MONTHLY VULNERABILITY INSIGHTS

Based on Data from Secunia Research

SEPTEMBER 2024

flexera™

Author: Jeroen Braak

Content

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.

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

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

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

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

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

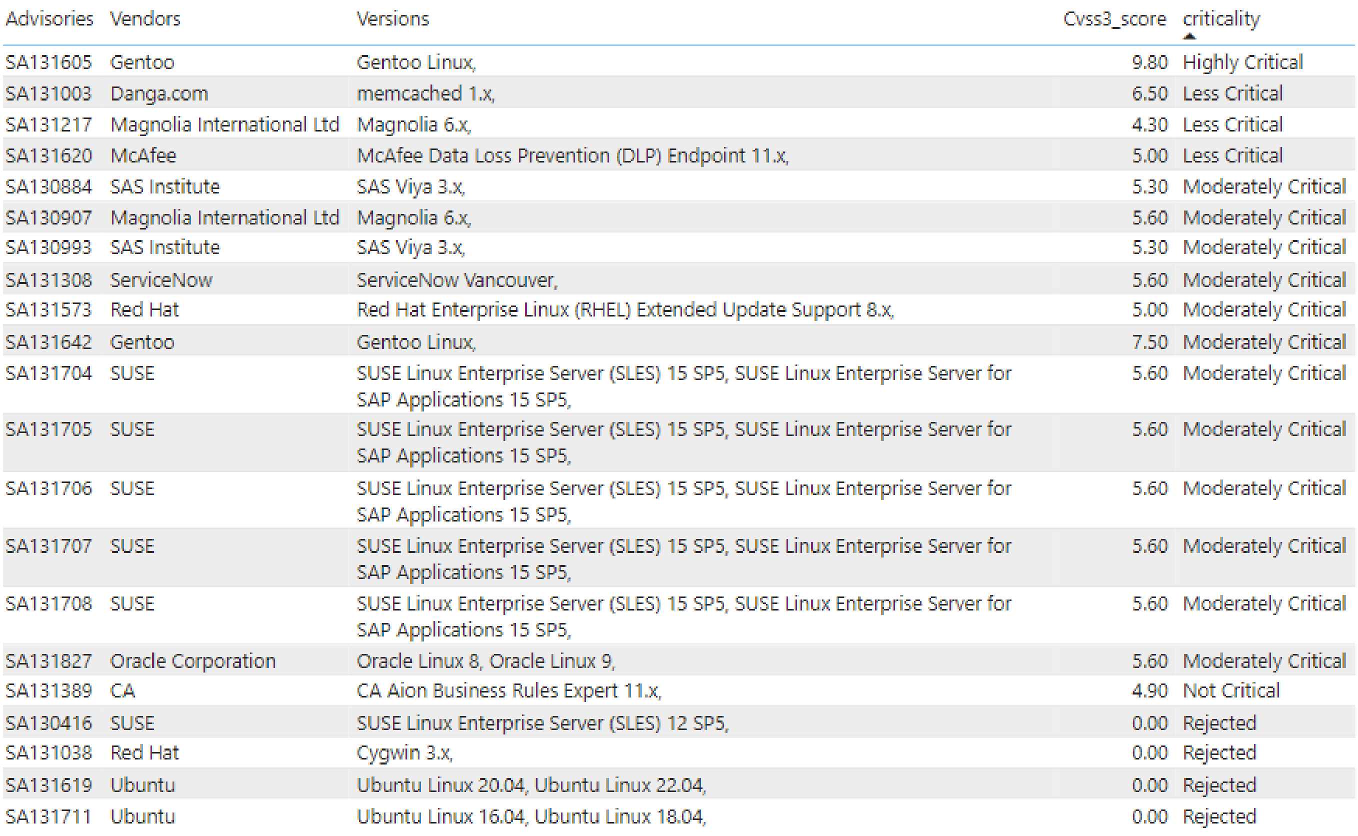
Total advisories: **1,000** ↑ (last month: **975**)

Important conclusions from this month report are:

- With 1,000 advisories, we're keeping the high pace with an average **over 1,000 advisories** per month. (last year ~730)
- This means a serious increase in the number of advisories: **+ 35.8% YTD (**last month +38%)
- **21** (last month:**14**) Advisories do not have a CVE assigned to it including 1 highly critical (Gentoo) see below more info:
- **Less** than half (**43%**) of all vulnerabilities reported in this month have a "Remote Attack Vector" (last month **53.29%**)
- The Secunia Research Team reported **1 Extremely** critical advisories this month (Last month: **8**) for **Microsoft**.
- Threat Intelligence indicates again that **Moderately Critical Vulnerabilities** are targeted by hackers.
- Threat Intel also indicates lower number of links to Cyber Exploits:
  - **108** (***last month:130***) advisories contain at least one vulnerability linked to a **Recent Cyber Exploit**
  - **349** (***last month**:**340)*** advisories contained at least one vulnerability linked to a **Historical Cyber Exploit**.
- More than **half** of all advisories are disclosed by these 4 usual (Linux) suspect vendors (**Linux, Red Hat,SUSE and Ubuntu**)
- Interestingly among these vendors are also the ones with the most **rejected advisories**:
  - **Linux, RedHat, Ubuntu and SUSE** reported **160 out of 248** advisories were rejected.
- The trend is continuing with **Linux Foundation** bombarding the community with many "vulnerabilities", most of them without any threat or risk, nevertheless, researchers need to test and validate the information which is a lot of effort.
- **Cisco** contributed to half of all Networking related Advisories this month
- **Last month** we reported that **52.21%**of all Secunia Advisories had a **Threat** (exploits, malware, ransomware, etc.) associated with them, **this month** the number has been **LOWER to 54.40%**

Using Threat Intelligence is going to help you with prioritizing what needs to be **patched** immediately.

Advisories (Vulnerabilities) without CVE's associated.



Advisories	Vendors	Versions	Cvss3_score	criticality
SA131605	Gentoo	Gentoo Linux,	9.80	Highly Critical
SA131003	Danga.com	memcached 1.x,	6.50	Less Critical
SA131217	Magnolia International Ltd	Magnolia 6.x,	4.30	Less Critical
SA131620	McAfee	McAfee Data Loss Prevention (DLP) Endpoint 11.x,	5.00	Less Critical
SA130884	SAS Institute	SAS Viya 3.x,	5.30	Moderately Critical
SA130907	Magnolia International Ltd	Magnolia 6.x,	5.60	Moderately Critical
SA130993	SAS Institute	SAS Viya 3.x,	5.30	Moderately Critical
SA131308	ServiceNow	ServiceNow Vancouver,	5.60	Moderately Critical
SA131573	Red Hat	Red Hat Enterprise Linux (RHEL) Extended Update Support 8.x,	5.00	Moderately Critical
SA131642	Gentoo	Gentoo Linux,	7.50	Moderately Critical
SA131704	SUSE	SUSE Linux Enterprise Server (SLES) 15 SP5, SUSE Linux Enterprise Server for SAP Applications 15 SP5,	5.60	Moderately Critical
SA131705	SUSE	SUSE Linux Enterprise Server (SLES) 15 SP5, SUSE Linux Enterprise Server for SAP Applications 15 SP5,	5.60	Moderately Critical
SA131706	SUSE	SUSE Linux Enterprise Server (SLES) 15 SP5, SUSE Linux Enterprise Server for SAP Applications 15 SP5,	5.60	Moderately Critical
SA131707	SUSE	SUSE Linux Enterprise Server (SLES) 15 SP5, SUSE Linux Enterprise Server for SAP Applications 15 SP5,	5.60	Moderately Critical
SA131708	SUSE	SUSE Linux Enterprise Server (SLES) 15 SP5, SUSE Linux Enterprise Server for SAP Applications 15 SP5,	5.60	Moderately Critical
SA131827	Oracle Corporation	Oracle Linux 8, Oracle Linux 9,	5.60	Moderately Critical
SA131389	CA	CA Aion Business Rules Expert 11.x,	4.90	Not Critical
SA130416	SUSE	SUSE Linux Enterprise Server (SLES) 12 SP5,	0.00	Rejected
SA131038	Red Hat	Cygwin 3.x,	0.00	Rejected
SA131619	Ubuntu	Ubuntu Linux 20.04, Ubuntu Linux 22.04,	0.00	Rejected
SA131711	Ubuntu	Ubuntu Linux 16.04, Ubuntu Linux 18.04,	0.00	Rejected

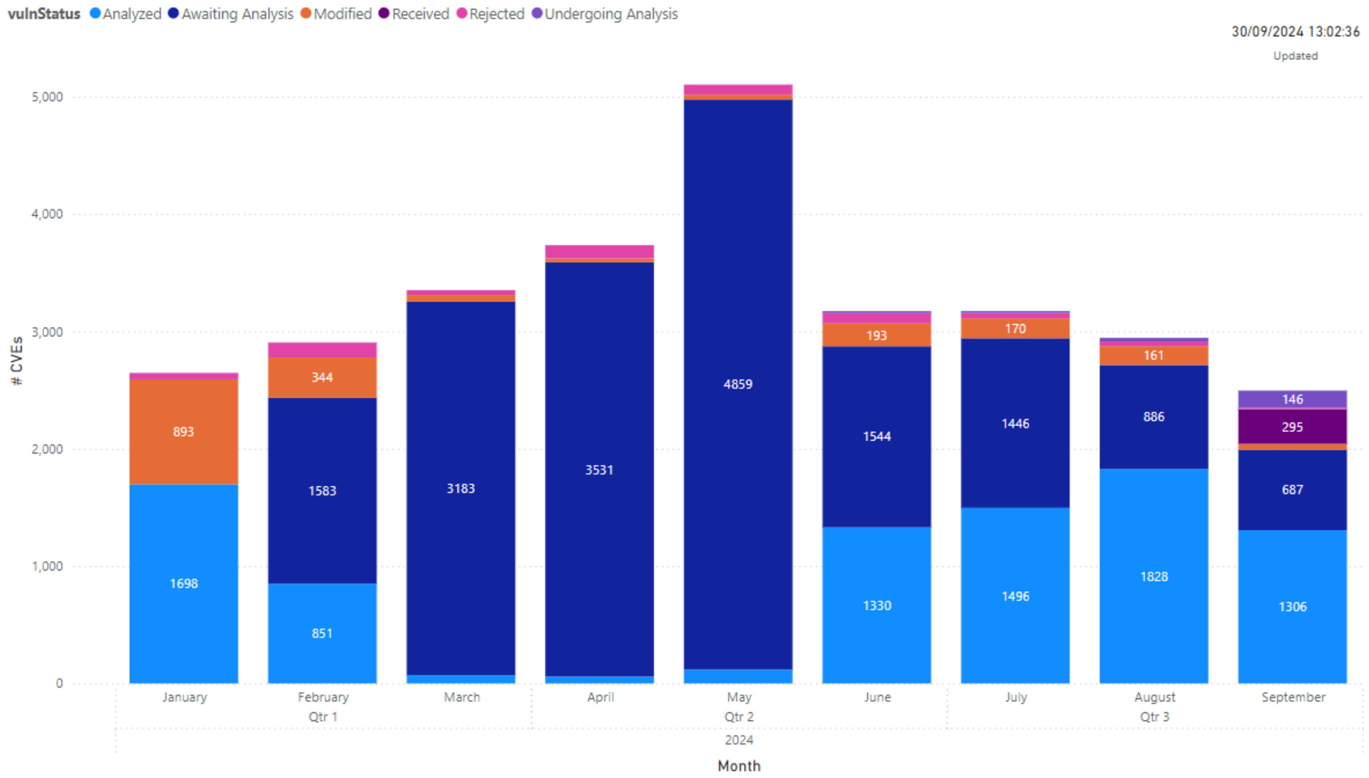
NVD Update

The bad news:
The NVD is still grappling with a significant backlog of over 17,000 CVEs year-to-date, which started in mid-February 2024. This has led to a state of unreliability in many data feeds and vulnerability management solutions that depend on timely NVD updates.

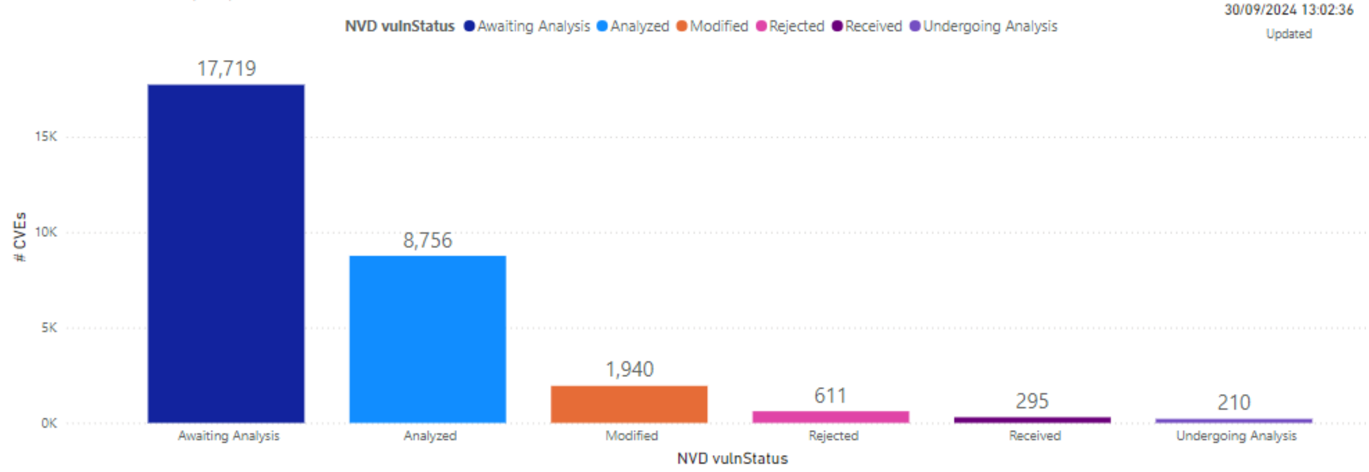
We strongly recommend leveraging trusted Software Vulnerability and Threat Intelligence sources like Flexera's Software Vulnerability Manager (SVM) or Software Vulnerability Research (SVR). Unlike the NVD, these solutions remain unaffected by the delays and continue to provide reliable, accurate, real-time vulnerability and threat intelligence.

The good news:
The NVD has started to make progress in processing its backlog and is improving the speed of its analytics. However, the rate of new CVE disclosures still exceeds what the NVD team and their contractors can handle.

For those seeking a "free" alternative, CISA's vulnrichment tool can be an option to consider.

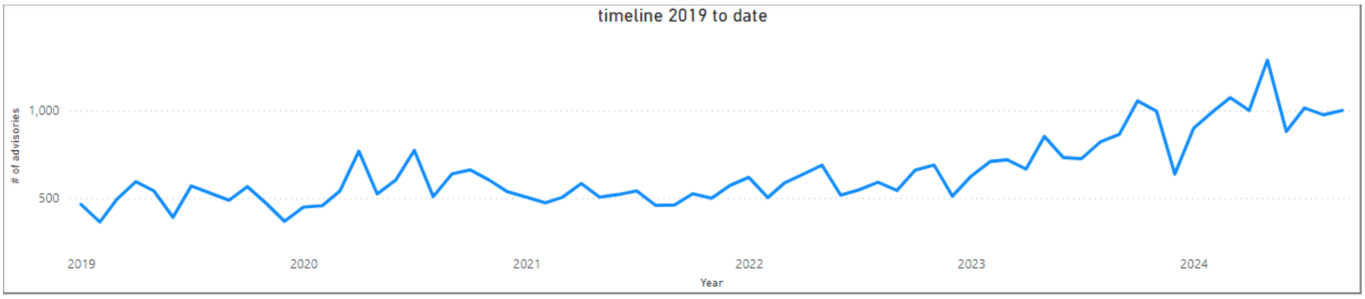


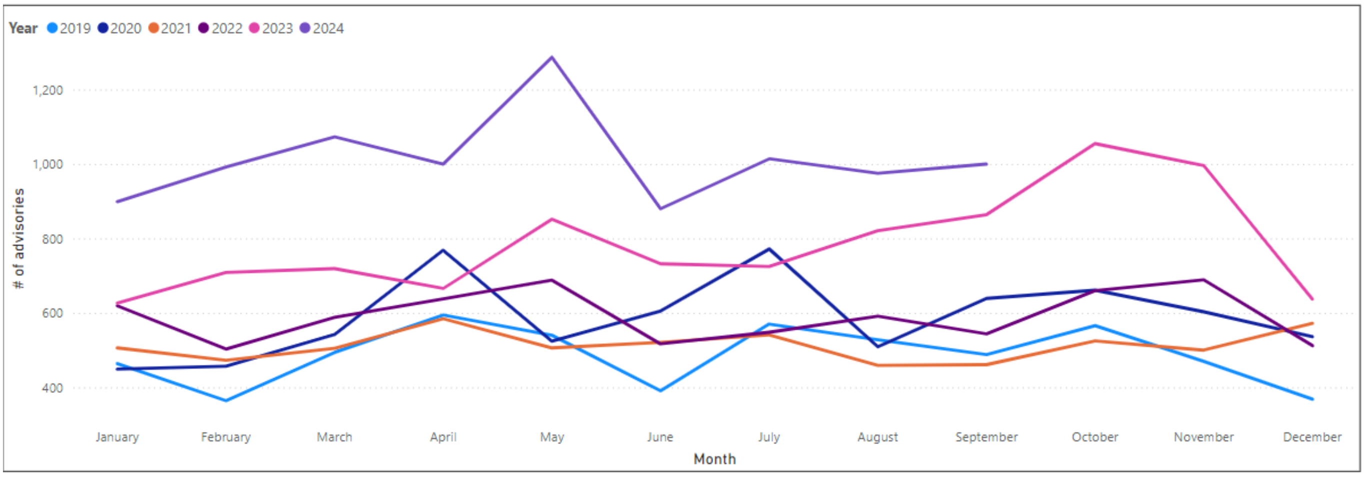
2024 NVD VulnStatus (YTD)

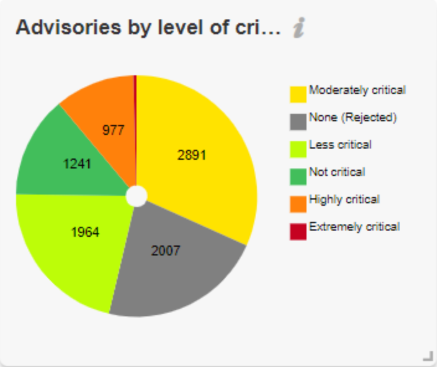


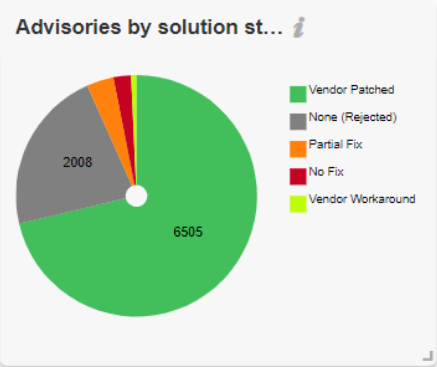
Year-to-date overview

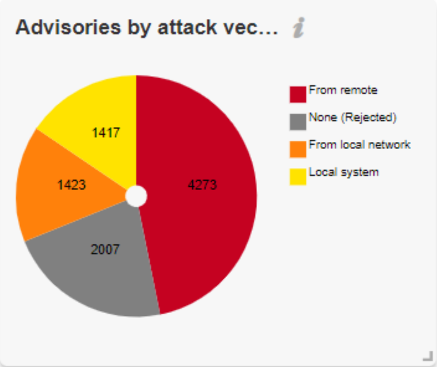
As of **September 30, 2024**, the year-to-date total is **9,120** Advisories ↑ which is 35.8% higher than 2023: **6,714** YTD Advisories)

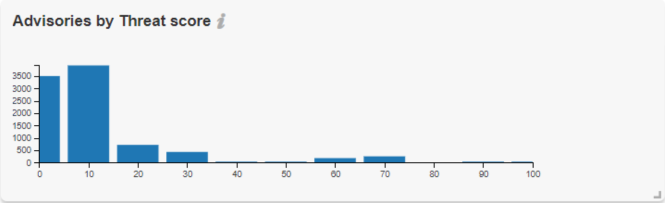

timeline 2019 to date

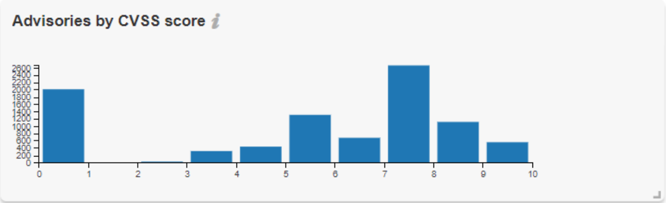



Advisories by level of cri...


Advisories by solution st...


Advisories by attack vec...


Advisories by Threat score


Advisories by CVSS score

Monthly data

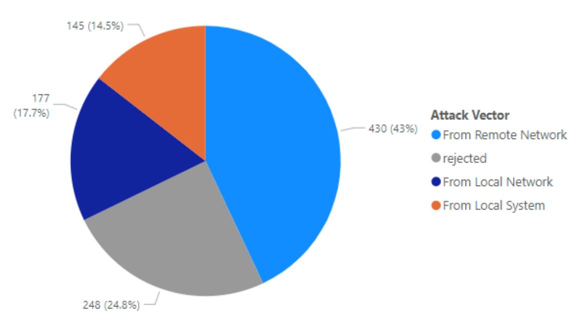
This month, a total of **1,000** ↑ (last month: **975**) advisories were reported by the Secunia Research Team.

This month:	**#**	**Change** *(last month):*
Total # of advisories	**1,000**	↑ ***(975)***
Unique Vendors	**85**	↑ ***(81)***
Unique Products	**304**	↑ **(290*)***
Unique Versions	**411**	↑ ***(359)***
Rejected Advisories *	**248**	↑ ***(245)***
NEW Advisories without CVE ID	**21**	↑ ***(14)***
Advisories with Threat Score (>0)	**544**	↑ **(509)**
Total Unique CVE ID's reported	**2,234**	↓ **(2,837)**
		↑ increased ↓lower ↔ same

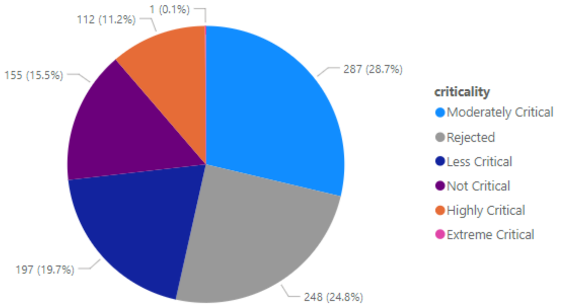
** **248** advisories have received the "rejected" status which means in general that leveraging it would require one or more violations of security best practices (e.g., product not securely configured or not used securely) or that it was "too weak of a gain" (e.g., administrative, local users already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

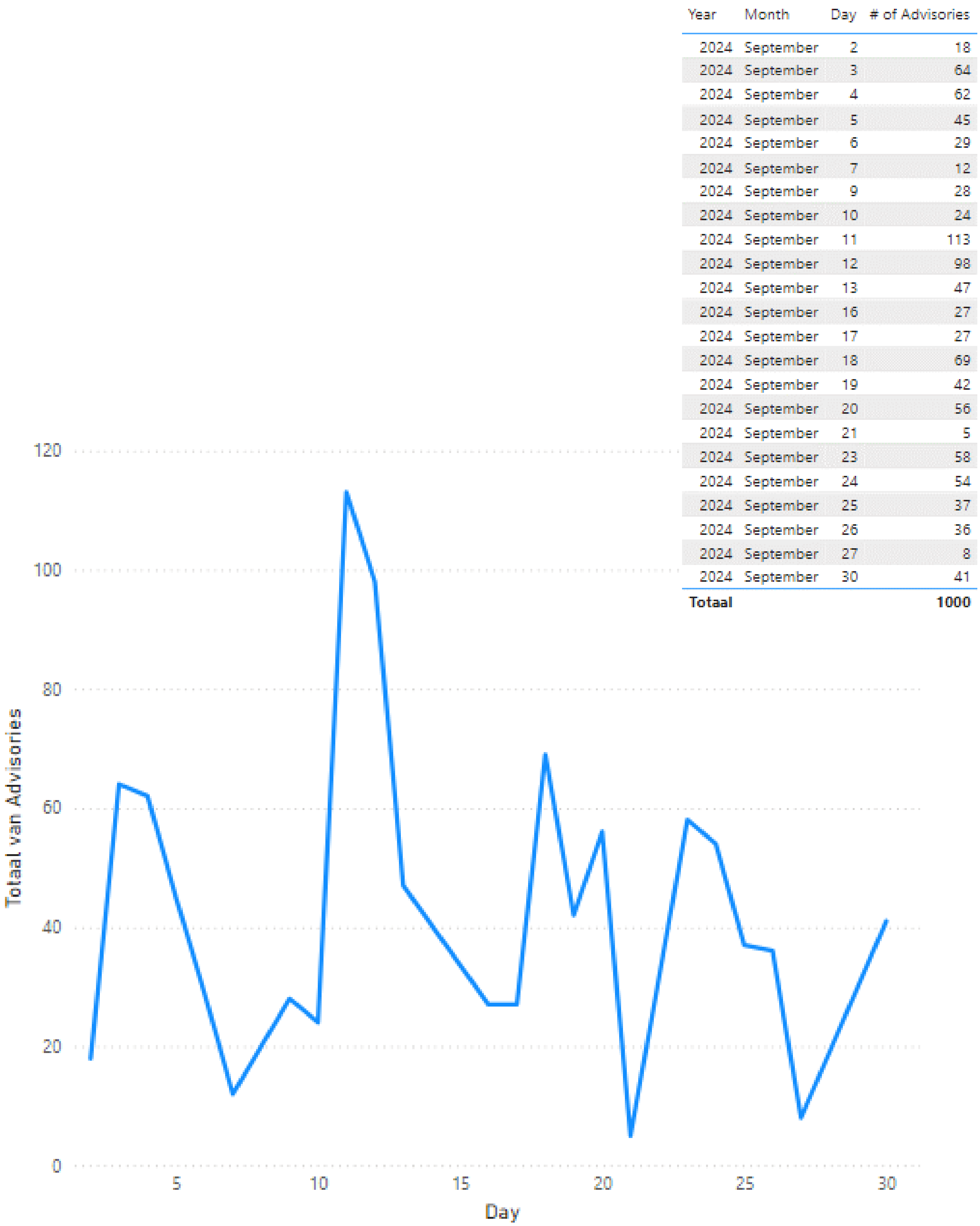


Advisories by criticality



Advisories per day

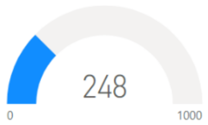
Below an overview of the daily advisory count.



Year	Month	Day	# of Advisories
2024	September	2	18
2024	September	3	64
2024	September	4	62
2024	September	5	45
2024	September	6	29
2024	September	7	12
2024	September	9	28
2024	September	10	24
2024	September	11	113
2024	September	12	98
2024	September	13	47
2024	September	16	27
2024	September	17	27
2024	September	18	69
2024	September	19	42
2024	September	20	56
2024	September	21	5
2024	September	23	58
2024	September	24	54
2024	September	25	37
2024	September	26	36
2024	September	27	8
2024	September	30	41
Totaal			**1000**

Rejected advisories.

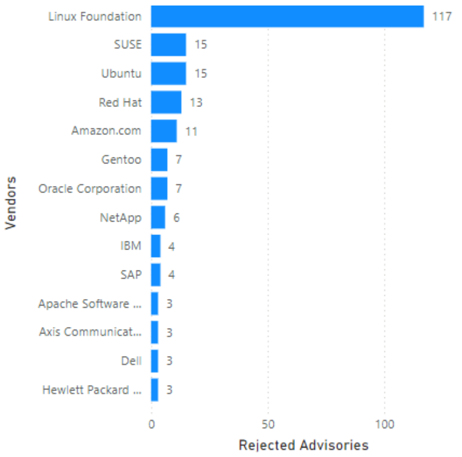
There are many vulnerabilities posted to the National Vulnerability Database (NVD) by a lot of people and companies. They are not always valid, assigned a proper criticality, and in some cases, a vulnerability may be legitimate but not afford the attacker any benefit.

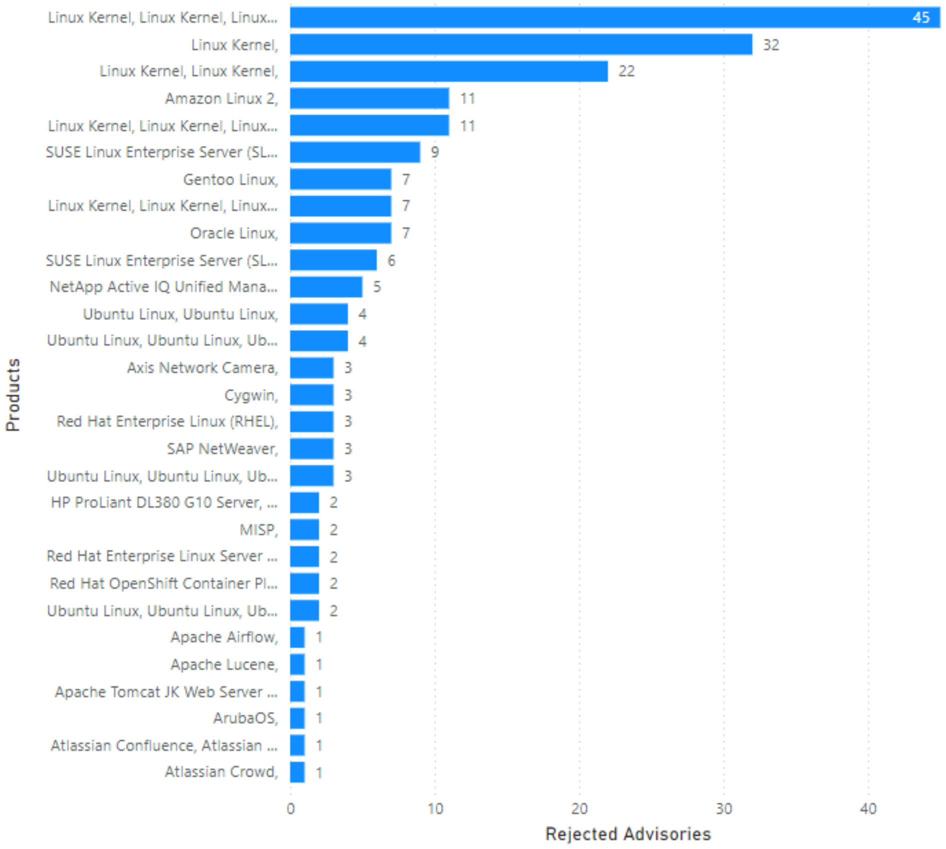


The Secunia Research team at Flexera evaluates vulnerabilities from hundreds of sources, rescores them when necessary and even rejects vulnerabilities not worth your attention. Rejection Advisories help you to reduce the volume of vulnerabilities to be mitigated by helping you focus only on those that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

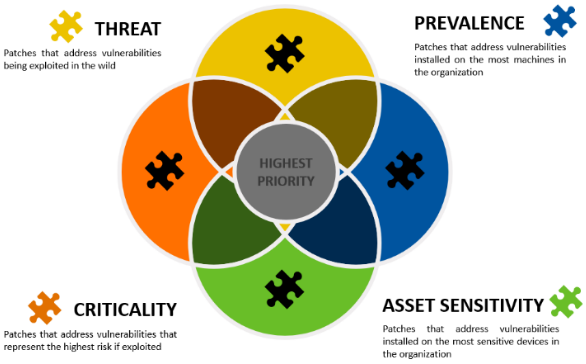
- What systems would result in the most risk if compromised?
- Is it a high-risk device? **Patch**.

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**.



Patches that address vulnerabilities being exploited in the wild

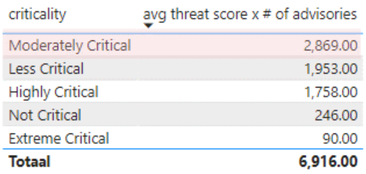
Patches that address vulnerabilities installed on the most machines in the organization

Patches that address vulnerabilities that represent the highest risk if exploited

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.



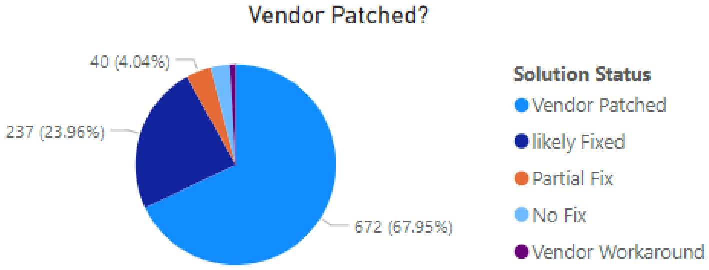
criticality	avg threat score x # of advisories
Moderately Critical	2,869.00
Less Critical	1,953.00
Highly Critical	1,758.00
Not Critical	246.00
Extreme Critical	90.00
Totaal	**6,916.00**

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.

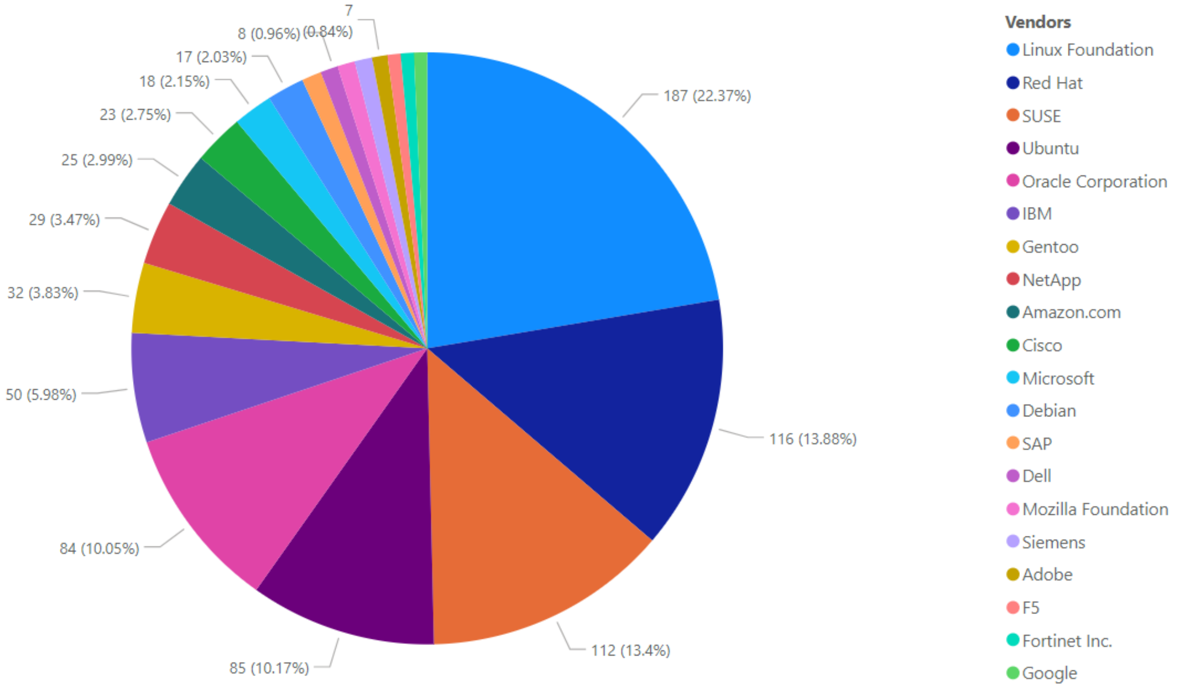
Take away 2:

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)

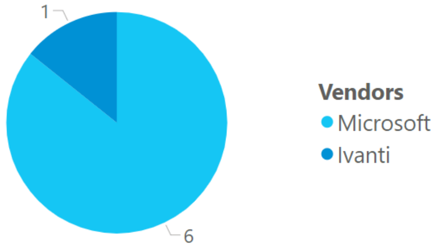


Vendor view

Top vendors with the most advisories

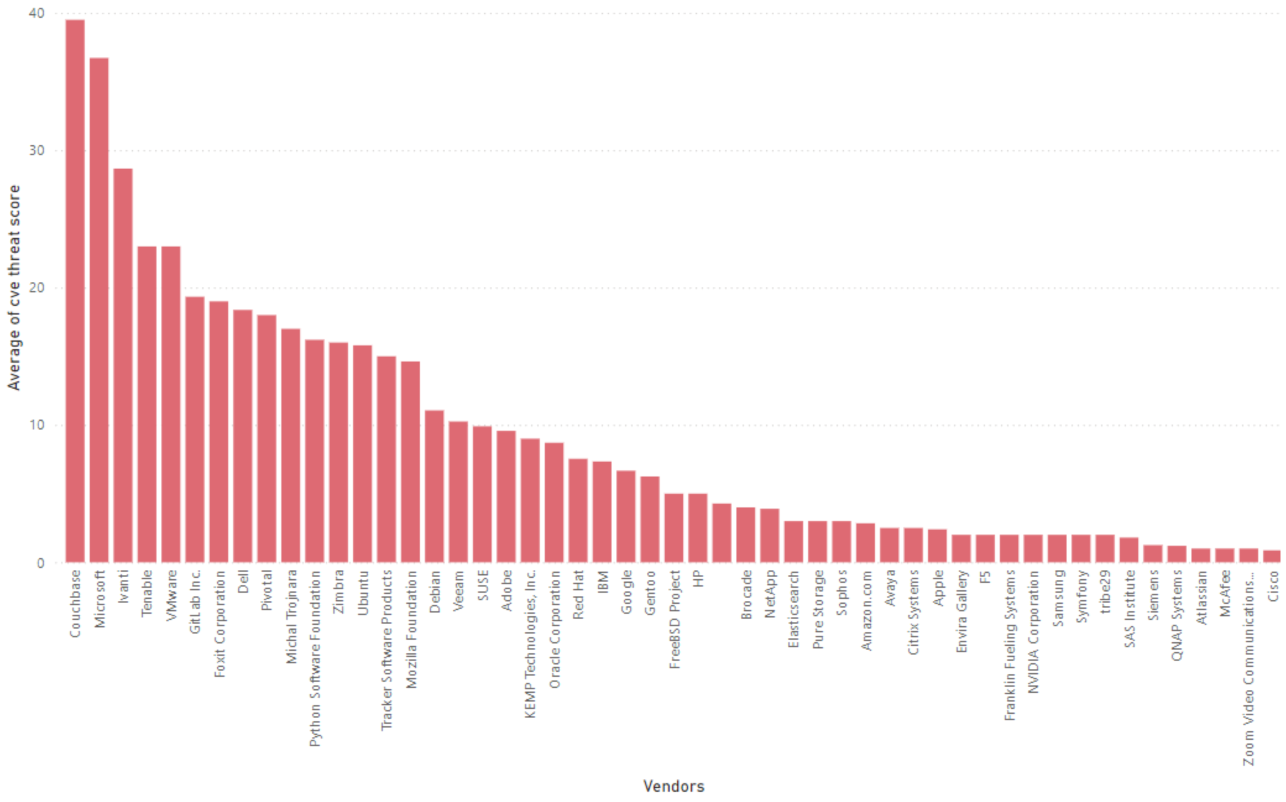


Top vendors with zero-day



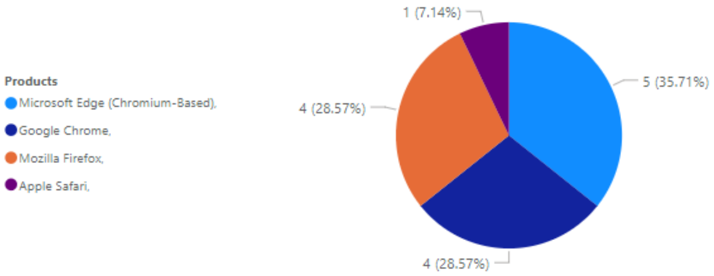
Advisories	Versions
SA131604	Ivanti Cloud Services Appliance 4.x,
SA131186	Microsoft Office 2019 / O365, Microsoft Office LTSC 2021, Microsoft Office LTSC 2021 Microsoft Office Online Server, Microsoft Publisher 2016 / O365,
SA131201	Microsoft Windows 10, Microsoft Windows Server 2016,
SA131198	Microsoft Windows 11,
SA131202	Microsoft Windows Server 2012,
SA131200	Microsoft Windows Server 2019,
SA131199	Microsoft Windows Server 2022,

Top Vendors with highest average threat score



Browser-related advisories

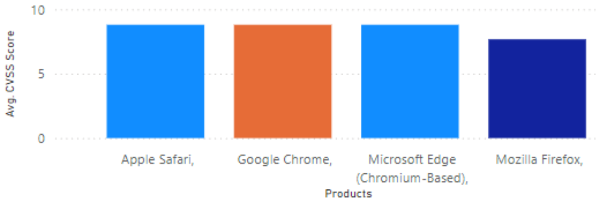
Advisories per browser



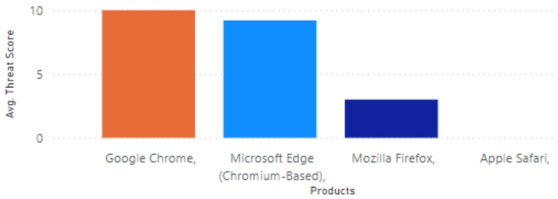
Browser zero-day vulnerabilities

No browser zero-day reported

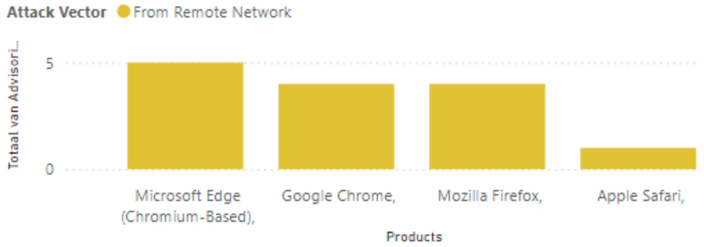
Average CVSS (criticality) score per browser



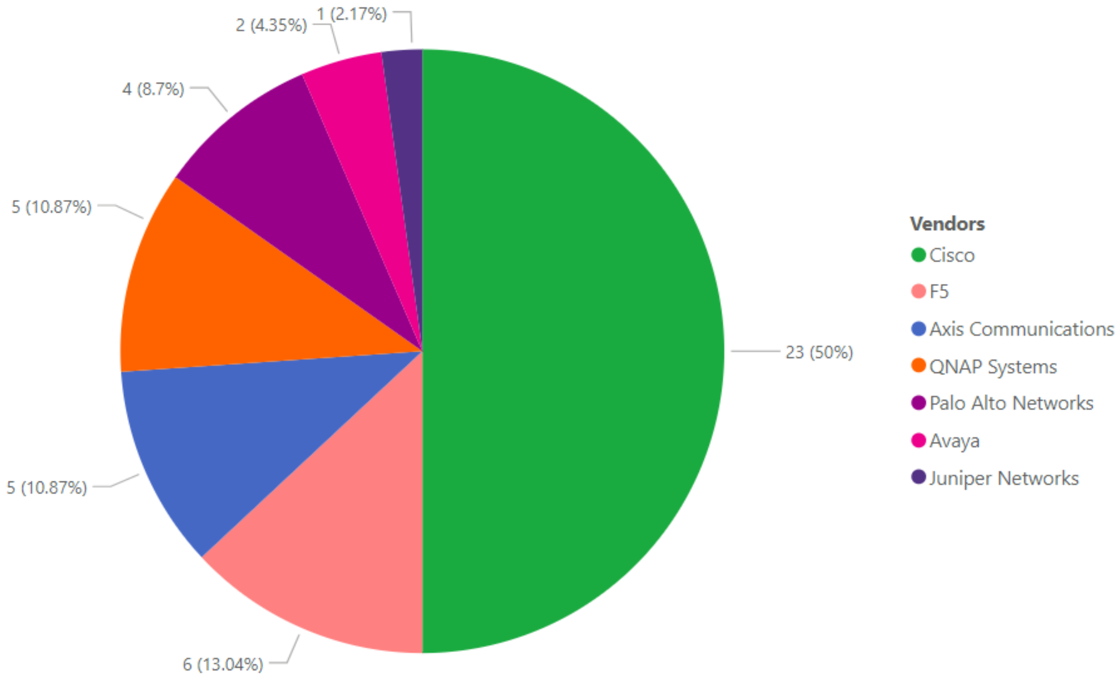
Average threat score per browser



What's the Attack Vector?



Networking related advisories

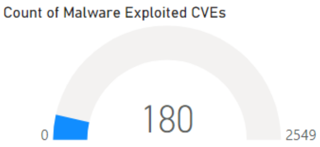


Threat intelligence

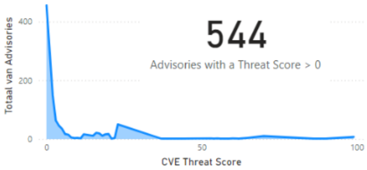
In a world where there are more than 25,000 new vulnerabilities every year, being smart about prioritizing remediation efforts is essential. Leveraging Threat Intelligence, another valuable layer of insight is provided to help you understand which of the vulnerabilities affecting your environment are 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+)	**544** ↓ (509)	54.40%
SAIDs with no threat score (=0)	**456** ↑ *(466)*	45.60%

SAID: Secunia Advisory Identifier

Range	# SAIDS	*Last month*
Low-range threat score SAIDs (1-12)	**356** ↑	***(303)***
Medium-range threat score SAIDs (13-23)	**150** ↓	***(152)***
Critical-range threat score SAIDs (45-70)	25 ↑	*(16)*
Very critical threat score SAIDs (71-99)	9 ↓	*(34)*
High-range threat score SAIDs (24-44)	4 =	*(4)*

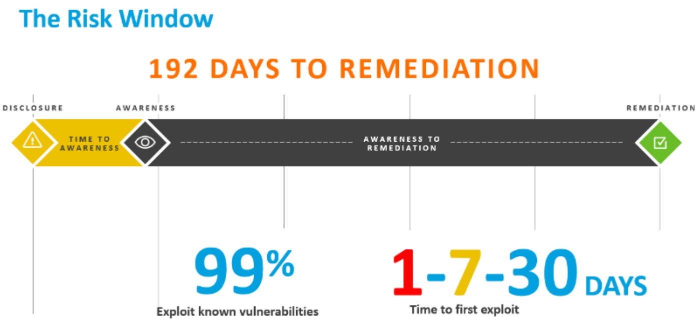
More information about how the Secunia team calculates the threat score:

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

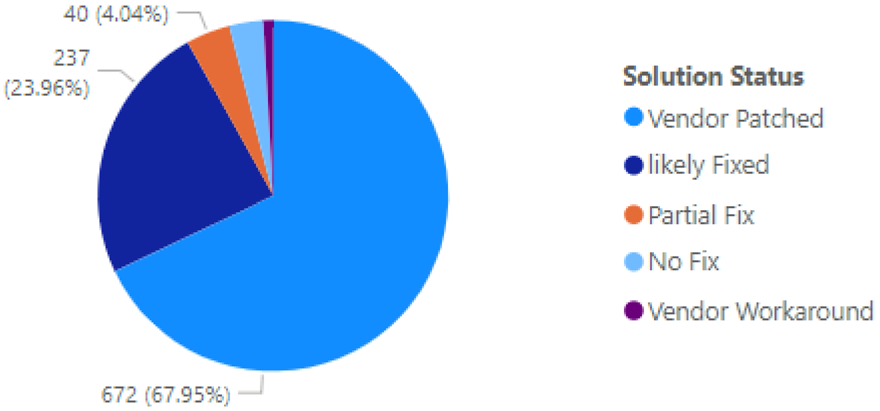
Patching

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

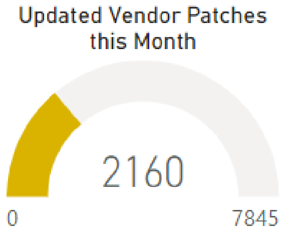


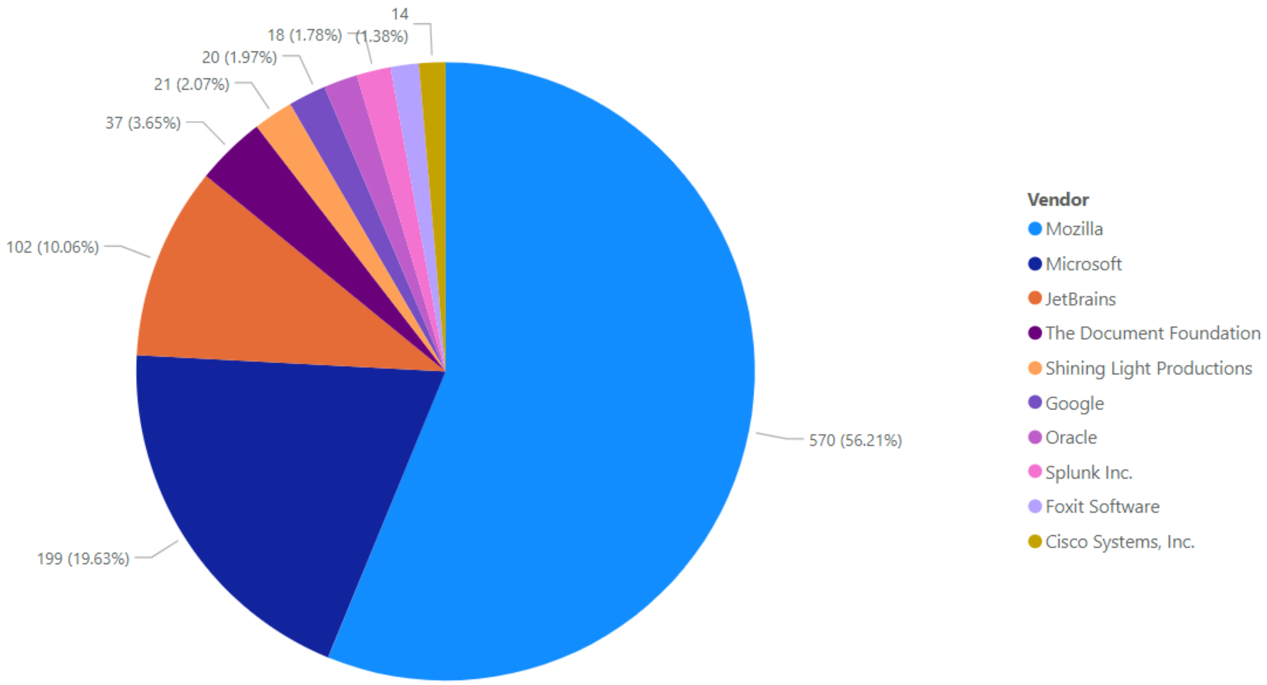
Flexera's Vendor Patch Module (VPM) statistics

Flexera has the largest third-party patch catalog **(7500+)** 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)



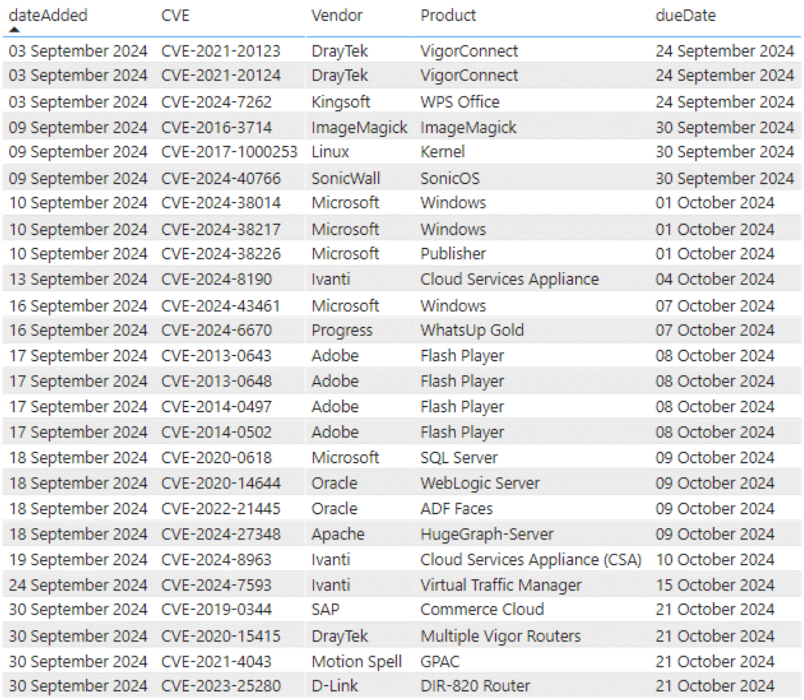


Other sources

CISA

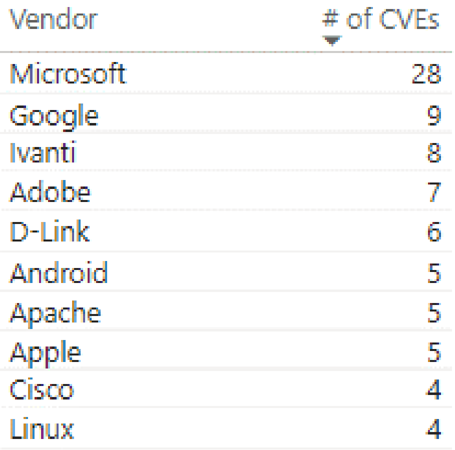
For the benefit of the cybersecurity community and network defenders—and to help every organization better manage vulnerabilities and keep pace with threat activity—CISA maintains the authoritative source of vulnerabilities that have been exploited in the wild: the Known Exploited Vulnerability (KEV) 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



dateAdded	CVE	Vendor	Product	dueDate
03 September 2024	CVE-2021-20123	DrayTek	VigorConnect	24 September 2024
03 September 2024	CVE-2021-20124	DrayTek	VigorConnect	24 September 2024
03 September 2024	CVE-2024-7262	Kingsoft	WPS Office	24 September 2024
09 September 2024	CVE-2016-3714	ImageMagick	ImageMagick	30 September 2024
09 September 2024	CVE-2017-1000253	Linux	Kernel	30 September 2024
09 September 2024	CVE-2024-40766	SonicWall	SonicOS	30 September 2024
10 September 2024	CVE-2024-38014	Microsoft	Windows	01 October 2024
10 September 2024	CVE-2024-38217	Microsoft	Windows	01 October 2024
10 September 2024	CVE-2024-38226	Microsoft	Publisher	01 October 2024
13 September 2024	CVE-2024-8190	Ivanti	Cloud Services Appliance	04 October 2024
16 September 2024	CVE-2024-43461	Microsoft	Windows	07 October 2024
16 September 2024	CVE-2024-6670	Progress	WhatsUp Gold	07 October 2024
17 September 2024	CVE-2013-0643	Adobe	Flash Player	08 October 2024
17 September 2024	CVE-2013-0648	Adobe	Flash Player	08 October 2024
17 September 2024	CVE-2014-0497	Adobe	Flash Player	08 October 2024
17 September 2024	CVE-2014-0502	Adobe	Flash Player	08 October 2024
18 September 2024	CVE-2020-0618	Microsoft	SQL Server	09 October 2024
18 September 2024	CVE-2020-14644	Oracle	WebLogic Server	09 October 2024
18 September 2024	CVE-2022-21445	Oracle	ADF Faces	09 October 2024
18 September 2024	CVE-2024-27348	Apache	HugeGraph-Server	09 October 2024
19 September 2024	CVE-2024-8963	Ivanti	Cloud Services Appliance (CSA)	10 October 2024
24 September 2024	CVE-2024-7593	Ivanti	Virtual Traffic Manager	15 October 2024
30 September 2024	CVE-2019-0344	SAP	Commerce Cloud	21 October 2024
30 September 2024	CVE-2020-15415	DrayTek	Multiple Vigor Routers	21 October 2024
30 September 2024	CVE-2021-4043	Motion Spell	GPAC	21 October 2024
30 September 2024	CVE-2023-25280	D-Link	DIR-820 Router	21 October 2024

Top 10 (YTD) KEV vendors

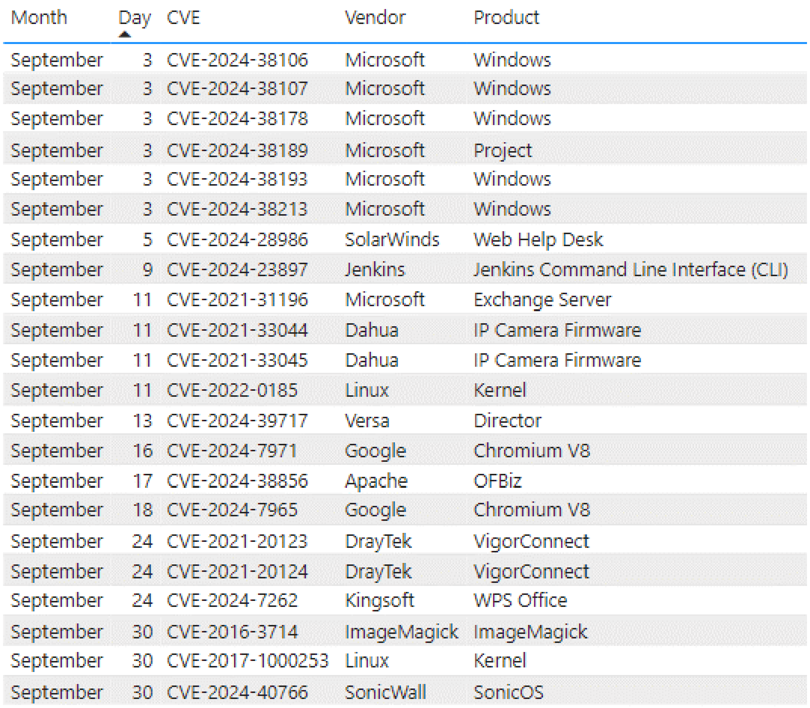


Vendor	# of CVEs
Microsoft	28
Google	9
Ivanti	8
Adobe	7
D-Link	6
Android	5
Apache	5
Apple	5
Cisco	4
Linux	4

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
September	3	CVE-2024-38106	Microsoft	Windows
September	3	CVE-2024-38107	Microsoft	Windows
September	3	CVE-2024-38178	Microsoft	Windows
September	3	CVE-2024-38189	Microsoft	Project
September	3	CVE-2024-38193	Microsoft	Windows
September	3	CVE-2024-38213	Microsoft	Windows
September	5	CVE-2024-28986	SolarWinds	Web Help Desk
September	9	CVE-2024-23897	Jenkins	Jenkins Command Line Interface (CLI)
September	11	CVE-2021-31196	Microsoft	Exchange Server
September	11	CVE-2021-33044	Dahua	IP Camera Firmware
September	11	CVE-2021-33045	Dahua	IP Camera Firmware
September	11	CVE-2022-0185	Linux	Kernel
September	13	CVE-2024-39717	Versa	Director
September	16	CVE-2024-7971	Google	Chromium V8
September	17	CVE-2024-38856	Apache	OFBiz
September	18	CVE-2024-7965	Google	Chromium V8
September	24	CVE-2021-20123	DrayTek	VigorConnect
September	24	CVE-2021-20124	DrayTek	VigorConnect
September	24	CVE-2024-7262	Kingsoft	WPS Office
September	30	CVE-2016-3714	ImageMagick	ImageMagick
September	30	CVE-2017-1000253	Linux	Kernel
September	30	CVE-2024-40766	SonicWall	SonicOS

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