MONTHLY VULNERABILITY INSIGHTS

Based on Data from Secunia Research

DECEMBER 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.

The anatomy of a Security Advisory

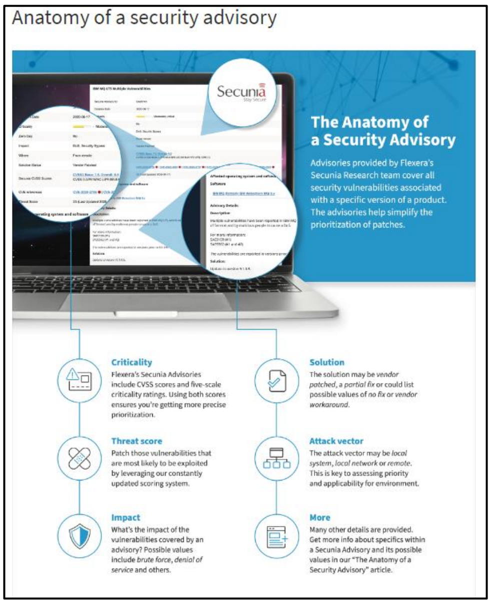
A security advisory is a summary of the work that Secunia Research performs to communicate standardized, validated and enriched vulnerability research on a specific software product version.

We issue Secunia Research criticality ratings and common vulnerability scoring system (CVSS) metrics after a distinct analysis in the advisories. This dual rating method allows for a much-improved means of prioritizing by criticality—delivering a review that includes product context and related security best practices.

A *rejection advisory* issued by the research team issues means we've determined it's not worthy of your attention. This advisory comes if a vendor issues an advisory acknowledging vulnerability that we don't believe to be valid—and would have a product solution we aren't recommending or exceeding already. We send that out to save you considerable time.

If someone other than the vendor issues an advisory and we don't believe to be valid, we discard it. We take that action so you don't waste your time processing inconsequential vulnerability information.

check out this infographic.



Anatomy of a security advisory

The Anatomy of a Security Advisory

Advisories provided by Flexera's Secunia Research team cover all security vulnerabilities associated with a specific version of a product. The advisories help simplify the prioritization of patches.

Criticality
Flexera's Secunia Advisories include CVSS scores and five-scale criticality ratings. Using both scores ensures you're getting more precise prioritization.

Threat score
Patch those vulnerabilities that are most likely to be exploited by leveraging our constantly updated scoring system.

Impact
What's the impact of the vulnerabilities covered by an advisory? Possible values include *brute force*, *denial of service* and others.

Solution
The solution may be *vendor patched*, a *partial fix* or could list possible values of *no fix* or *vendor workaround*.

Attack vector
The attack vector may be *local system*, *local network* or *remote*. This is key to assessing priority and applicability for environment.

More
Many other details are provided. Get more info about specifics within a Secunia Advisory and its possible values in our "The Anatomy of a Security Advisory" article.

Summary

Total advisories : **512** ↓ (last month: **689**) .

December reported less advisories than in November ,

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

- 86 rejected advisories have been reported
- The Secunia Research Team reported **4 Extremely** critical advisories this month (3 last month)
- **7 Zero-Day** Advisory reported (incl. **Citrix**,**Fortinet**,**Microsoft Edge**, **Google Chrome, Windows Server**)
- Over **1,456** CVE's (last month : **1,620**) were covered in the **512** Advisories
- Threat Intelligence indicates that more **Medium and Highly Critical Vulnerabilities** are targeted by hackers.
- More than half of all advisories are disclosed by 4 vendors (**SUSE** 19%, **IBM** 16%, **Amazon** 11%, **Ubuntu** 9%)
- **NetApp** is contributing to **85%** of all Networking related Advisories.

Last month we reported that **59.22%** of all Secunia Advisories had a **Threat** (exploits, malware, ransomware , etc.) associated with them, this month the number has been lower to **64.66%**

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)

Noticeable information this month:

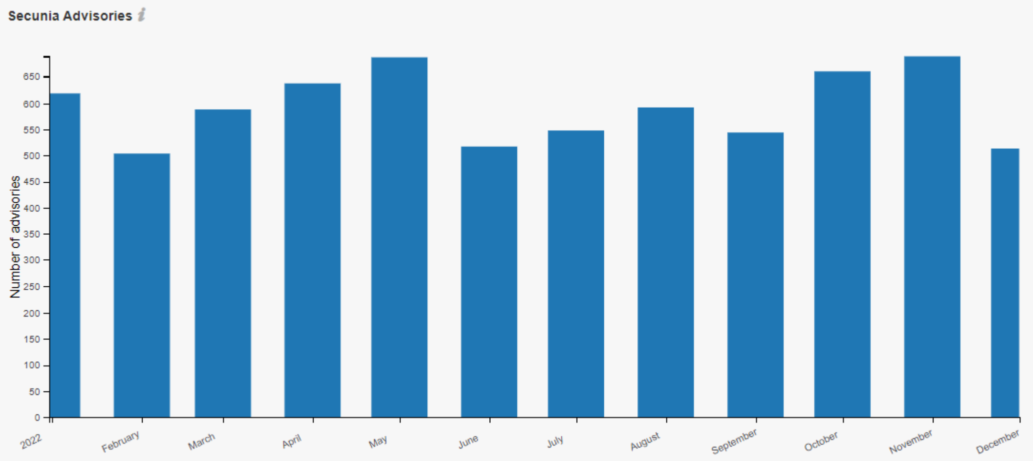
- **Google Chrome** continues to disclose zero-day vulnerabilities with #9 (CVE-2022-4262) this year
- **Fortinet** Warns of Active Exploitation of New SSL-VPN Pre-auth RCE Vulnerability (CVE-2022-42475)
- Critical Ping Vulnerability Allows Remote Attackers to Take Over **FreeBSD** Systems (CVE-2022-23093)
- Hackers Actively Exploiting **Citrix ADC** and **Gateway** Zero-Day Vulnerability (CVE-2022-27518)
- **Microsoft** addresses two zero days in December (Edge, Windows Server) reported in 3 SAID's.
- **Log4Shell :** 35% of Log4 downloads continue to be of vulnerable versions of the software.
  the US Department of Homeland Security review board earlier this year concluded that Log4 is an endemic security risk that organizations will need to contend with for years.
- **CISA** added 9 vulnerabilities on the **KEV** (Known Exploited Vulnerabilities) list . the related December vulns are:
  - CVE-2022-42856, Apple iOS/Safari,MacOS, WebkitGTK,Debian for wpewebkit, SUSE for webkitgtk3
  - CVE-2022-4262, Google Chromium, Microsoft Edge, Debian update for Chromium
  - CVE-2022-42475, FortiOS
  - CVE-2022-27518, Citrix

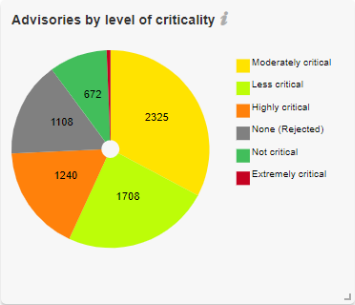
Interesting sources of information:

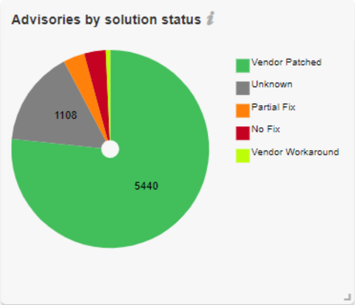
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- https://www.bleepingcomputer.com/news/security/
- https://thehackernews.com/search/label/Vulnerability
- https://www.darkreading.com/vulnerability-management?page=1
- https://portswigger.net/daily-swig/vulnerabilities
- https://www.securityweek.com/virus-threats/vulnerabilities

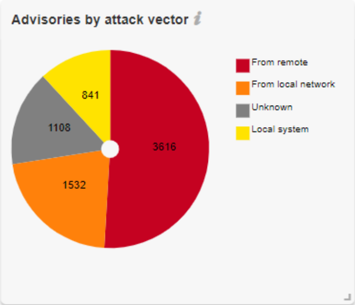
Year-to-date overview

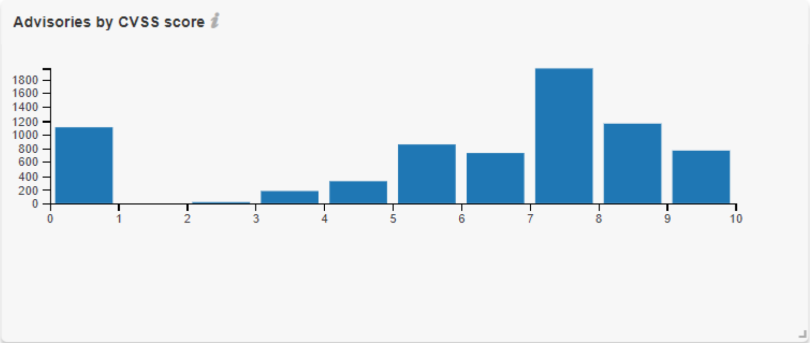
As of **December 31, 2022**, the year-to-date total is at **7,097** Advisories ↑ which is higher than 2021 : **6,153** YTD Advisories)

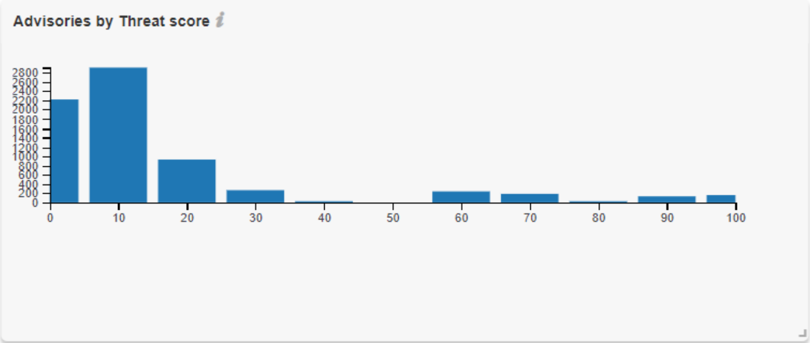












Monthly data

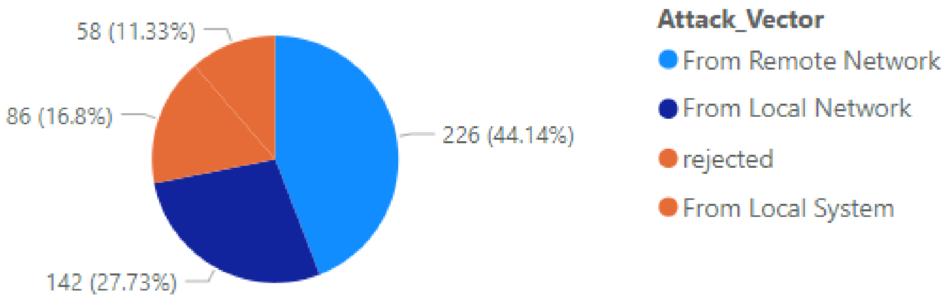
This month, a total of **689** ↑ (last month: **689**) advisories were reported by the Secunia Research Team.

This month:	**#**	**Change** *(last month):*
Total # of advisories	**512**	↓ *(689)*
Unique Vendors	**81**	↓ *(97)*
Unique Products	**318**	↑ *(307)*
Unique Versions	**374**	↓ *(386)*
Rejected Advisories *	**86**	↓ *(153)*
		↑ increased ↓lower ↔ same

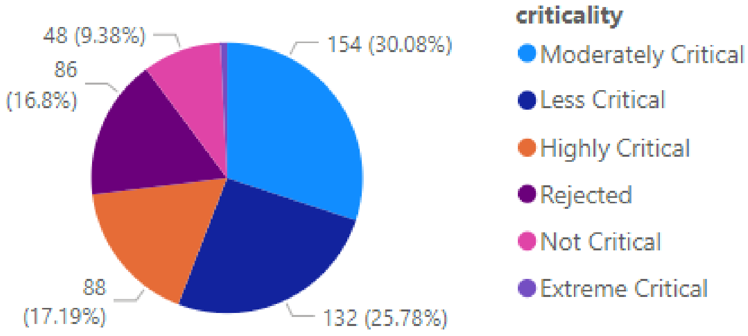
* ***153*** *advisories have received the “rejected” status which means in general that leveraging it would require one or more violations of security best practices (e.g., product not securely configured or not used securely) or that it was “too weak of a gain” (e.g., administrative, local users already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

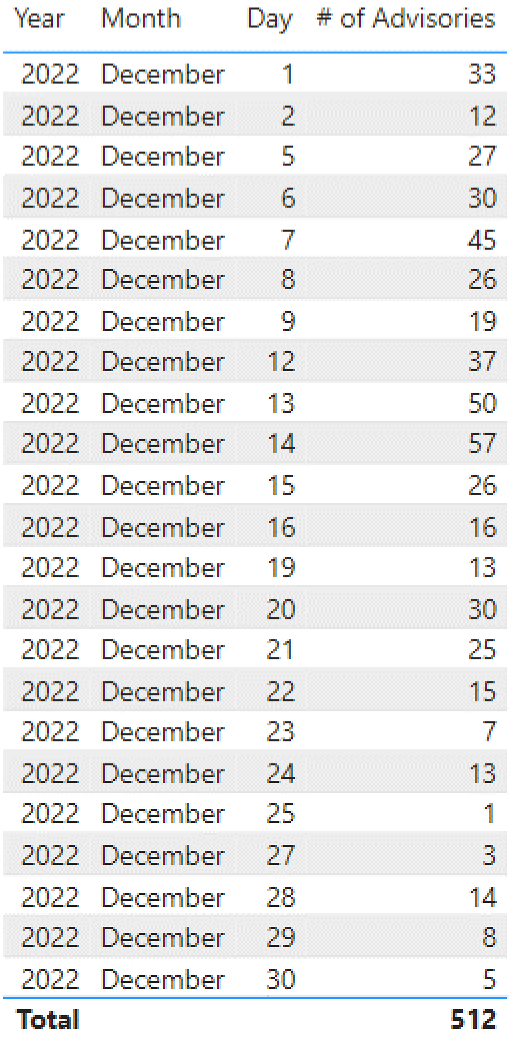


Advisories by criticality



Advisories per day

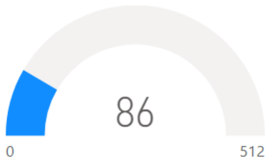
Below an overview of the daily advisory count.



Year	Month	Day	# of Advisories
2022	December	1	33
2022	December	2	12
2022	December	5	27
2022	December	6	30
2022	December	7	45
2022	December	8	26
2022	December	9	19
2022	December	12	37
2022	December	13	50
2022	December	14	57
2022	December	15	26
2022	December	16	16
2022	December	19	13
2022	December	20	30
2022	December	21	25
2022	December	22	15
2022	December	23	7
2022	December	24	13
2022	December	25	1
2022	December	27	3
2022	December	28	14
2022	December	29	8
2022	December	30	5
Total			**512**

Rejected advisories

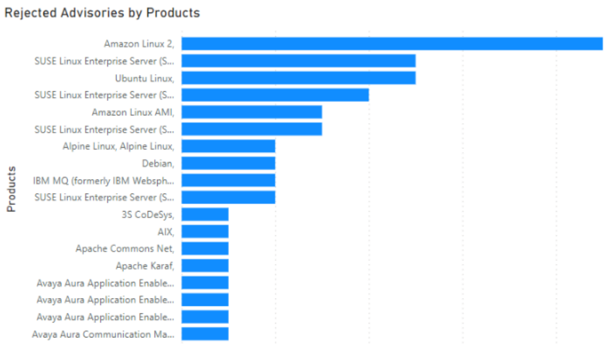
There are many vulnerabilities posted to the National Vulnerability Database (NVD) by a lot of people and companies. They are not always valid, assigned a proper criticality, and in some cases, a vulnerability may be legitimate but not afford the attacker any benefit.

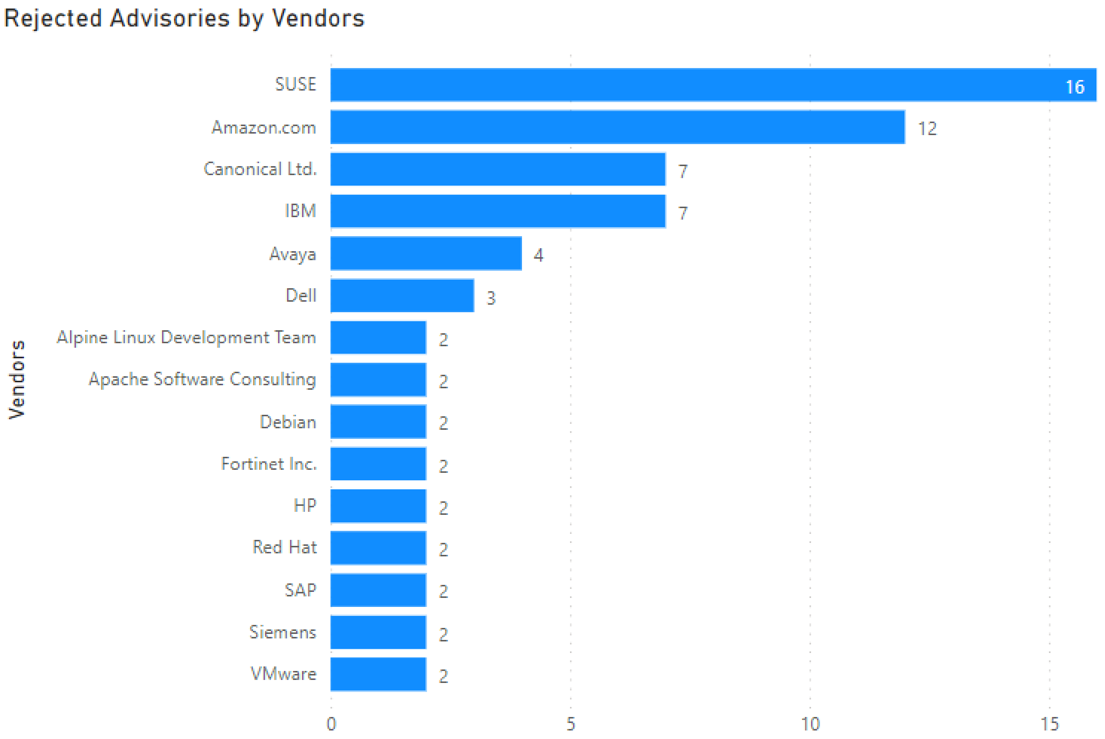


The Secunia Research team at Flexera evaluates vulnerabilities from hundreds of sources, rescores them when necessary and even rejects vulnerabilities not worth your attention. Rejection Advisories help you to reduce the volume of vulnerabilities to be mitigated by helping you focus only on those that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

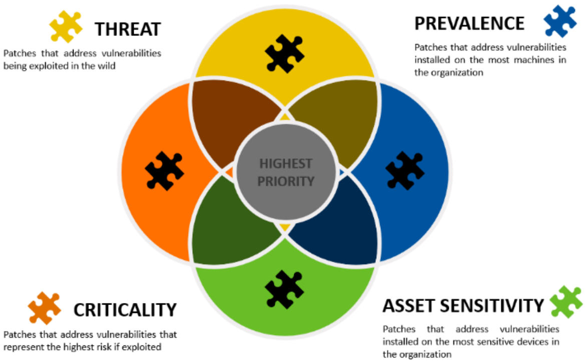
- What systems would result in the most risk if compromised?
- Is it a high-risk device? **Patch**.

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:

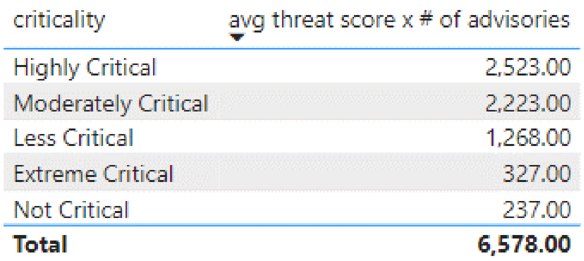
- The newest and most impactful method focuses on the likelihood of exploitation.
- Is it likely to be exploited? **Patch**.


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 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	2,523.00
Moderately Critical	2,223.00
Less Critical	1,268.00
Extreme Critical	327.00
Not Critical	237.00
Total	**6,578.00**

Take away 1:

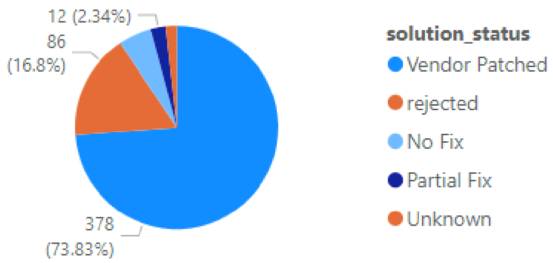
Critical vulnerabilities do not necessarily present the most risk.

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:

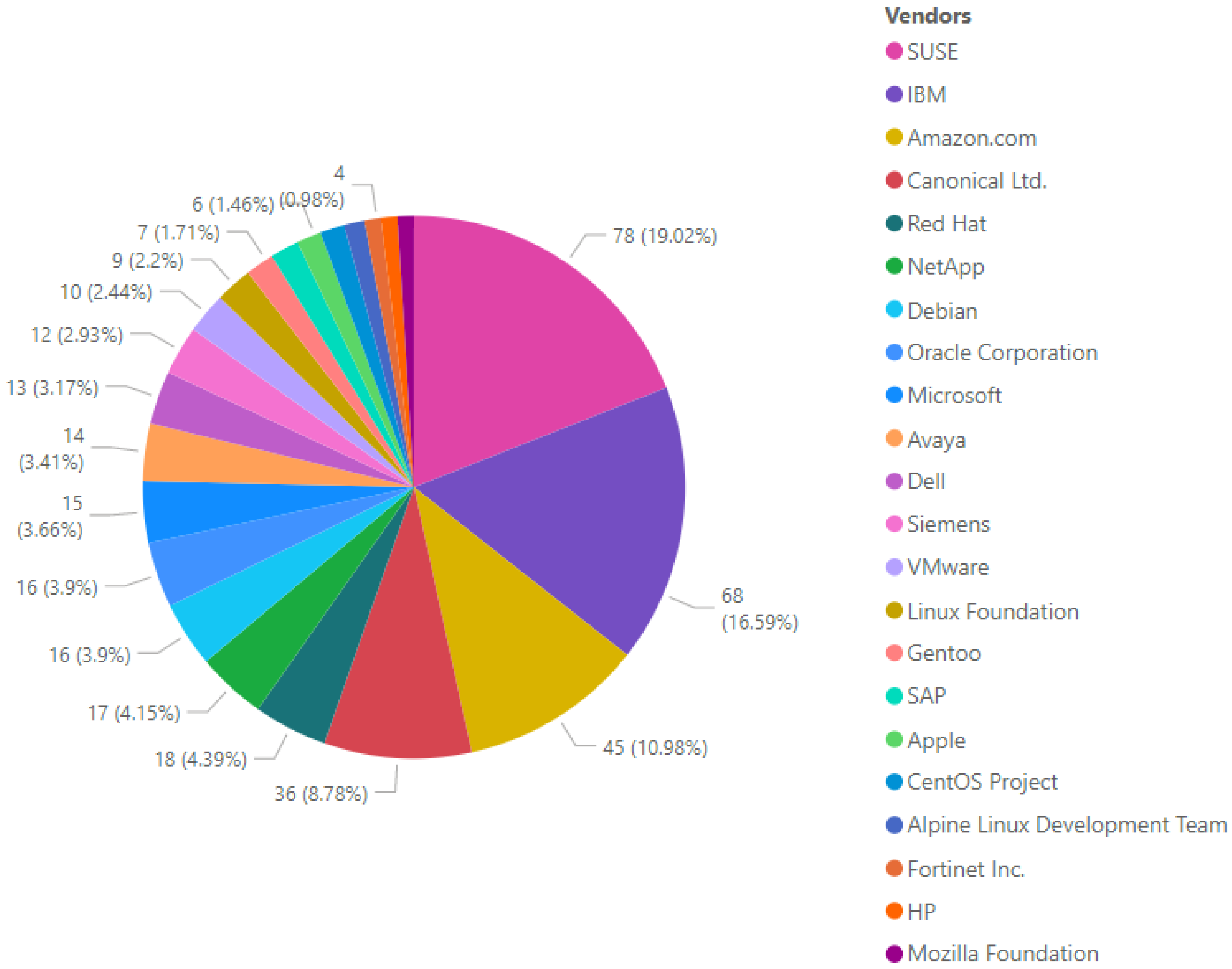
Most vulnerabilities have a patch available (typically within 24 hours after disclosure).



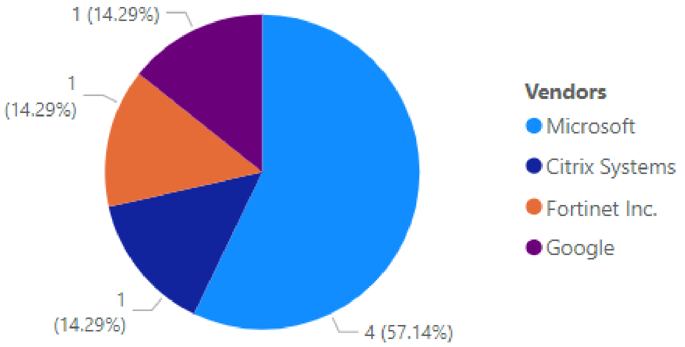
Previous month :	481 *Vendor Patched* (69.81%)
This Month :	**378** Vendor Patched (**73.83%)**

Vendor view

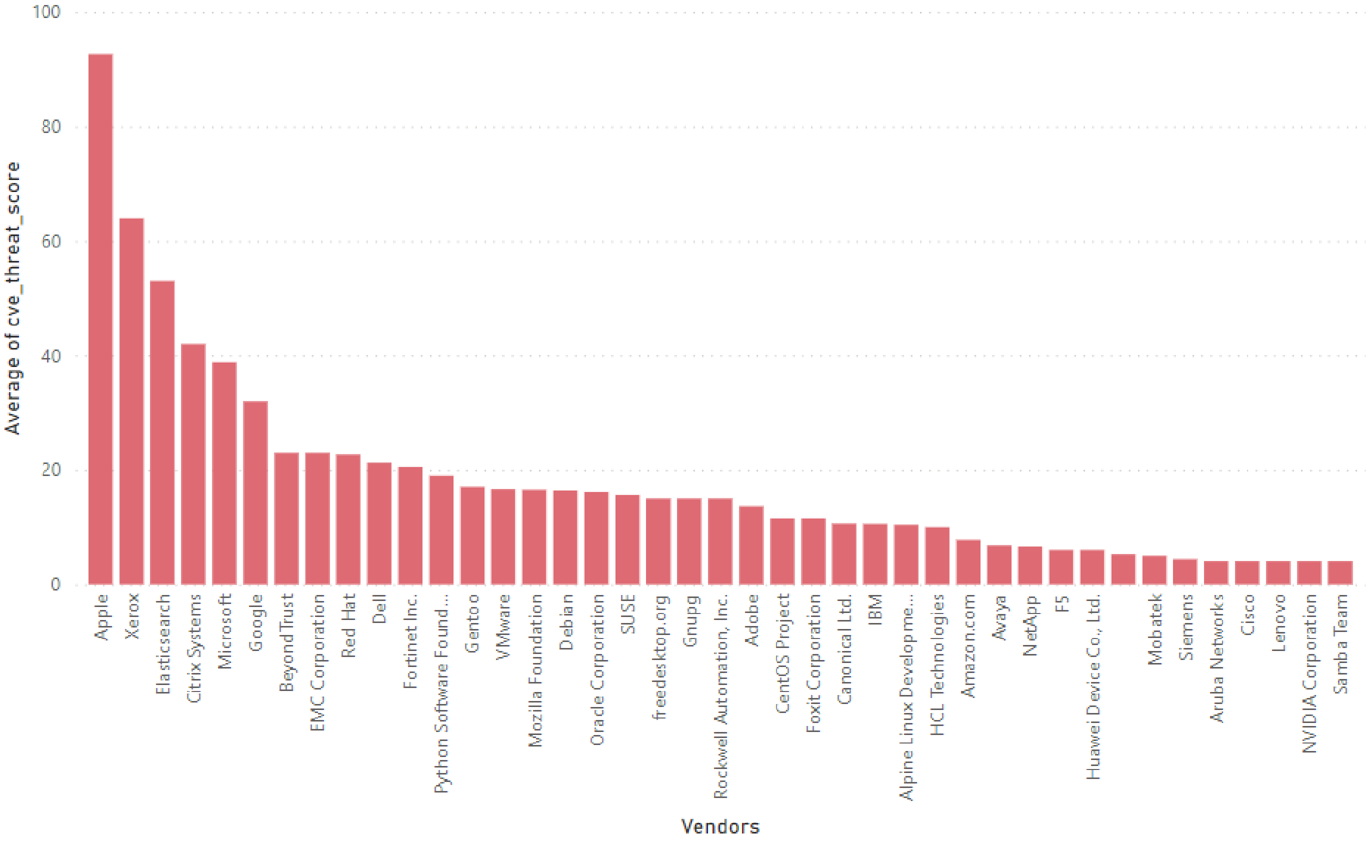
Top vendors with the most advisories



Top vendors with zero-day

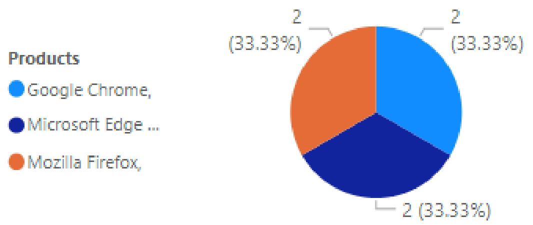


Top Vendors with highest average threat score

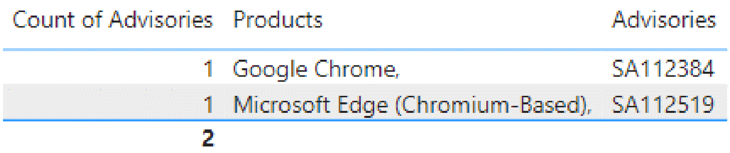


Browser-related advisories

Advisories per browser

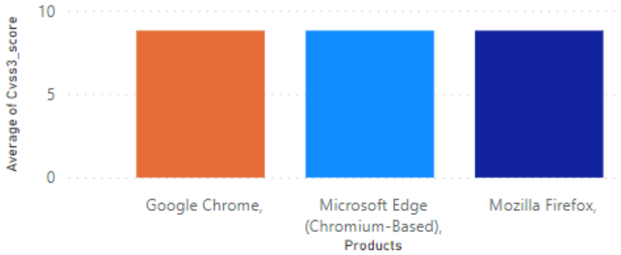


Browser zero-day vulnerabilities

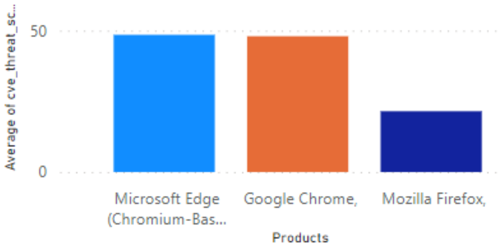


Count of Advisories	Products	Advisories
1	Google Chrome,	SA112384
1	Microsoft Edge (Chromium-Based),	SA112519
2		

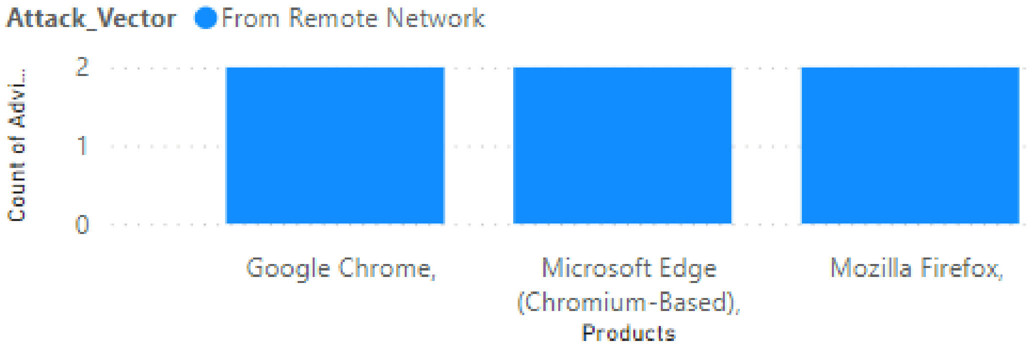
Average CVSS (criticality) score per browser



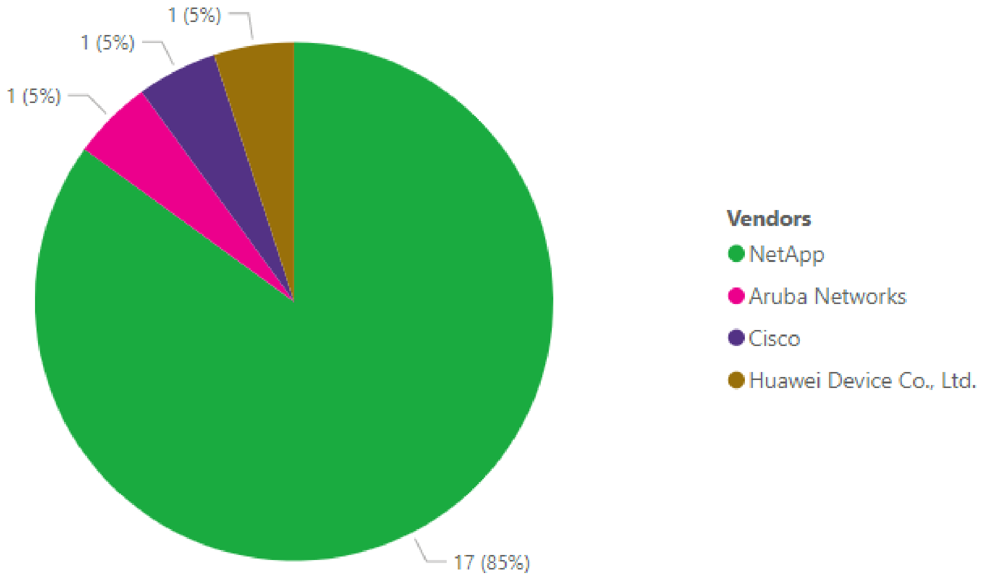
Average threat score per browser



What's the Attack Vector ?



Networking related advisories

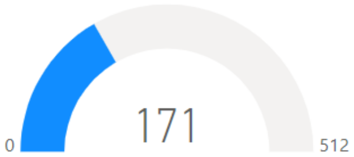


Threat intelligence

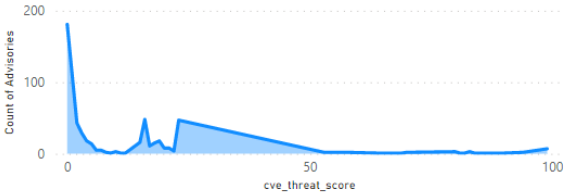
In a world where there are more than 18,000 new vulnerabilities every year, being smart about prioritizing remediation efforts is essential. Leveraging Threat Intelligence, another valuable layer of insight is provided to help you understand which of the vulnerabilities affecting your environment are actually being exploited in the wild.

Leveraging machine learning, artificial intelligence, and human curation from thousands of sources in the open, deep and dark web, Threat Intelligence augments Software Vulnerability Research's vulnerability intelligence with a Threat Score that provides the ultimate prioritization tool for your busy desktop operations teams.

Count of malware-exploited CVEs



Count of advisories by CVE threat score



Threat intelligence advisory statistics:

SAIDs with a threat score (1+)	**331**↓(408)	64.65%
SAIDs with no threat score (=0)	**181**↓*(281)*	35.35%

SAID: Secunia Advisory Identifier

Range	Score		*Last month*
Medium-range threat score SAIDs (13-23)	**175**	↓	***(256)***
Low-range threat score SAIDs (1-12)	**122**	↓	***(120)***
Very critical threat score SAIDs (71-99)	25	↓	*(26)*
Critical-range threat score SAIDs (45-70)	9	↓	*(5)*
High-range threat score SAIDs (24-44)	0	↓	*(1)*

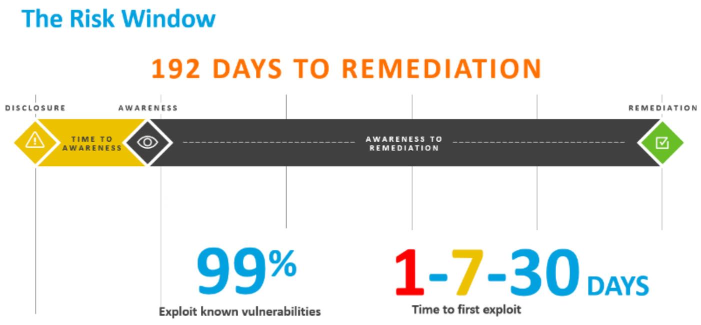
More information about how the Secunia team calculates the threat score :

- Evidence of exploitation
- Criteria for the threat Score Calculation
- Threat Score Calculation - Examples

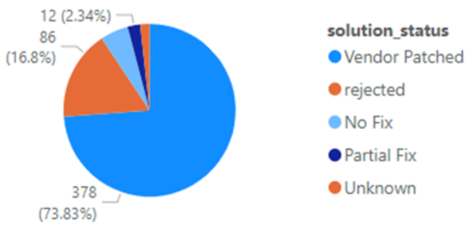
Patching

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

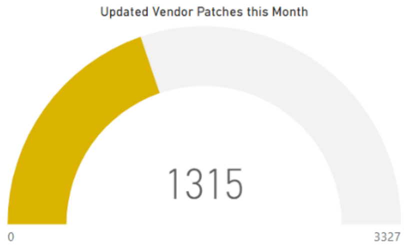


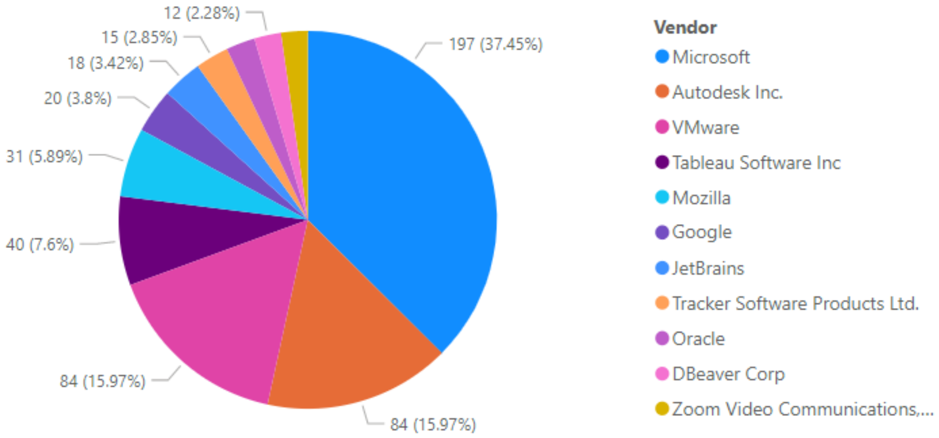
Flexera’s Vendor Patch Module (VPM) statistics

Flexera has the largest third-party patch catalog **(More than 3300)** 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