MONTHLY VULNERABILITY INSIGHTS

Based on Data from Secunia Research

OCTOBER 2023

flexera™

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.

Summary

Total advisories: **1,055** ↑ (last month: **864**).

Again a record breaking month, with **1,055** advisories being reported this month (September: **864**)

2022 was already the record-breaking year with the highest number of Secunia Advisories reported,
however 2023 has already exceeded 2022 in October by more than **10%**!
2023 is on its way to crush 2022 with an approx. **25-35% increase**!

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

- Almost **56.87%** of all vulnerabilities reported in this month have a "**Remote Attack Vector**" (last month 52.2%)
- The Secunia Research Team reported only **6 Extremely** critical advisories this month. (Last month: **11**)
- **18 Zero-Day** Advisories reported. (last month :17) for Cisco, Citrix, Apple, Microsoft, Atlassian and Android
- Over **1,857 unique** CVE's (last month: **1,892**) were covered in the **1055** Advisories.
- Threat Intelligence indicates again that **Moderately Critical Vulnerabilities** are targeted by hackers.
- More than **65%** of all advisories are disclosed by these 5 usual suspect vendors (**Suse, Oracle, Amazon**, **RedHat and Ubuntu**)
- Interestingly among these vendors are also the ones with the most **rejected advisories**:
    - **Amazon**: 24 out of 152 advisories were rejected by the Secunia Research Team.
    - **SUSE:** 22 out of 152
    - **Ubuntu:** 17 out of 152
    - **RedHat:** 4 out of 152
- **Juniper and F5** contributed to more than 70% of all Networking related Advisories this month.

Last month we reported that 72.11% of all Secunia Advisories had a **Threat** (exploits, malware, ransomware, etc.) associated with them, **this month** the number has been **higher** to **73.36%**

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 global threats, 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 can 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 and/or events this month:

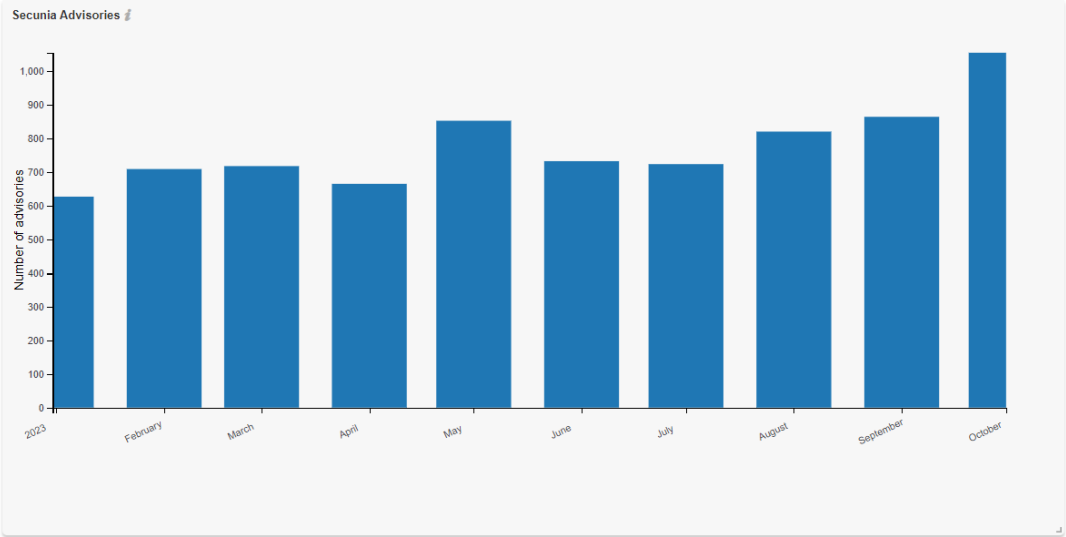
- Oct. 4: Atlassian has disclosed an actively exploited critical zero-day vulnerability in publicly accessible Confluence Data Center and Server instances. There is evidence that a known nation-state actor is actively exploiting CVE-2023-22515.
- Oct. 4: Apple rolls out security patches for actively exploited iOS Zero-Day Vulnerability (CVE-2023-42824) for iOS **prior to 16.6**.
- Oct.10: Microsoft Patch Tuesday released 103 **Microsoft** including **two zero-day CVE's** that have been actively exploited by malicious cyber actors. Secunia Research has bundled them in 10 Zero-day Advisories.
- Oct.10: Multiple **zero-day** vulnerabilities have been discovered in **NetScaler** ADC (formerly **Citrix** ADC) and NetScaler Gateway (formerly Citrix Gateway
- Oct.16: 2 **zero-day** Vulnerabilities in **CISCO** IOS XE Software Web UI Feature that can be used in a sophisticated attack using first CVE-2023-20198 to gain access and then exploit CVE-2023-20273 to elevate privilege to root.
- Oct.25: A malicious actor with network access to **VMWare vCenter** Server may trigger an out-of-bounds write potentially leading to remote code execution. (CVE-2023-34048)

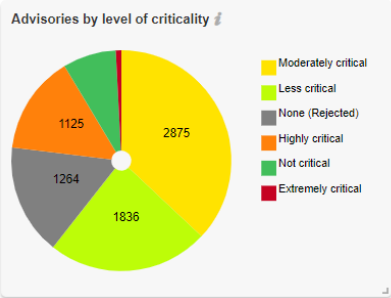
Interesting sources of information:

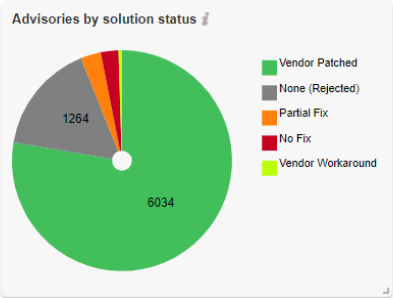
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- https://www.bleepingcomputer.com/news/security/
- https://thehackernews.com/search/label/Vulnerability
- https://www.darkreading.com/vulnerability-management?page=1
- https://portswigger.net/daily-swig/vulnerabilities
- https://www.securityweek.com/virus-threats/vulnerabilities

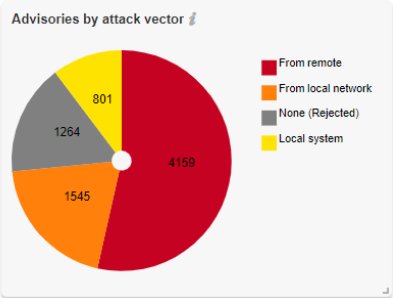
Year-to-date overview

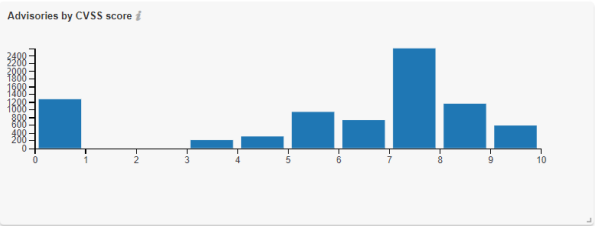
As of **November 1, 2023**, the year-to-date total is at **7,769** Advisories ↑ which is higher than 2022 : **5,896** YTD Advisories)

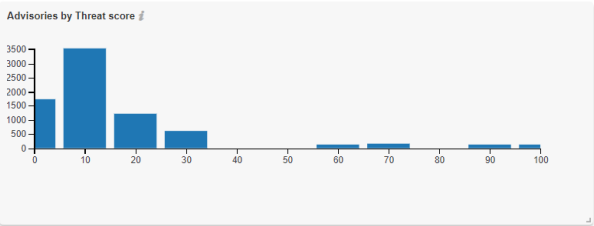












Monthly data

This month, a total of **1055** ↑ (last month: **864**) advisories were reported by the Secunia Research Team.

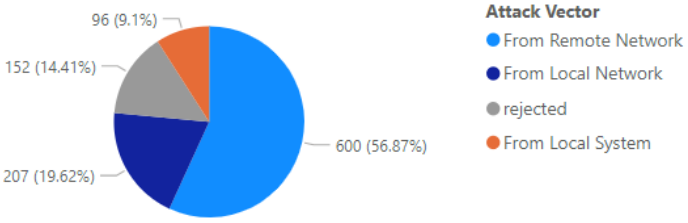
This month:	#	Change *(last month):*
Total # of advisories	**1055**	↑ ***(864)***
Unique Vendors	**101**	↑ ***(89)***
Unique Products	**383**	↑ ***(348)***
Unique Versions	**482**	↑ ***(439)***
Rejected Advisories *	**152**	↑ ***(151)***
Total Unique CVE ID's reported	**1856**	↑ **(1893)**

↑ increased ↓lower ↔ same

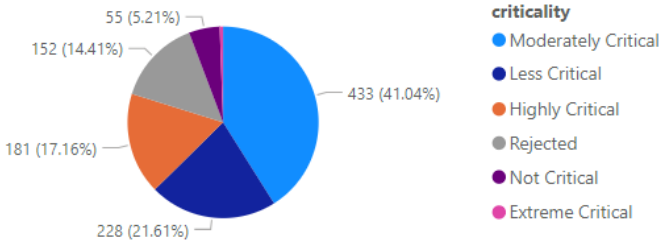
** **152** advisories have received the "rejected" status which means in general that leveraging it would require one or more violations of security best practices (e.g., product not securely configured or not used securely) or that it was "too weak of a gain" (e.g., administrative, local users already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



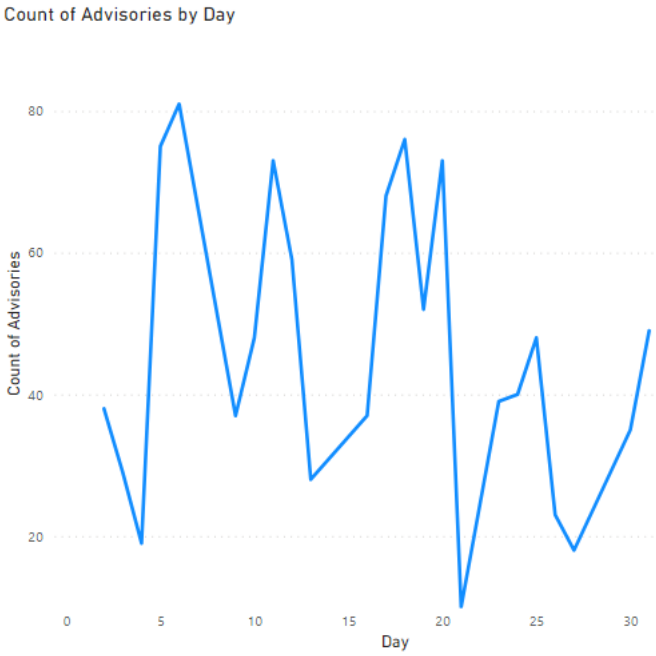
Advisories by criticality



Advisories per day

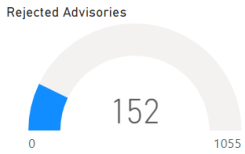
Below an overview of the daily advisory count.

Year	Month	Day	# of Advisories
2023	October	2	38
2023	October	3	29
2023	October	4	19
2023	October	5	75
2023	October	6	81
2023	October	9	37
2023	October	10	48
2023	October	11	73
2023	October	12	59
2023	October	13	28
2023	October	16	37
2023	October	17	68
2023	October	18	76
2023	October	19	52
2023	October	20	73
2023	October	21	10
2023	October	23	39
2023	October	24	40
2023	October	25	48
2023	October	26	23
2023	October	27	18
2023	October	30	35
2023	October	31	49
Total			**1055**



Rejected advisories.

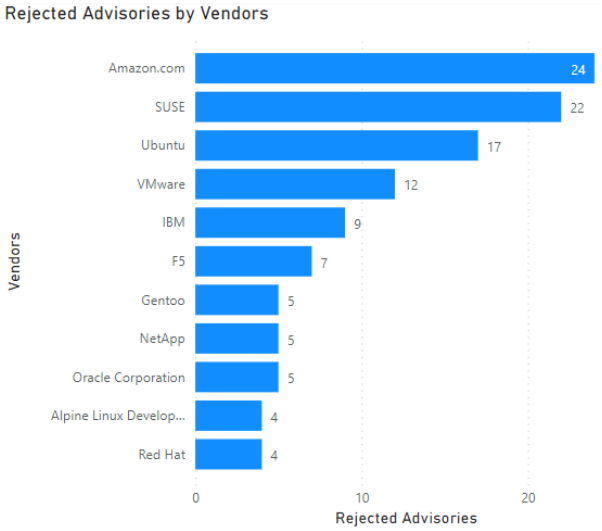
There are many vulnerabilities posted to the National Vulnerability Database (NVD) by a lot of people and companies. They are not always valid, assigned a proper criticality, and in some cases, a vulnerability may be legitimate but not afford the attacker any benefit.

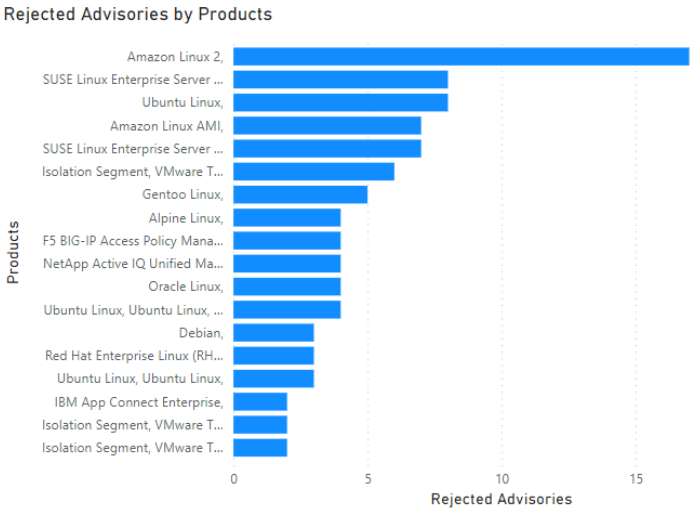


The Secunia Research team at Flexera evaluates vulnerabilities from hundreds of sources, rescores them when necessary and even rejects vulnerabilities not worth your attention. Rejection Advisories help you to reduce the volume of vulnerabilities to be mitigated by helping you focus only on those that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

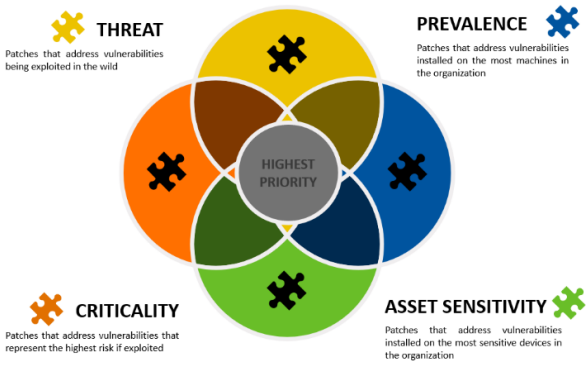
- What systems would result in the most risk if compromised?
- Is it a high-risk device? **Patch**.

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.

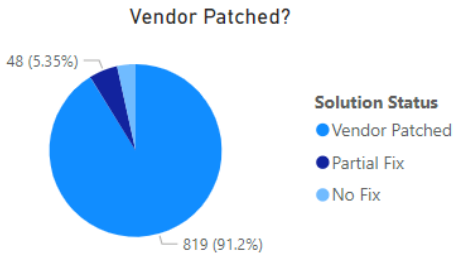
criticality	avg threat score x # of advisories
Moderately Critical	14,205.00
Highly Critical	6,869.00
Less Critical	2,596.00
Extreme Critical	516.00
Not Critical	320.00
Total	**24,506.00**

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.

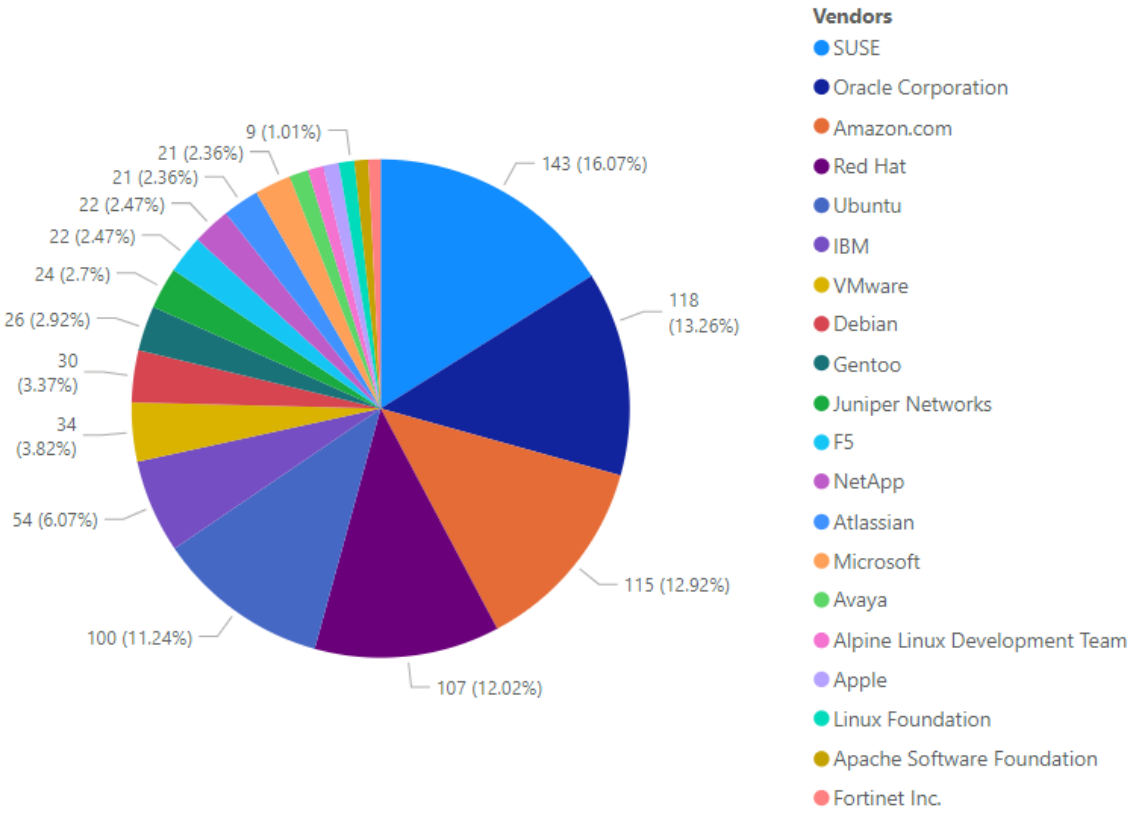
Take away 2:

Most vulnerabilities have a patch available (typically within 24 hours after disclosure).
(No fix : no patch available for this insecure version, therefore need to upgrade)

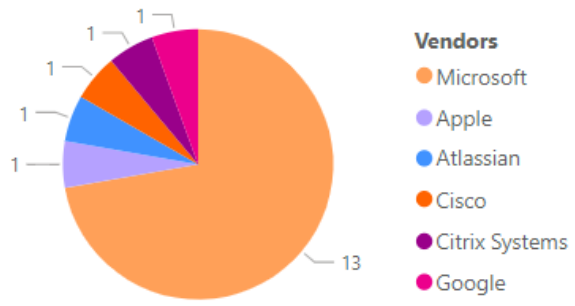


Vendor view

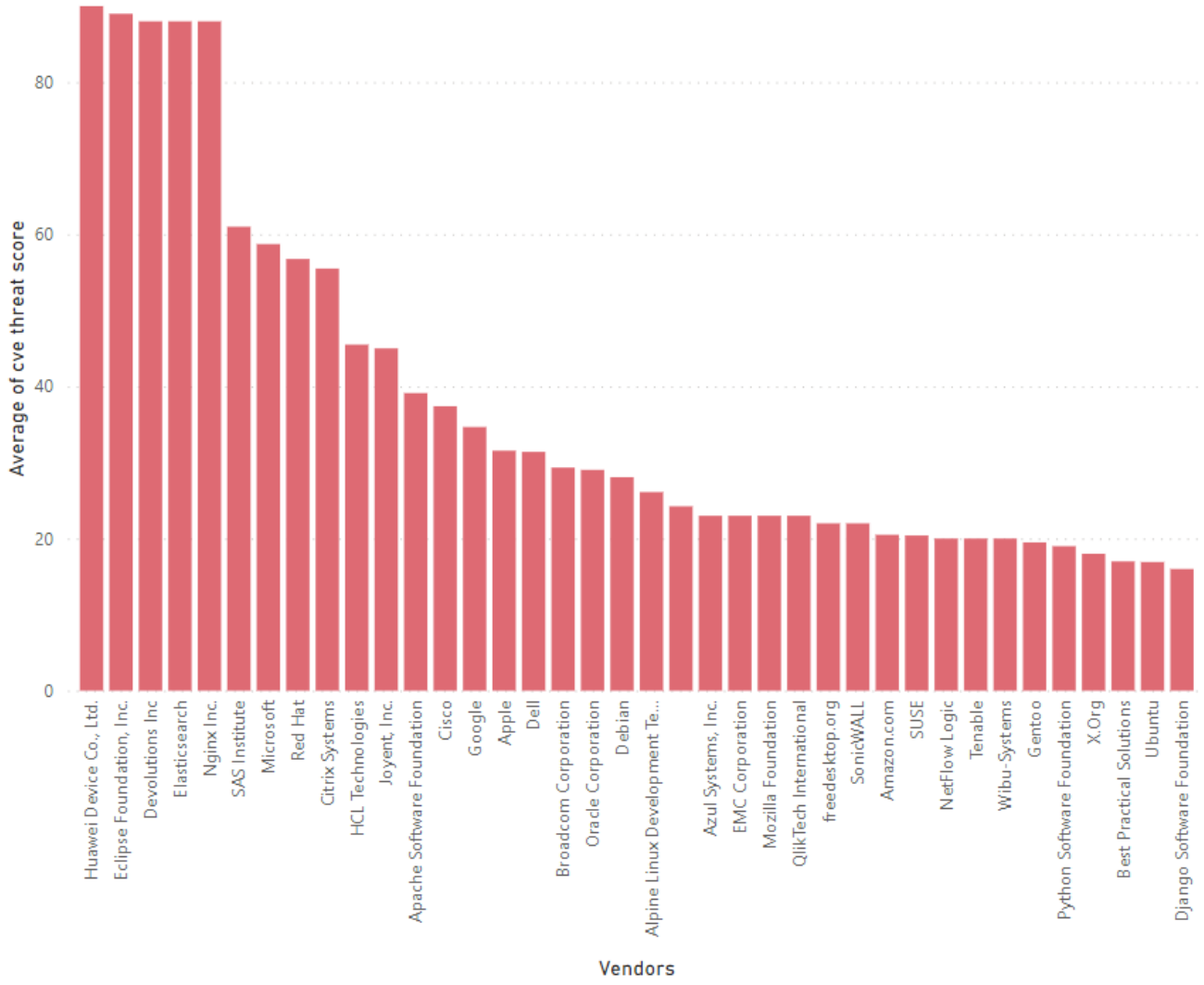
Top vendors with the most advisories



Top vendors with zero-day

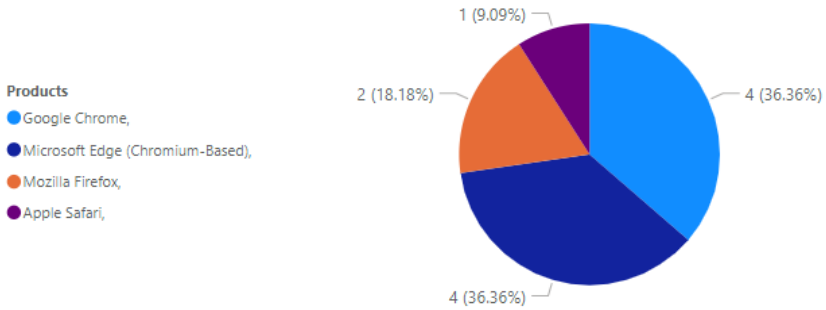


Top Vendors with highest average threat score



Browser-related advisories

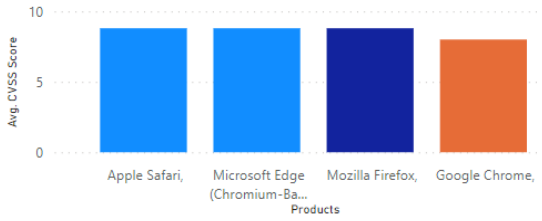
Advisories per browser



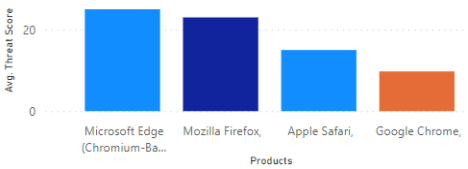
Browser zero-day vulnerabilities

Count of Advisories	Products	Advisories
1	Microsoft Edge (Chromium-Based),	SA119898
1		

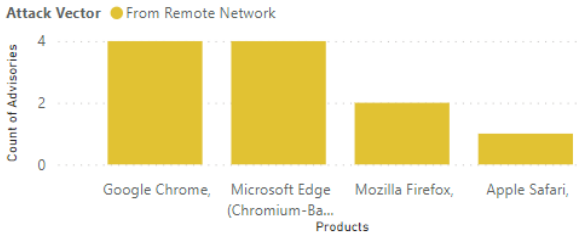
Average CVSS (criticality) score per browser



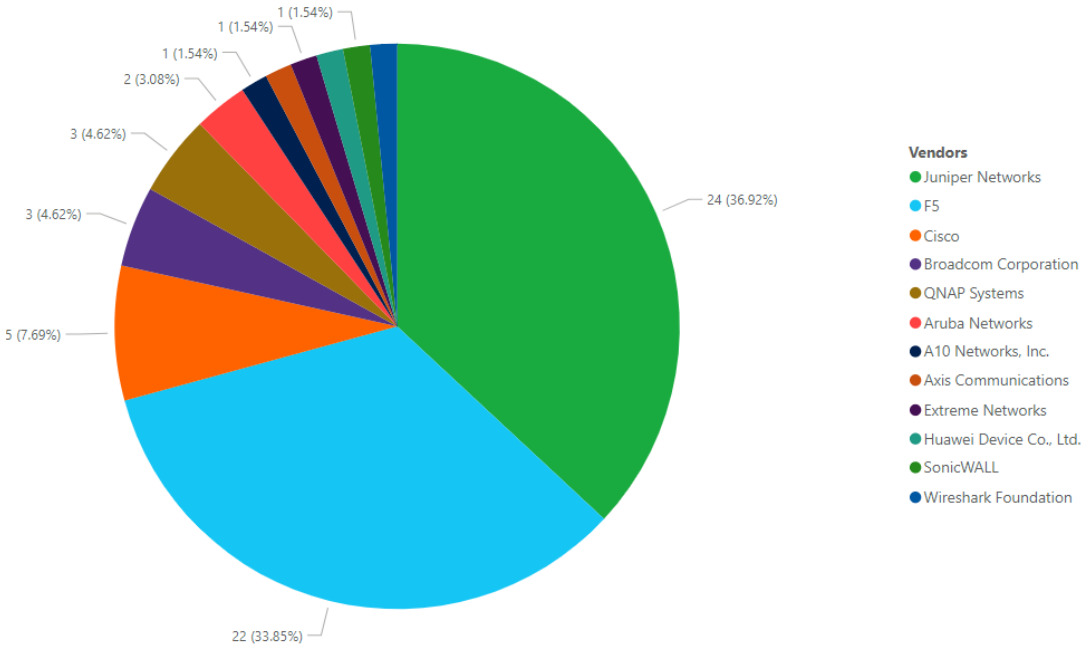
Average threat score per browser



What's the Attack Vector?



Networking related advisories

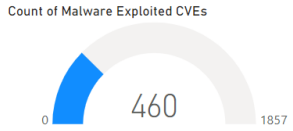


Threat intelligence

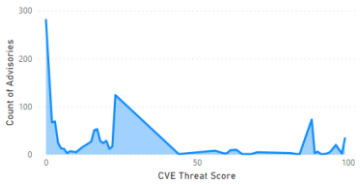
In a world where there are more than 18,000 new vulnerabilities every year, being smart about prioritizing remediation efforts is essential. Leveraging Threat Intelligence, another valuable layer of insight is provided to help you understand which of the vulnerabilities affecting your environment are 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+)	**774**↑(623)	73.36%
SAIDs with no threat score (=0)	**281**↑*(241)*	26.64%

SAID: Secunia Advisory Identifier

Range	# SAIDS	*Last month*
Medium-range threat score SAIDs (13-23)	**365** ↓	*(403)*
Low-range threat score SAIDs (1-12)	**216** ↑	*(149)*
Very critical threat score SAIDs (71-99)	152 ↑	*(60)*
Critical-range threat score SAIDs (45-70)	40 ↑	*(4)*
High-range threat score SAIDs (24-44)	1 ↓	*(7)*

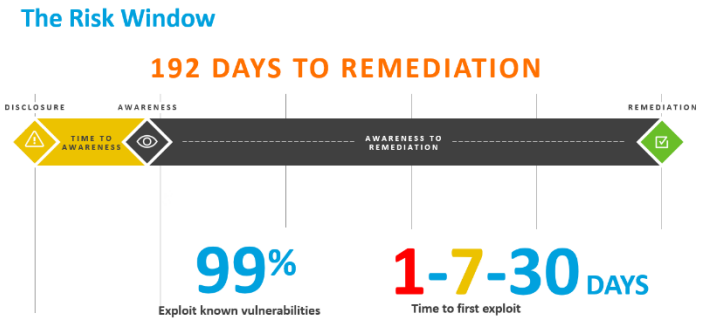
More information about how the Secunia team calculates the threat score :

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

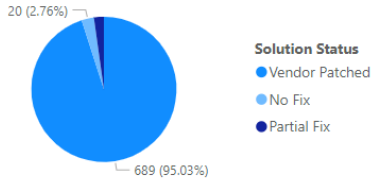
Patching

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

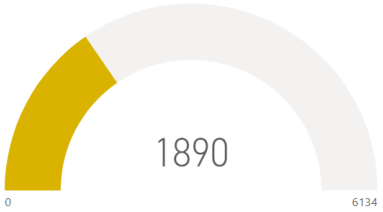


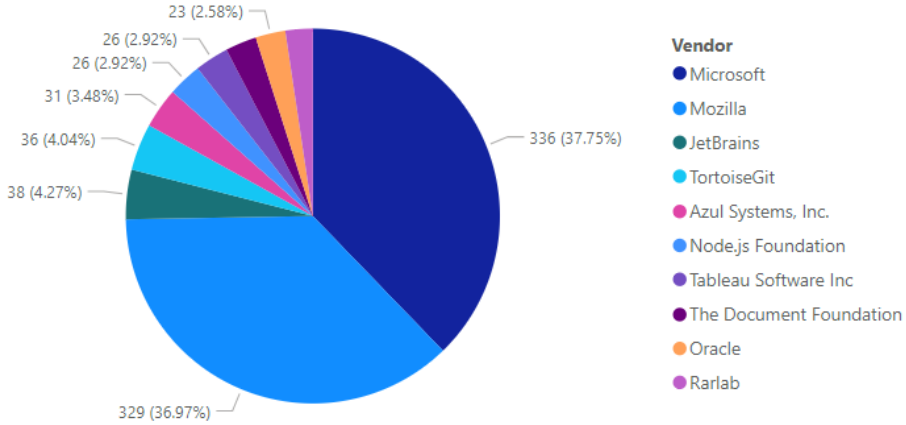
Flexera's Vendor Patch Module (VPM) statistics

Flexera has the largest third-party patch catalog **(More than 6,000)** 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, NOT including MS Patch Tuesday patches)





Other sources

CISA

For the benefit of the cybersecurity community and network defenders—and to help every organization better manage vulnerabilities and keep pace with threat activity—CISA maintains the authoritative source of vulnerabilities that have been exploited in the wild: the Known Exploited Vulnerability (KEV) catalog. CISA strongly recommends all organizations review and monitor the KEV catalog and prioritize remediation of the listed vulnerabilities to reduce the likelihood of compromise by known threat actors.

This months' the additions to the KEV catalog

First column "Day" is the date added to KEV Catalog.

Day	CVE	Vendor	Product	Month	Day
2	CVE-2023-5217	Google	Chrome libvpx	October	23
3	CVE-2023-4211	Arm	Mali GPU Kernel Driver	October	24
4	CVE-2023-28229	Microsoft	Windows CNG Key Isolation Service	October	25
4	CVE-2023-42793	JetBrains	TeamCity	October	25
5	CVE-2023-22515	Atlassian	Confluence Data Center and Server	October	13
5	CVE-2023-40044	Progress	WS_FTP Server	October	26
5	CVE-2023-42824	Apple	iOS and iPadOS	October	26
10	CVE-2023-20109	Cisco	IOS and IOS XE	October	31
10	CVE-2023-21608	Adobe	Acrobat and Reader	October	31
10	CVE-2023-36563	Microsoft	WordPad	October	31
10	CVE-2023-41763	Microsoft	Skype for Business	October	31
10	CVE-2023-44487	IETF	HTTP/2	October	31
16	CVE-2023-20198	Cisco	IOS XE Web UI	October	20
18	CVE-2023-4966	Citrix	NetScaler ADC and NetScaler Gateway	November	8
23	CVE-2023-20273	Cisco	Cisco IOS XE Web UI	October	27
26	CVE-2023-5631	Roundcube	Webmail	November	16
31	CVE-2023-46747	F5	BIG-IP Configuration Utility	November	21
31	CVE-2023-46748	F5	BIG-IP Configuration Utility	November	21

Due Date this month

CISA adds known exploited vulnerabilities to the catalog when there is a clear action for the affected organization to take. The remediation action referenced in BOD 22-01 requires federal civilian executive branch (FCEB) agencies to take the following actions for all vulnerabilities in the KEV, and
CISA strongly encourages all organizations to do the same:

Month	Day	CVE	Vendor	Product
October	2	CVE-2023-41061	Apple	iOS, iPadOS, and watchOS
October	2	CVE-2023-41064	Apple	iOS, iPadOS, and macOS
October	3	CVE-2023-36761	Microsoft	Word
October	3	CVE-2023-36802	Microsoft	Streaming Service Proxy
October	4	CVE-2023-20269	Cisco	Adaptive Security Appliance and Firepower Threat Defense
October	4	CVE-2023-35674	Android	Framework
October	4	CVE-2023-4863	Google	Chromium WebP
October	5	CVE-2023-26369	Adobe	Acrobat and Reader
October	9	CVE-2014-8361	Realtek	SDK
October	9	CVE-2017-6884	Zyxel	EMG2926 Routers
October	9	CVE-2021-3129	Laravel	Ignition
October	9	CVE-2022-22265	Samsung	Mobile Devices
October	10	CVE-2023-28434	MinIO	MinIO
October	12	CVE-2023-41179	Trend Micro	Apex One and Worry-Free Business Security
October	13	CVE-2023-22515	Atlassian	Confluence Data Center and Server
October	16	CVE-2023-41991	Apple	Multiple Products
October	16	CVE-2023-41992	Apple	Multiple Products
October	16	CVE-2023-41993	Apple	Multiple Products
October	19	CVE-2018-14667	Red Hat	JBoss RichFaces Framework
October	20	CVE-2023-20198	Cisco	IOS XE Web UI
October	23	CVE-2023-5217	Google	Chrome libvpx
October	24	CVE-2023-4211	Arm	Mali GPU Kernel Driver
October	25	CVE-2023-28229	Microsoft	Windows CNG Key Isolation Service
October	25	CVE-2023-42793	JetBrains	TeamCity
October	26	CVE-2023-40044	Progress	WS_FTP Server
October	26	CVE-2023-42824	Apple	iOS and iPadOS
October	27	CVE-2023-20273	Cisco	Cisco IOS XE Web UI
October	31	CVE-2023-20109	Cisco	IOS and IOS XE
October	31	CVE-2023-21608	Adobe	Acrobat and Reader
October	31	CVE-2023-36563	Microsoft	WordPad
October	31	CVE-2023-41763	Microsoft	Skype for Business
October	31	CVE-2023-44487	IETF	HTTP/2

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