MONTHLY VULNERABILITY INSIGHTS

Based on Data from Secunia Research

JANUARY 2024

flexera™

Author: Jeroen Braak

Contents

Introduction 3
Secunia Research software vulnerability tracking process 3
The anatomy of a Security Advisory 3
Summary 4
Year-to-date overview 5
Monthly data 6
Vulnerability information 6
Advisories by attack vector 6
Advisories by criticality 6
Advisories per day 7
Rejected advisories. 8
..... 8
Addressing awareness with vulnerability insights 9
Vendor view 10
Top vendors with the most advisories 10
Top vendors with zero-day 11
Top Vendors with highest average threat score 11
Browser-related advisories 12
Advisories per browser 12
Browser zero-day vulnerabilities 12
Average CVSS (criticality) score per browser 12
Average threat score per browser 12
What's the Attack Vector? 12
Networking related advisories 13
Threat intelligence 14
Count of malware-exploited CVEs 14
Count of advisories by CVE threat score 14
Threat intelligence advisory statistics: 14
Patching 15
Vulnerabilities that are vendor patched 15
Flexera's Vendor Patch Module (VPM) statistics 15
This month's top vendor patches 15
Other sources 16
CISA 16
This months' the additions to the KEV catalog 16
Due Date this month 17
More information 18

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

Secunia
Stay Secure

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: **899** ↑ (last month: **637**)

The new year started with a relative high number (third highest in past 12 months) of advisories.
Please check the annual vulnerability report for a 2023 view on vulnerabilities.

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

- Almost **58%** of all vulnerabilities reported in this month have a "**Remote Attack Vector**" (last month 53.38%)
- The Secunia Research Team reported **9** **Extremely** critical advisories this month. (Last month: **3**)
- **10 Zero-Day** Advisories reported. (last month :3) for mostly **Apple**, **Microsoft**, **Citrix** and **Ivanti**.
- Over **1,766 unique** CVE's (last month: **1,518**) were covered in the **899** Advisories.
- Threat Intelligence indicates again that **Moderately Critical Vulnerabilities** are targeted by hackers.
- This month **218** advisories contain at least one vulnerability linked to a **Recent Cyber Exploit**
- More than **half** of all advisories are disclosed by these 4 usual suspect vendors (**Red Hat, Oracle, Amazon** and **Ubuntu**)
- Interestingly among these vendors are also the ones with the most **rejected advisories**:
    - **Red Hat:** 28 out of 134 advisories were rejected by the Secunia Research Team.
    - **Amazon**: 26 out of 134
    - **SUSE:** 13 out of 134
    - **Oracle:** 10 out of 134
- **Juniper Networks** contributed to half of all Networking related Advisories this month.

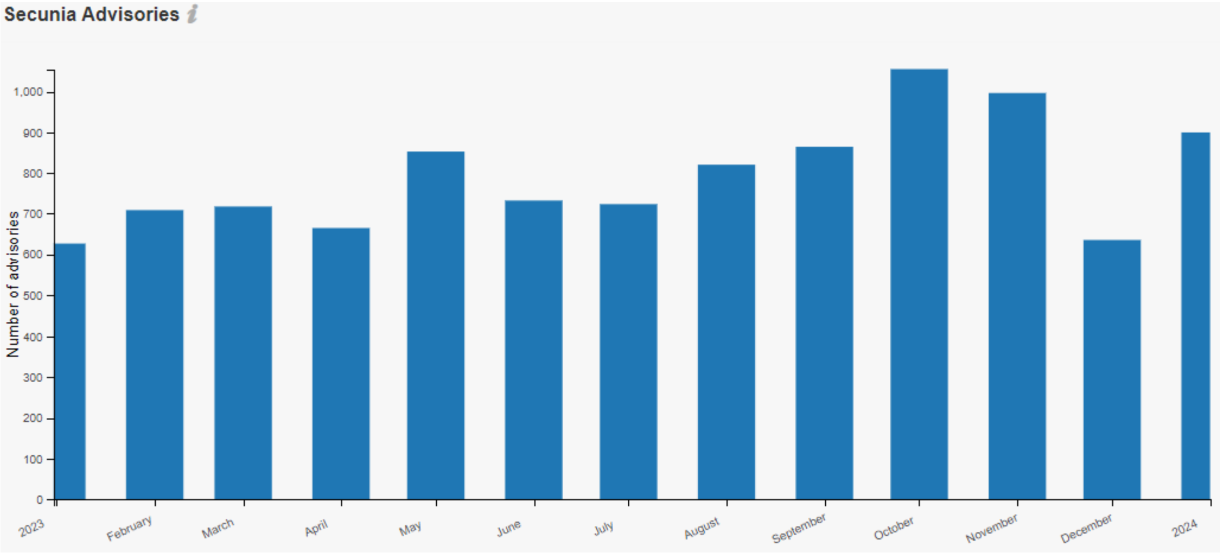
Last month we reported that 73.94% of all Secunia Advisories had a **Threat** (exploits, malware, ransomware, etc.) associated with them, **this month** the number has been **a little higher** to **74.86%**

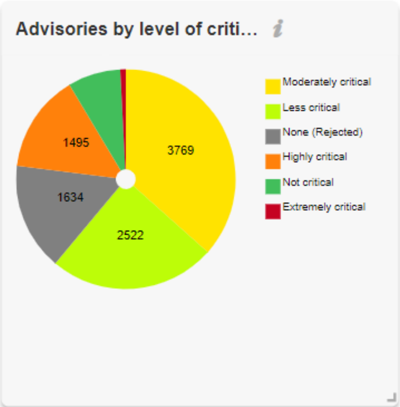
Using Threat Intelligence is going to help you with prioritizing what needs to be **patched** immediately.

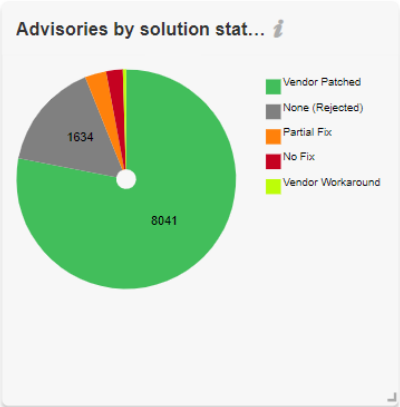
Software Vulnerability – and Patch Management is becoming more and more important.
Due to the ongoing global threats, attacks on critical infrastructures in many countries are increasing.
Back in 2019 (just before Covid) patching was recommended within 30 days (or 14 days for CVSS score 7 or higher)
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)

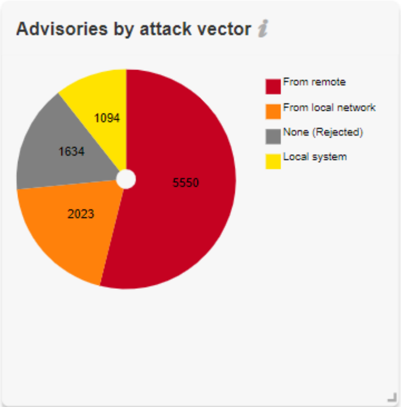
Year-to-date overview

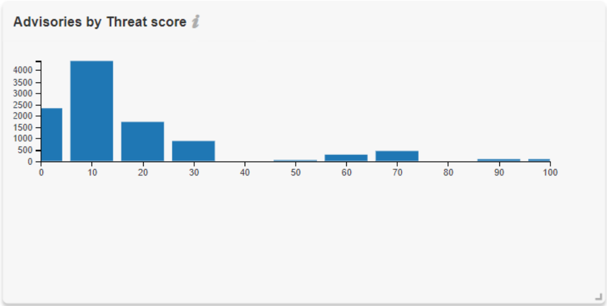
As of **January 31, 2024**, the year-to-date total is at **899** Advisories ↑ which is higher than 2023: **626** YTD Advisories)

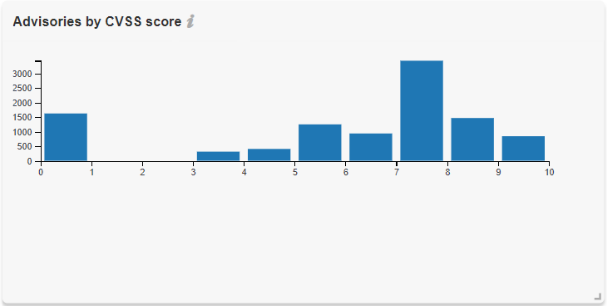












Monthly data

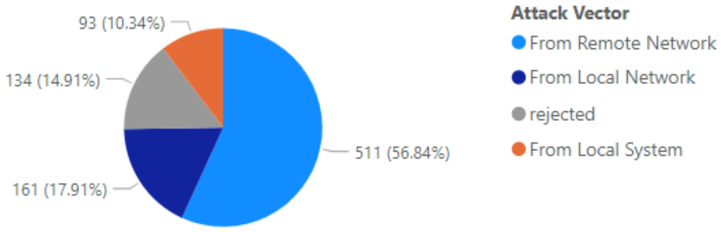
This month, a total of **899** ↓ (last month: **637**) advisories were reported by the Secunia Research Team.

This month:	**#**	**Change** *(last month):*
Total # of advisories	**899**	↑ *(637)*
Unique Vendors	**85**	↑ *(84)*
Unique Products	**318**	↑ **(271)**
Unique Versions	**413**	↑ *(329)*
Rejected Advisories *	**113**	↑ *(94)*
Total Unique CVE ID's reported	**1,766**	↑ **(1,518)**
		↑ increased ↓lower ↔ same

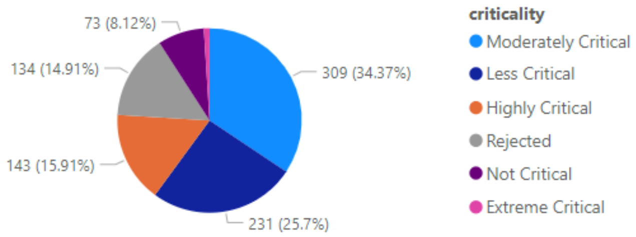
** **113** advisories have received the "rejected" status which means in general that leveraging it would require one or more violations of security best practices (e.g., product not securely configured or not used securely) or that it was "too weak of a gain" (e.g., administrative, local users already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

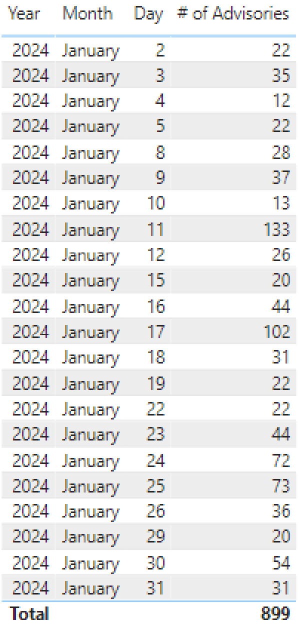


Advisories by criticality

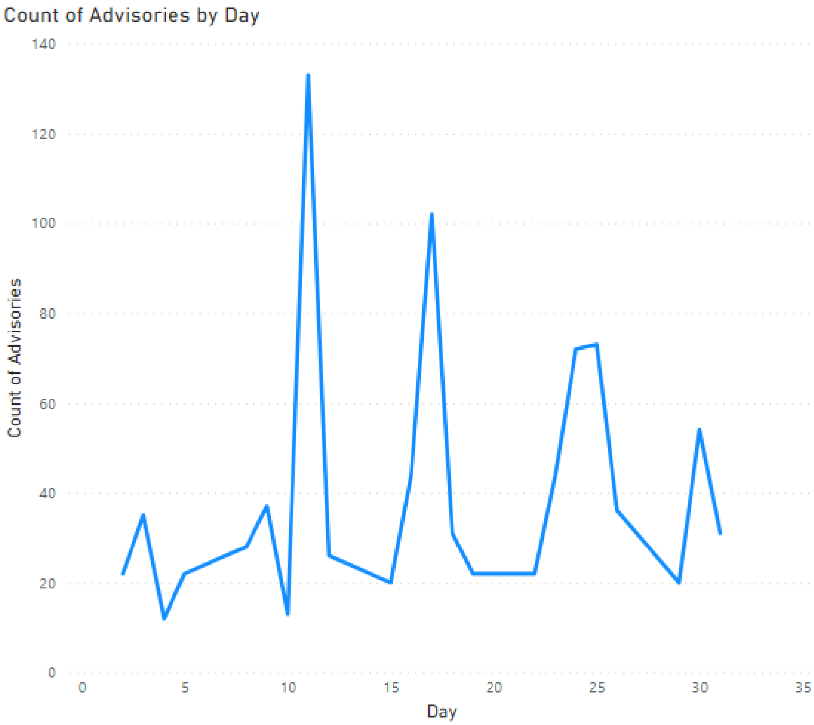


Advisories per day

Below an overview of the daily advisory count.

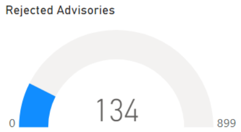


Year	Month	Day	# of Advisories
2024	January	2	22
2024	January	3	35
2024	January	4	12
2024	January	5	22
2024	January	8	28
2024	January	9	37
2024	January	10	13
2024	January	11	133
2024	January	12	26
2024	January	15	20
2024	January	16	44
2024	January	17	102
2024	January	18	31
2024	January	19	22
2024	January	22	22
2024	January	23	44
2024	January	24	72
2024	January	25	73
2024	January	26	36
2024	January	29	20
2024	January	30	54
2024	January	31	31
Total			**899**



Rejected advisories.

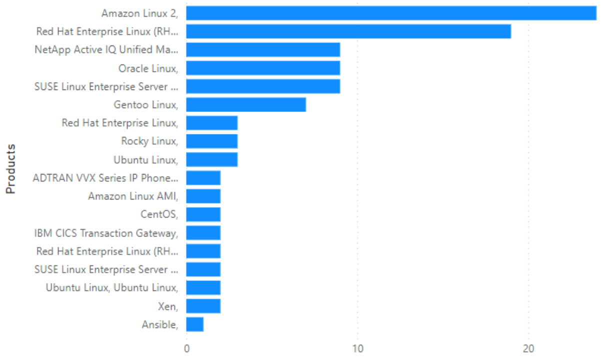
There are many vulnerabilities posted to the National Vulnerability Database (NVD) by a lot of people and companies. They are not always valid, assigned a proper criticality, and in some cases, a vulnerability may be legitimate but not afford the attacker any benefit.

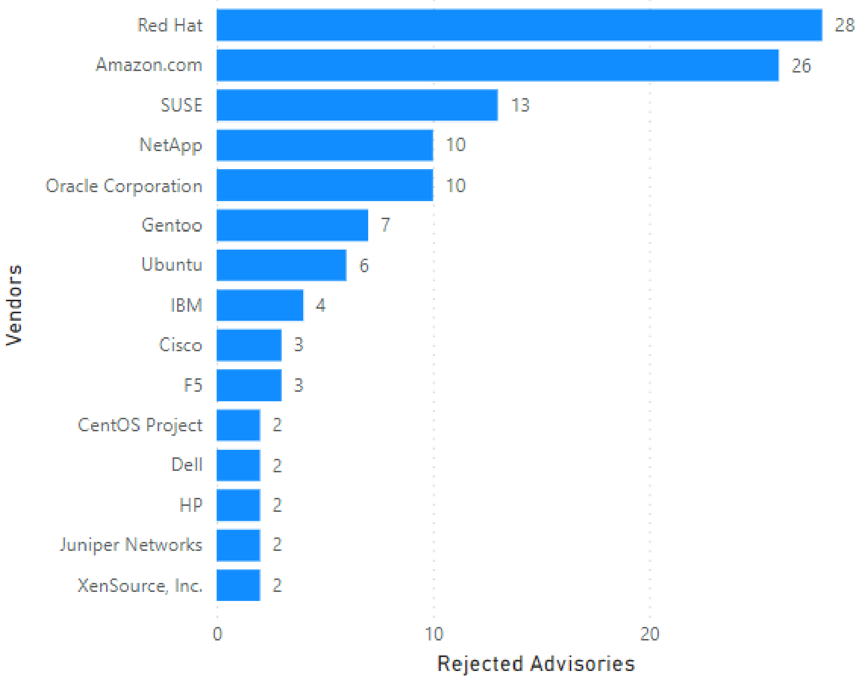


The Secunia Research team at Flexera evaluates vulnerabilities from hundreds of sources, rescores them when necessary and even rejects vulnerabilities not worth your attention. Rejection Advisories help you to reduce the volume of vulnerabilities to be mitigated by helping you focus only on those that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

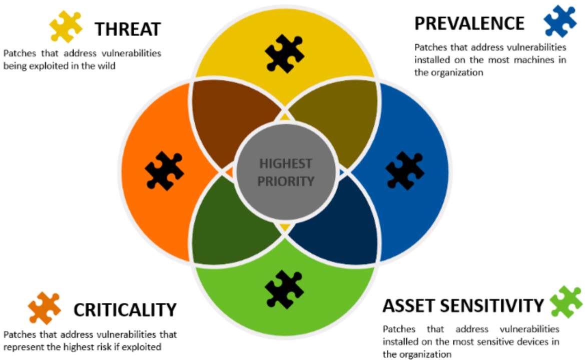
- What systems would result in the most risk if compromised?
- Is it a high-risk device? **Patch**.

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**.

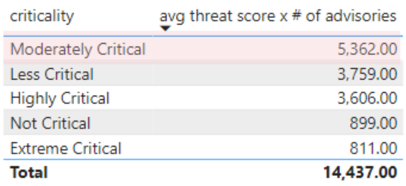
Threat Intelligence:

- 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.



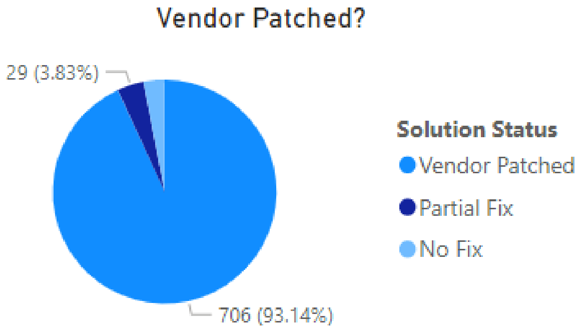
criticality	avg threat score x # of advisories
Moderately Critical	5,362.00
Less Critical	3,759.00
Highly Critical	3,606.00
Not Critical	899.00
Extreme Critical	811.00
Total	**14,437.00**

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.

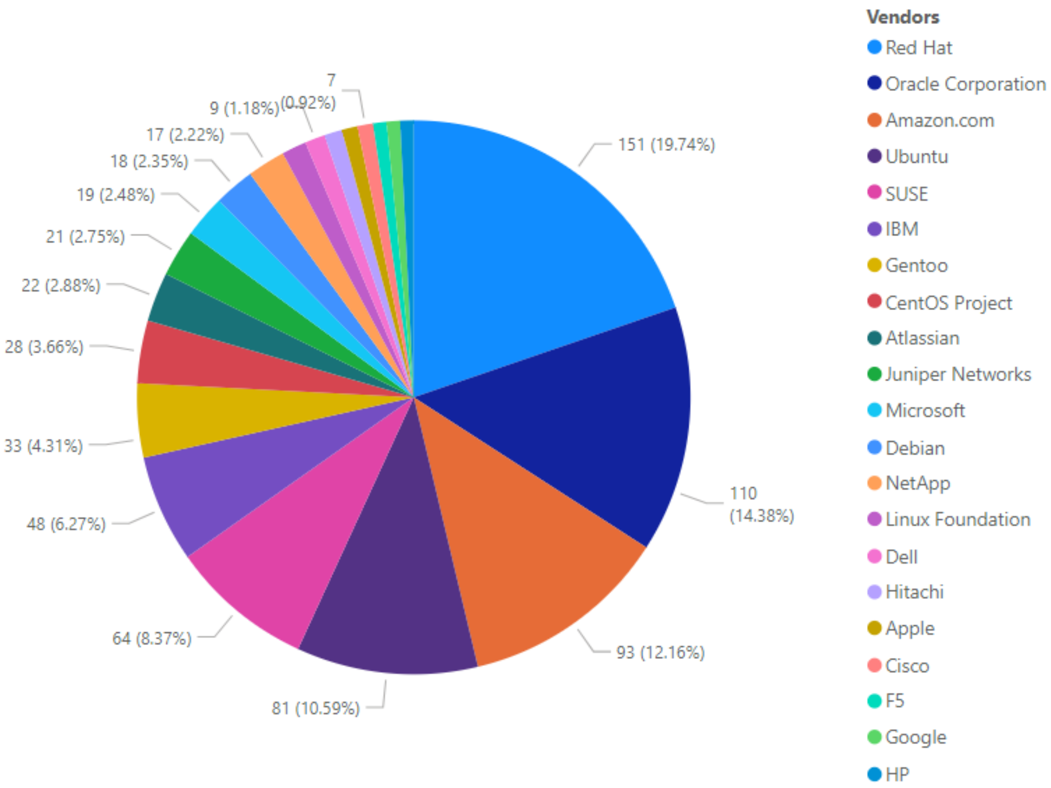
Take away 2:

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)

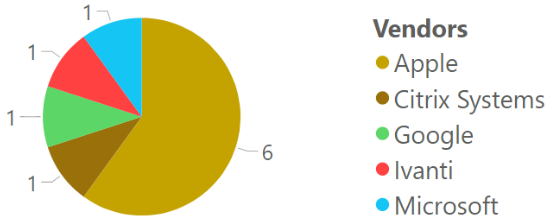


Vendor view

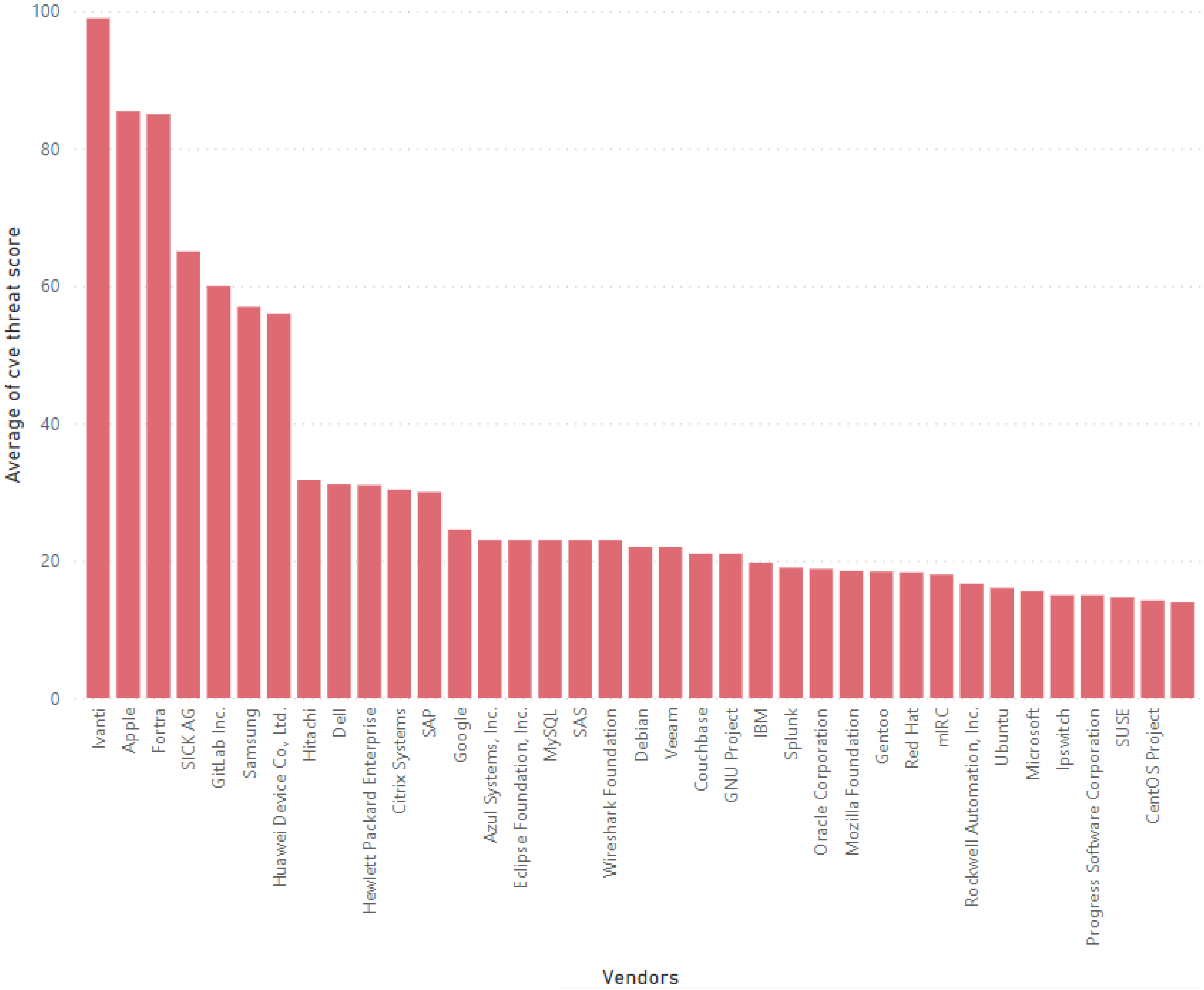
Top vendors with the most advisories



Top vendors with zero-day

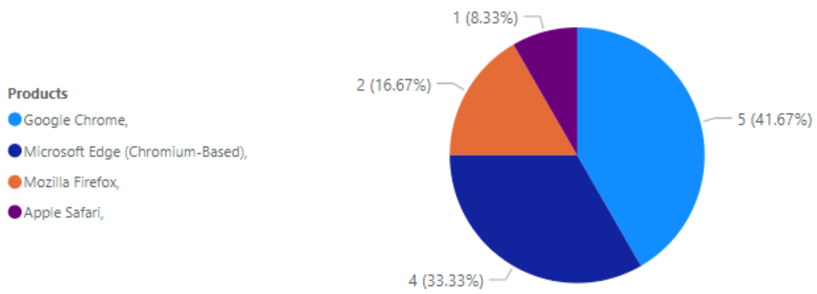


Top Vendors with highest average threat score

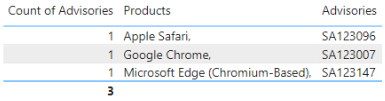


Browser-related advisories

Advisories per browser

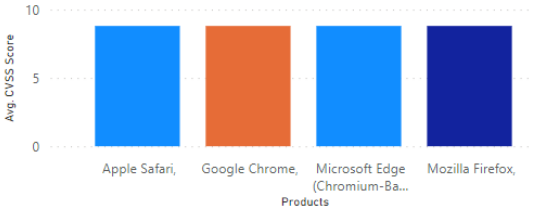


Browser zero-day vulnerabilities

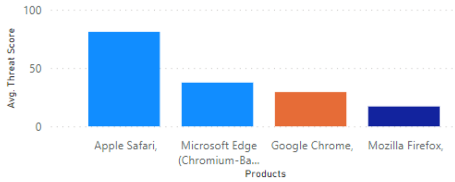


Count of Advisories	Products	Advisories
1	Apple Safari,	SA123096
1	Google Chrome,	SA123007
1	Microsoft Edge (Chromium-Based),	SA123147
3		

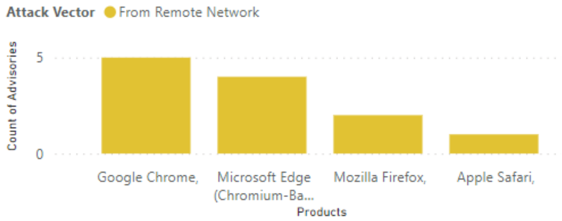
Average CVSS (criticality) score per browser



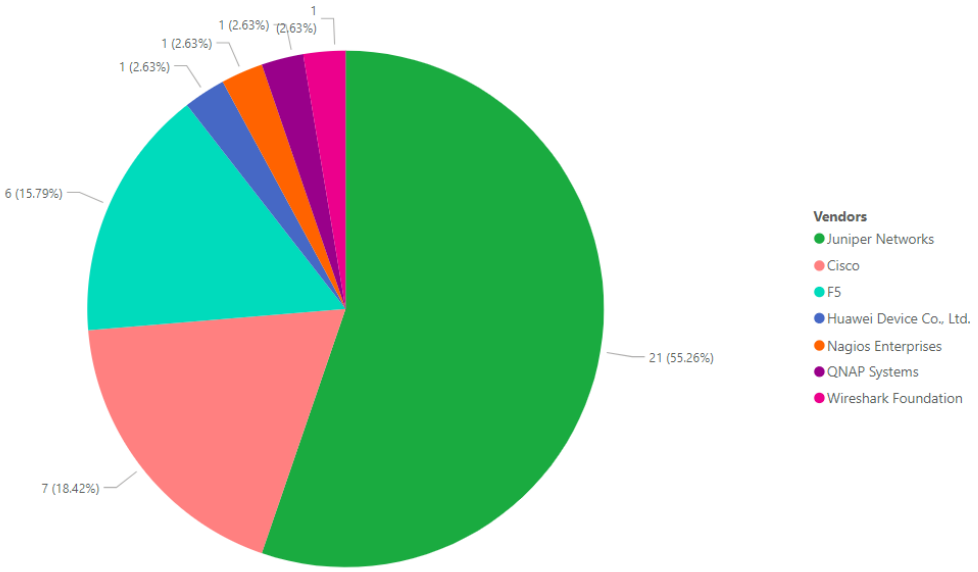
Average threat score per browser



What's the Attack Vector?



Networking related advisories

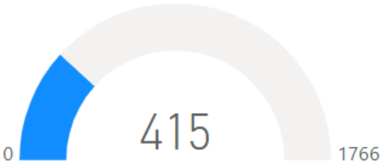


Threat intelligence

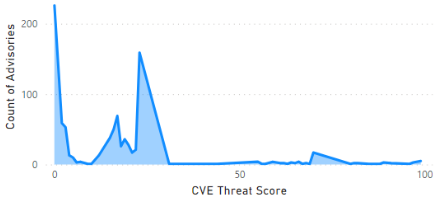
In a world where there are more than 18,000 new vulnerabilities every year, being smart about prioritizing remediation efforts is essential. Leveraging Threat Intelligence, another valuable layer of insight is provided to help you understand which of the vulnerabilities affecting your environment are 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+)	**673**↑*(471)*	74.86%
SAIDs with no threat score (=0)	**226**↑*(166)*	52.14%

SAID: Secunia Advisory Identifier

Range	# SAIDS		*Last month*
Medium-range threat score SAIDs (13-23)	**444**	↑	***(208)***
Low-range threat score SAIDs (1-12)	**157**	↑	***(212)***
Critical-range threat score SAIDs (45-70)	45	↑	*(35)*
Very critical threat score SAIDs (71-99)	22	↑	*(14)*
High-range threat score SAIDs (24-44)	5	↑	*(2)*

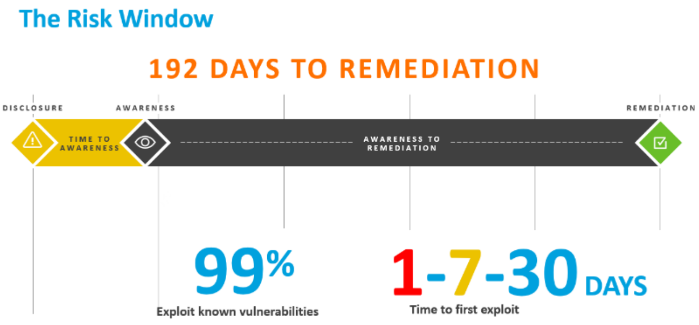
More information about how the Secunia team calculates the threat score:

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

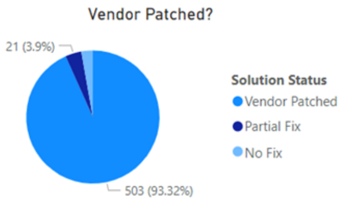
Patching

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

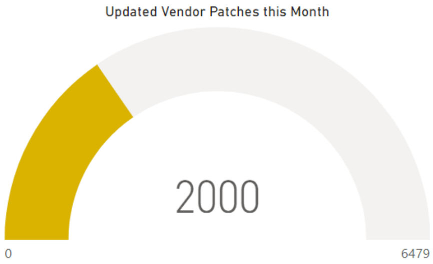


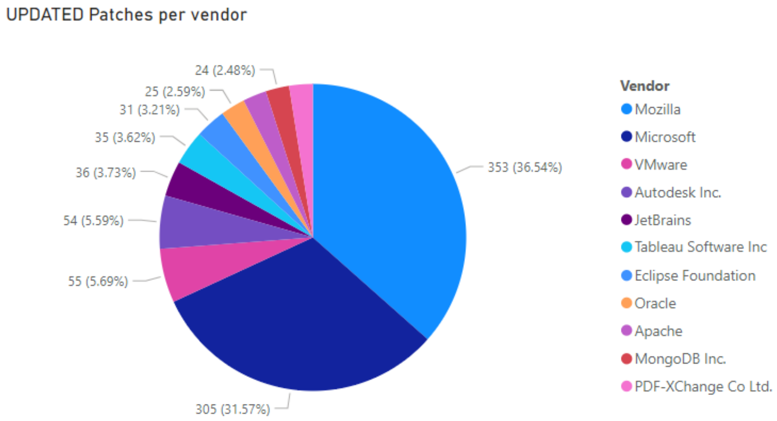
Flexera's Vendor Patch Module (VPM) statistics

Flexera has the largest third-party patch catalog **(More than 6,400)** 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)





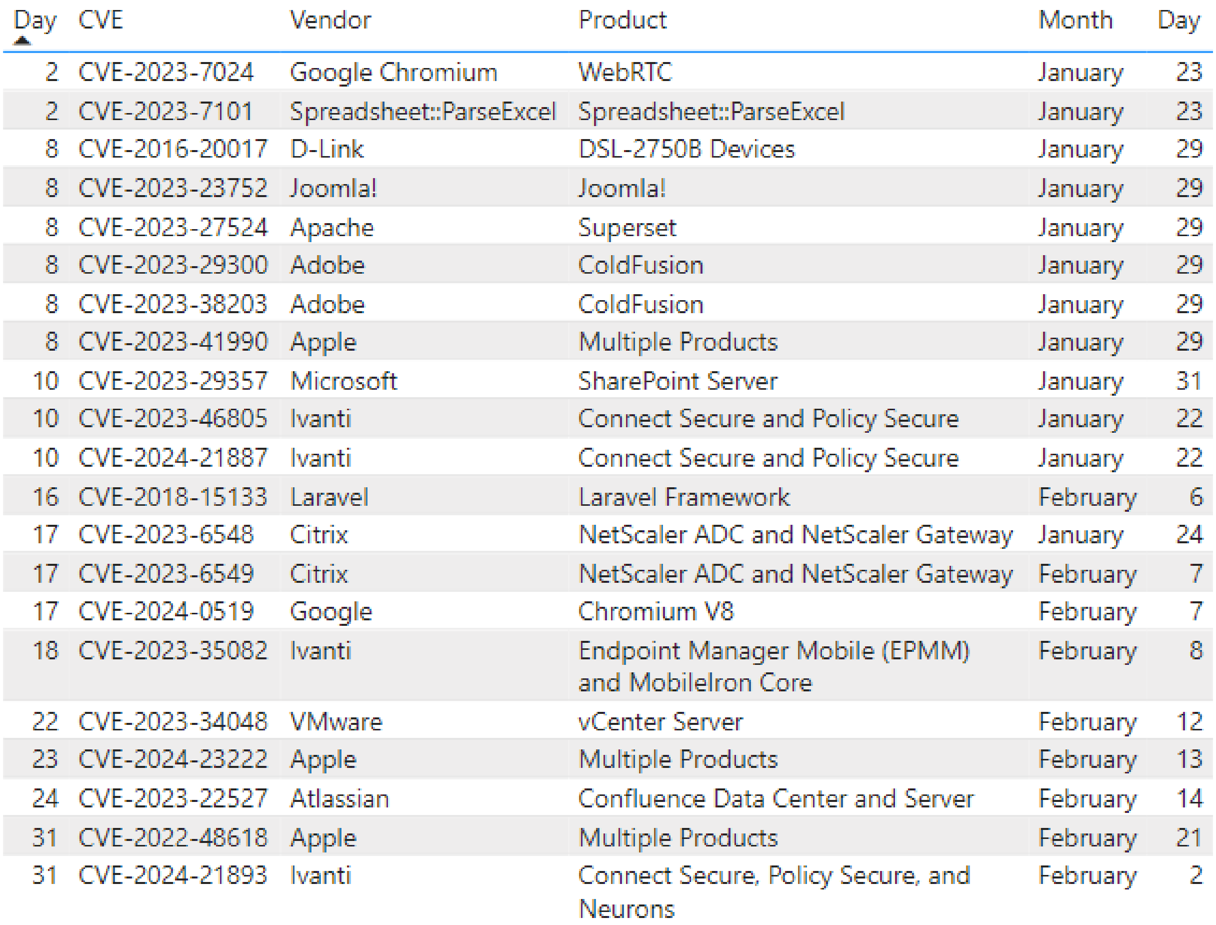
Other sources

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.

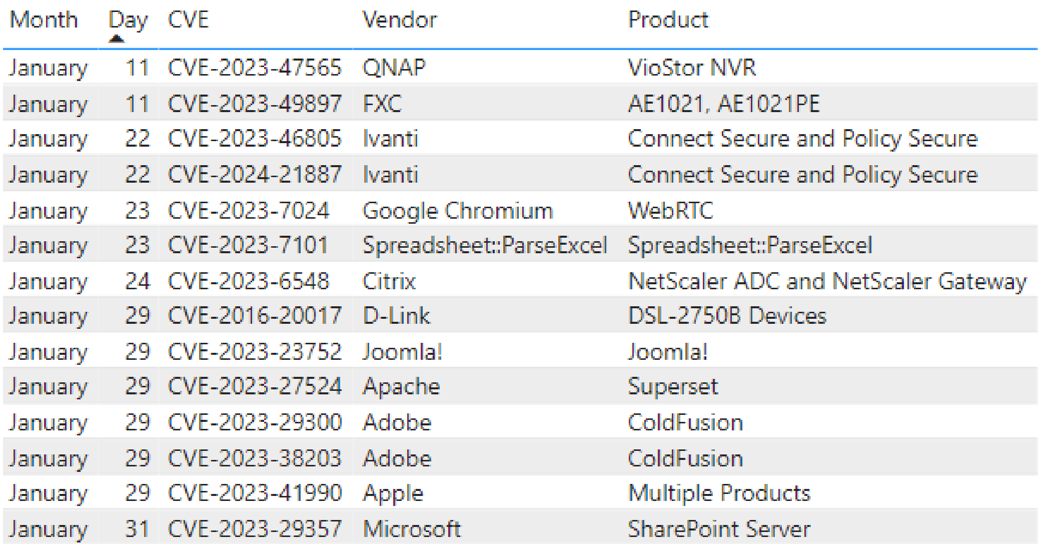


Day ▲	CVE	Vendor	Product	Month	Day
2	CVE-2023-7024	Google Chromium	WebRTC	January	23
2	CVE-2023-7101	Spreadsheet::ParseExcel	Spreadsheet::ParseExcel	January	23
8	CVE-2016-20017	D-Link	DSL-2750B Devices	January	29
8	CVE-2023-23752	Joomla!	Joomla!	January	29
8	CVE-2023-27524	Apache	Superset	January	29
8	CVE-2023-29300	Adobe	ColdFusion	January	29
8	CVE-2023-38203	Adobe	ColdFusion	January	29
8	CVE-2023-41990	Apple	Multiple Products	January	29
10	CVE-2023-29357	Microsoft	SharePoint Server	January	31
10	CVE-2023-46805	Ivanti	Connect Secure and Policy Secure	January	22
10	CVE-2024-21887	Ivanti	Connect Secure and Policy Secure	January	22
16	CVE-2018-15133	Laravel	Laravel Framework	February	6
17	CVE-2023-6548	Citrix	NetScaler ADC and NetScaler Gateway	January	24
17	CVE-2023-6549	Citrix	NetScaler ADC and NetScaler Gateway	February	7
17	CVE-2024-0519	Google	Chromium V8	February	7
18	CVE-2023-35082	Ivanti	Endpoint Manager Mobile (EPMM) and MobileIron Core	February	8
22	CVE-2023-34048	VMware	vCenter Server	February	12
23	CVE-2024-23222	Apple	Multiple Products	February	13
24	CVE-2023-22527	Atlassian	Confluence Data Center and Server	February	14
31	CVE-2022-48618	Apple	Multiple Products	February	21
31	CVE-2024-21893	Ivanti	Connect Secure, Policy Secure, and Neurons	February	2

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
January	11	CVE-2023-47565	QNAP	VioStor NVR
January	11	CVE-2023-49897	FXC	AE1021, AE1021PE
January	22	CVE-2023-46805	Ivanti	Connect Secure and Policy Secure
January	22	CVE-2024-21887	Ivanti	Connect Secure and Policy Secure
January	23	CVE-2023-7024	Google Chromium	WebRTC
January	23	CVE-2023-7101	Spreadsheet::ParseExcel	Spreadsheet::ParseExcel
January	24	CVE-2023-6548	Citrix	NetScaler ADC and NetScaler Gateway
January	29	CVE-2016-20017	D-Link	DSL-2750B Devices
January	29	CVE-2023-23752	Joomla!	Joomla!
January	29	CVE-2023-27524	Apache	Superset
January	29	CVE-2023-29300	Adobe	ColdFusion
January	29	CVE-2023-38203	Adobe	ColdFusion
January	29	CVE-2023-41990	Apple	Multiple Products
January	31	CVE-2023-29357	Microsoft	SharePoint Server

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