CVE-2020-25097 CVE-2021-33037 CVE-2021-35578 CVE-2021-30663 CVE-2021-35565 CVE-2021-28651 CVE-2020-16042 CVE-2021-30758 CVE-2021-33620 CVE-2021-35567 CVE-2021-22116 CVE-2020-26950 CVE-2021-3580 CVE-2021-22946 CVE-2021-23964 CVE-2020-35113 CVE-2021-36386 CVE-2021-3530 CVE-2021-30749 CVE-2021-22901 CVE-2021-22924 CVE-2021-30762 CVE-2021-31806 CVE-2021-22945 CVE-2021-30665 CVE-2021-29967 CVE-2021-29955 CVE-2021-30799 CVE-2021-1820 CVE-2021-36373 CVE-2021-35561 CVE-2021-22923 CVE-2021-3541 CVE-2021-30734 CVE-2021-36374 CVE-2018-19491
Threat Score	99 (Last Updated 2021-11-17)

Affected operating system and software

Operating systems

Oracle Solaris 11.x	CPE Exists. Click for details.

(continued Top Advisory)

Advisory Details:

Description:

Multiple vulnerabilities have been reported in Oracle Solaris, where multiple have an unknown impact and the
other ones can be exploited by malicious, local users to disclose sensitive information and bypass certain security
restrictions, by malicious users to conduct HTTP request smuggling attacks, disclose sensitive information, bypass
certain security restrictions, and cause a DoS (Denial of Service), and by malicious people to conduct HTTP request
smuggling, spoofing, and cross-site scripting attacks, disclose sensitive information, manipulate certain data,
bypass certain security restrictions, cause a DoS, and compromise a vulnerable system.

Solution:

Update to version 11.4 SRU 39.

Original advisory:

Oracle:
https://www.oracle.com/security-alerts/bulletinoct2021.html

Changelog:

2021-11-17: Initial release

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**