flexera™

# MONTHLY VULNERABILITY INSIGHTS

*Based on Data from Secunia Research*

# NOVEMBER 2025

Author: Jeroen Braak

# Reuse

## 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

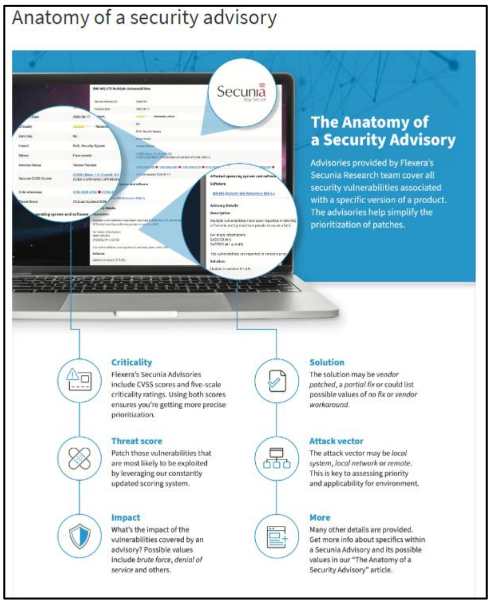
A security advisory is a summary of the work that Secunia Research performs to communicate standardized, validated and enriched vulnerability research on a specific software product version.

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.

**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.

# Monthly Summary

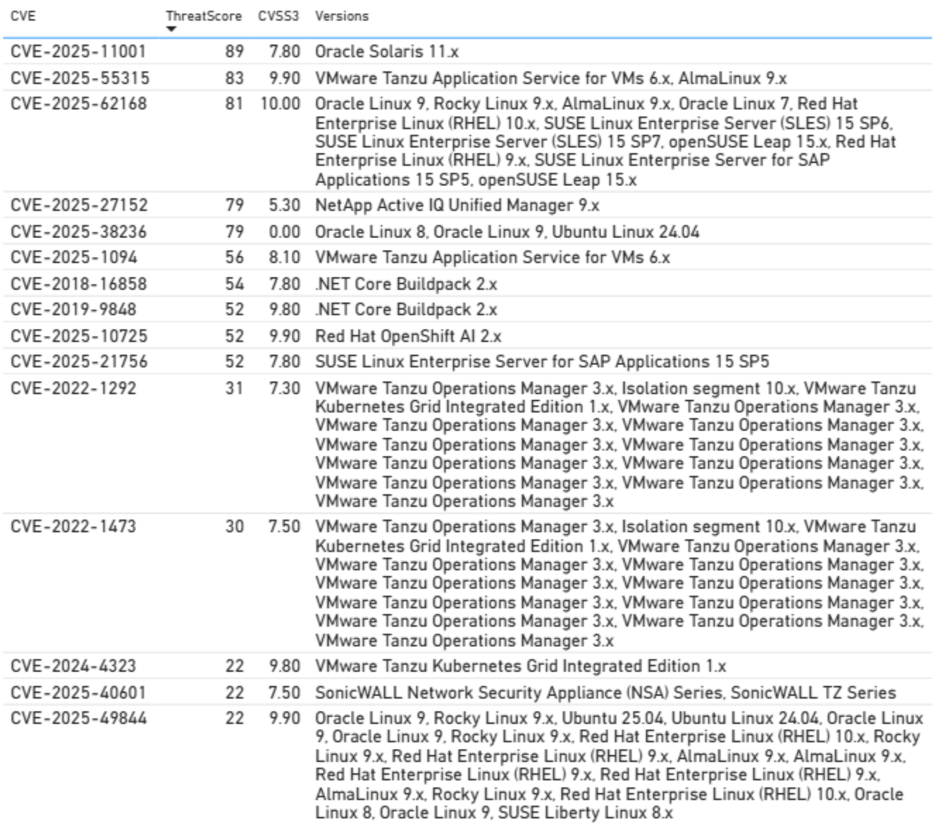
Total advisories: **1,289 (**last month: **1,526**)

## Important conclusions from this month's report are:

- This month 1,289 Advisories (**Ranked #6** ,since 2002) .
- Flexera has increased the Vendor Patch Catalog again this month to **12,354 patches** ( last month: 12,176 patches)
- Year to Date 2025 is now also record breaking with **13,562** advisories ( 2024: 11,437) which is an 18.6% increase.
- Secunia reported **36** (last month : 20) Advisories without CVE that have a CVSS range 0.0 – 7.8, the top 6 :

| Advisories | Versions | Consequence | Secunia Criticality | Secunia CVSS3 | Attack Vector |
|---|---|---|---|---|---|
| SA148095 | Debian 12.x, Debian 13.x | Security Bypass | Highly Critical | 9.8 | From Remote Network |
| SA147332 | Ubuntu 25.04, Ubuntu Linux 24.04 | Security Bypass | Highly Critical | 9.8 | From Remote Network |
| SA147174 | Confluent Platform 7.x | Security Bypass | Less Critical | 8 | From Local Network |
| SA147476 | WibuKey Runtime for Windows 6.x | Privilege escalation | Less Critical | 7.8 | From Local System |
| SA147538 | Libxml2 | DoS | Moderately Critical | 7.5 | From Remote Network |
| SA147410 | libarchive 3.x | Exposure of sensitive information | Moderately Critical | 7.5 | From Remote Network |

- **6 Zero-day** Advisories reported for Microsoft Windows and Server, Edge and Google Chrome (last month : 8 zero-day Advisories)
- With **188 rejection advisories** (last month 250) , we see that **Linux Foundation** continues to be the top provider of rejection advisories (41) , **Suse** (40) , **RedHat** and **Oracle** (14)
- 73 Advisories disclosed for **Rocky Linux** on the Open-Source list (#4 position on the vendor list)
- Notable is the spike on October 11 , when 192 Advisories were released with more than 71% was related to **SUSE** (33.33%) , **Amazon.com** (26,56%) and **Red Hat** (11.46%)
- **Secunia Research** identified several **KEV**'s that have not been added to the **CISA KEV**: (as of Dec. 2. 2025 )



| CVE | ThreatScore | CVSS3 | Versions |
|---|---|---|---|
| CVE-2025-11001 | 89 | 7.80 | Oracle Solaris 11.x |
| CVE-2025-55315 | 83 | 9.90 | VMware Tanzu Application Service for VMs 6.x, AlmaLinux 9.x |
| CVE-2025-62168 | 81 | 10.00 | Oracle Linux 9, Rocky Linux 9.x, AlmaLinux 9.x, Oracle Linux 7, Red Hat Enterprise Linux (RHEL) 10.x, SUSE Linux Enterprise Server (SLES) 15 SP6, SUSE Linux Enterprise Server (SLES) 15 SP7, openSUSE Leap 15.x, Red Hat Enterprise Linux (RHEL) 9.x, SUSE Linux Enterprise Server for SAP Applications 15 SP5, openSUSE Leap 15.x |
| CVE-2025-27152 | 79 | 5.30 | NetApp Active IQ Unified Manager 9.x |
| CVE-2025-38236 | 79 | 0.00 | Oracle Linux 8, Oracle Linux 9, Ubuntu Linux 24.04 |
| CVE-2025-1094 | 56 | 8.10 | VMware Tanzu Application Service for VMs 6.x |
| CVE-2018-16858 | 54 | 7.80 | .NET Core Buildpack 2.x |
| CVE-2019-9848 | 52 | 9.80 | .NET Core Buildpack 2.x |
| CVE-2025-10725 | 52 | 9.90 | Red Hat OpenShift AI 2.x |
| CVE-2025-21756 | 52 | 7.80 | SUSE Linux Enterprise Server for SAP Applications 15 SP5 |
| CVE-2022-1292 | 31 | 7.30 | VMware Tanzu Operations Manager 3.x, Isolation segment 10.x, VMware Tanzu Kubernetes Grid Integrated Edition 1.x, VMware Tanzu Operations Manager 3.x, VMware Tanzu Operations Manager 3.x, VMware Tanzu Operations Manager 3.x, VMware Tanzu Operations Manager 3.x, VMware Tanzu Operations Manager 3.x, VMware Tanzu Operations Manager 3.x, VMware Tanzu Operations Manager 3.x, VMware Tanzu Operations Manager 3.x, VMware Tanzu Operations Manager 3.x, VMware Tanzu Operations Manager 3.x |
| CVE-2022-1473 | 30 | 7.50 | VMware Tanzu Operations Manager 3.x, Isolation segment 10.x, VMware Tanzu Kubernetes Grid Integrated Edition 1.x, VMware Tanzu Operations Manager 3.x, VMware Tanzu Operations Manager 3.x, VMware Tanzu Operations Manager 3.x, VMware Tanzu Operations Manager 3.x, VMware Tanzu Operations Manager 3.x, VMware Tanzu Operations Manager 3.x, VMware Tanzu Operations Manager 3.x, VMware Tanzu Operations Manager 3.x, VMware Tanzu Operations Manager 3.x, VMware Tanzu Operations Manager 3.x |
| CVE-2024-4323 | 22 | 9.80 | VMware Tanzu Kubernetes Grid Integrated Edition 1.x |
| CVE-2025-40601 | 22 | 7.50 | SonicWALL Network Security Appliance (NSA) Series, SonicWALL TZ Series |
| CVE-2025-49844 | 22 | 9.90 | Oracle Linux 9, Rocky Linux 9.x, Ubuntu 25.04, Ubuntu Linux 24.04, Oracle Linux 9, Oracle Linux 9, Rocky Linux 9.x, Red Hat Enterprise Linux (RHEL) 10.x, Rocky Linux 9.x, Red Hat Enterprise Linux (RHEL) 9.x, AlmaLinux 9.x, AlmaLinux 9.x, Red Hat Enterprise Linux (RHEL) 9.x, Red Hat Enterprise Linux (RHEL) 9.x, AlmaLinux 9.x, Rocky Linux 9.x, Red Hat Enterprise Linux (RHEL) 10.x, Oracle Linux 8, Oracle Linux 9, SUSE Liberty Linux 8.x |

# Notable Vulnerability – and Threat Intelligence news:

November 2025 told a different story beneath the surface. From surging vulnerability disclosures to state-level breaches and ransomware attacks, the month revealed a cybersecurity landscape marked by speed, stealth, and severity. From an Advisory view:

- **SA147563 & SA147563| Microsoft Edge & Google Chrome |**
  **Zero Day: Yes |Extreme Critical | CVSS: 8.8 | Threat Score: 96**
  Type Confusion in V8 in Google Chrome prior to 142.0.7444.175 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)

  These threats have been associated with the following exploits:
  - zero day
  - Tsundere (Botnet)
  - Clop Ransomware (Ransomware)
  - BadIIS
  - EVEREST Ransomware (Ransomware)

  **CVE-2025-13223** ●Actively being exploited!

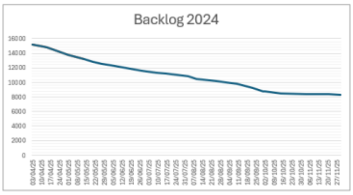
- **SA147828 + SA147824 + SA147825 + SA147632 | Windows 10+11, Windows Server '19+'22+'25**
  **Zero Day: Yes | Highly Critical |CVSS:9.8| Threat Score:99**
  **Multiple** vulnerabilities have been reported with Windows Server and Windows Client ,
  which can be exploited by malicious, local users to disclose sensitive information, cause a DoS (Denial of Service), and gain escalated privileges, by malicious users in a guest virtual machine to cause a DoS, by malicious users to compromise a vulnerable system, and by malicious people to bypass certain security restrictions and compromise a vulnerable system.
  **CVE-2025-62215 having the highest threat score (88) and added to the KEV.** ●Actively being exploited!

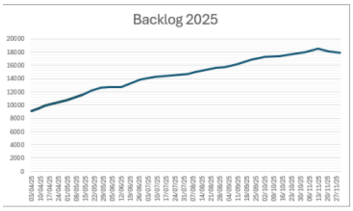
  Secunia: *Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Kernel allows an authorized attacker to elevate privileges locally.*

  KEV: *Microsoft Windows Kernel contains a race condition vulnerability that allows a local attacker with low-level privileges to escalate privileges. Successful exploitation of this vulnerability could enable the attacker to gain SYSTEM-level access.*

  These threats have been associated with the following exploits:
  - Clop Ransomware (Ransomware)
  - RondoDox (Botnet)
  - zero day
  - Akira Ransomware (Ransomware)
  - Race COndition

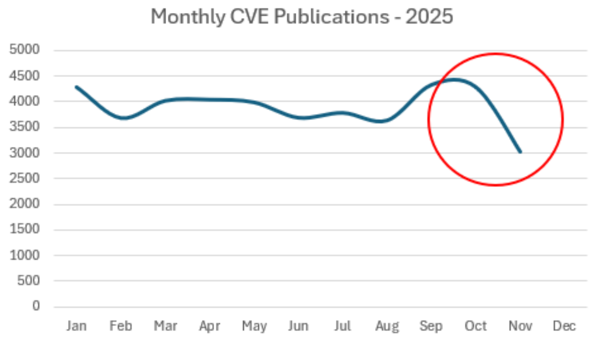
# NVD Update





After nearly two years of unrelenting growth, the Common Vulnerabilities and Exposures (CVE) backlog has finally shown a modest but noteworthy decline. This downward trend, while not dramatic, suggests a potential turning point in how disclosed software vulnerabilities are managed. However, this development calls for closer examination, especially regarding its causes and implications for organizations depending on accurate and timely vulnerability intelligence.

The improvement is not primarily due to an increase in analysis from the National Vulnerability Database (NVD). Instead, it appears to be the result of a significant reduction in new CVEs published by CVE.org and subsequently ingested by NVD. This distinction is important. The dip in numbers may reflect a slowdown in reporting or publishing activity rather than a fundamental solution to the underlying backlog.



Currently, more than 26,000 CVEs remain unanalyzed by the NVD. This leaves a substantial gap in vulnerability coverage and puts organizations at risk if they rely solely on NVD-based data. Many third-party solutions draw from the same incomplete source, which means they also miss critical information. As a result, security teams may lack the full picture required to assess and respond to threats in a timely and effective manner.

For organizations with compliance obligations or operating in high-risk sectors, this data gap poses a serious problem. Security teams must be able to trust the intelligence that informs their vulnerability management and patching strategies.

**Why Independent Vulnerability Research Matters**

This is where independent research becomes essential. Flexera's Secunia Research provides an alternative approach, one that goes beyond public data sources. It delivers verified, timely, and actionable intelligence backed by expert analysis. Rather than relying solely on automation, Secunia Research adds human verification, context around exploitability, and insights into product-specific risks.

Organizations need more than raw data. They need clarity on which vulnerabilities are relevant, which are exploitable, and which should be prioritized. This can only be achieved through high-quality, continuously updated intelligence that helps reduce the time between disclosure and remediation.

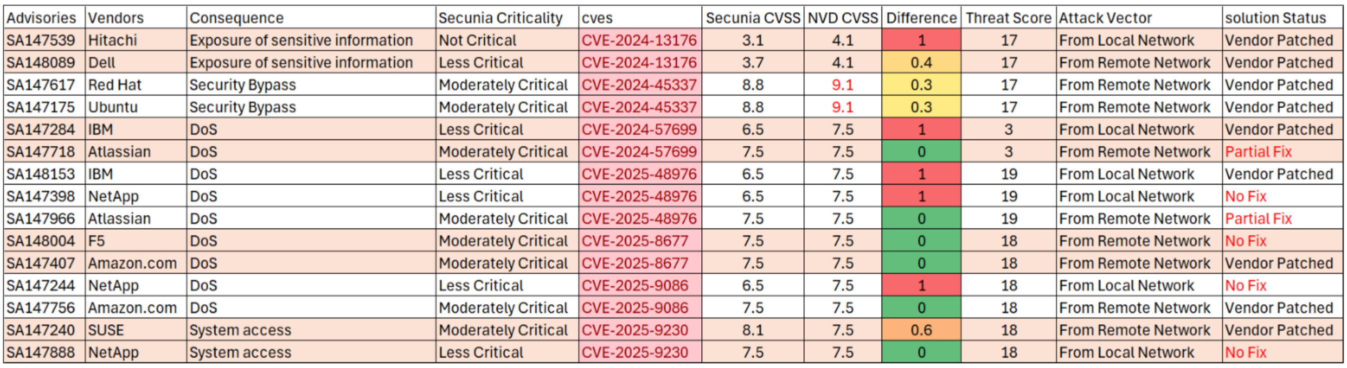
With the increasing pressure from regulations such as the NIS2 Directive in Europe or Australia's Essential Eight, the need for reliable and complete vulnerability intelligence is greater than ever. These frameworks require proactive and auditable approaches to cyber risk, something that cannot be delivered through partial or delayed CVE data.

Secunia Research helps close this gap, giving security and IT operations the insight they need to act quickly and confidently. For those serious about reducing risk and maintaining compliance, relying on **trusted** and **complete** intelligence is not optional. **It is essential.**

# Comparing NVD published information with this month's Secunia Research data

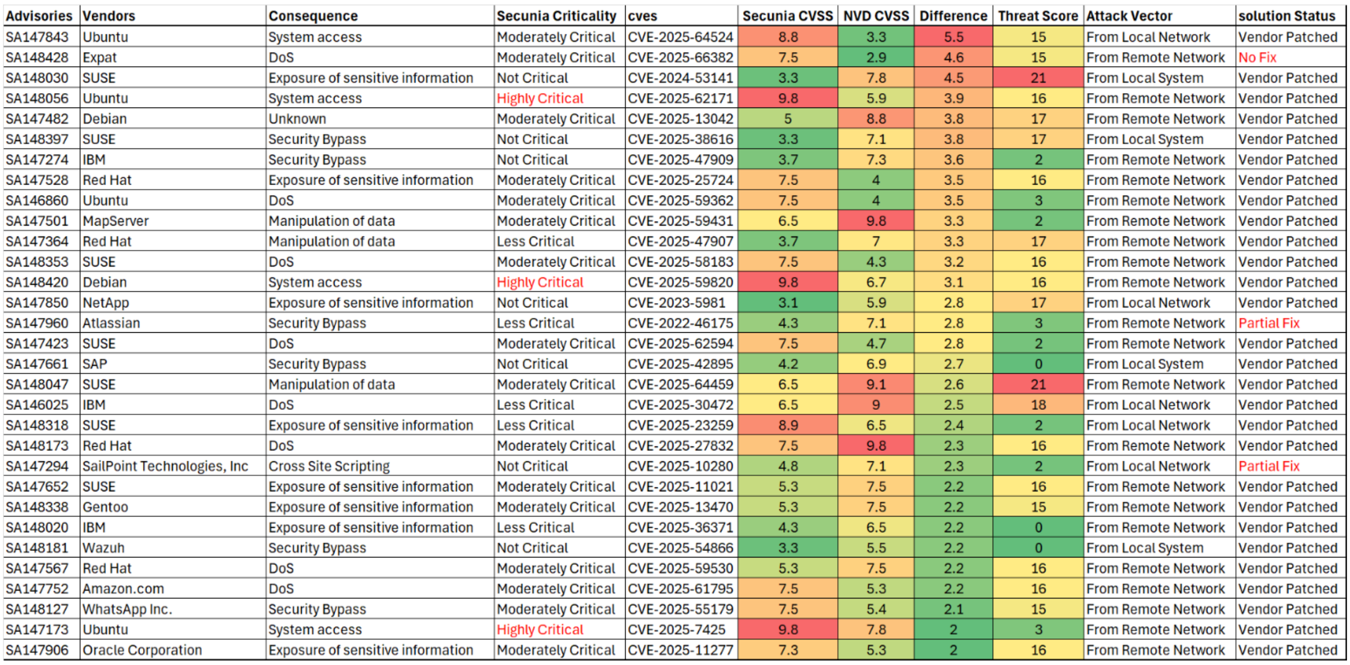
- Using only Secunia Advisories with 1 CVE associated
- No rejection Advisories used
- No NVD CVEs used that had no CVSS Score

Context Matters: (Same CVE , different scores, based vendor and product and context)



| Advisories | Vendors | Consequence | Secunia Criticality | cves | Secunia CVSS | NVD CVSS | Difference | Threat Score | Attack Vector | solution Status |
|---|---|---|---|---|---|---|---|---|---|---|
| SA147539 | Hitachi | Exposure of sensitive information | Not Critical | CVE-2024-13176 | 3.1 | 4.1 | 1 | 17 | From Local Network | Vendor Patched |
| SA148089 | Dell | Exposure of sensitive information | Less Critical | CVE-2024-13176 | 3.7 | 4.1 | 0.4 | 17 | From Remote Network | Vendor Patched |
| SA147617 | Red Hat | Security Bypass | Moderately Critical | CVE-2024-45337 | 8.8 | 9.1 | 0.3 | 17 | From Remote Network | Vendor Patched |
| SA147175 | Ubuntu | Security Bypass | Moderately Critical | CVE-2024-45337 | 8.8 | 9.1 | 0.3 | 17 | From Remote Network | Vendor Patched |
| SA147284 | IBM | DoS | Less Critical | CVE-2024-57699 | 6.5 | 7.5 | 1 | 3 | From Local Network | Vendor Patched |
| SA147718 | Atlassian | DoS | Moderately Critical | CVE-2024-57699 | 7.5 | 7.5 | 0 | 3 | From Remote Network | Partial Fix |
| SA148153 | IBM | DoS | Less Critical | CVE-2025-48976 | 6.5 | 7.5 | 1 | 19 | From Local Network | Vendor Patched |
| SA147398 | NetApp | DoS | Less Critical | CVE-2025-48976 | 6.5 | 7.5 | 1 | 19 | From Local Network | No Fix |
| SA147966 | Atlassian | DoS | Moderately Critical | CVE-2025-48976 | 7.5 | 7.5 | 0 | 19 | From Remote Network | Partial Fix |
| SA148004 | F5 | DoS | Moderately Critical | CVE-2025-8677 | 7.5 | 7.5 | 0 | 18 | From Remote Network | No Fix |
| SA147407 | Amazon.com | DoS | Moderately Critical | CVE-2025-8677 | 7.5 | 7.5 | 0 | 18 | From Remote Network | Vendor Patched |
| SA147244 | NetApp | DoS | Less Critical | CVE-2025-9086 | 6.5 | 7.5 | 1 | 18 | From Local Network | No Fix |
| SA147756 | Amazon.com | DoS | Moderately Critical | CVE-2025-9086 | 7.5 | 7.5 | 0 | 18 | From Remote Network | Vendor Patched |
| SA147240 | SUSE | System access | Moderately Critical | CVE-2025-9230 | 8.1 | 7.5 | 0.6 | 18 | From Remote Network | Vendor Patched |
| SA147888 | NetApp | System access | Less Critical | CVE-2025-9230 | 7.5 | 7.5 | 0 | 18 | From Local Network | No Fix |

Top CVE CVSS Score Compare ( Difference > 2)



| Advisories | Vendors | Consequence | Secunia Criticality | cves | Secunia CVSS | NVD CVSS | Difference | Threat Score | Attack Vector | solution Status |
|---|---|---|---|---|---|---|---|---|---|---|
| SA147843 | Ubuntu | System access | Moderately Critical | CVE-2025-64524 | 8.8 | 3.3 | 5.5 | 15 | From Local Network | Vendor Patched |
| SA148428 | Expat | DoS | Moderately Critical | CVE-2025-66382 | 7.5 | 2.9 | 4.6 | 15 | From Remote Network | No Fix |
| SA148030 | SUSE | Exposure of sensitive information | Not Critical | CVE-2024-53141 | 3.3 | 7.8 | 4.5 | 21 | From Local System | Vendor Patched |
| SA148056 | Ubuntu | System access | Highly Critical | CVE-2025-62171 | 9.8 | 5.9 | 3.9 | 16 | From Remote Network | Vendor Patched |
| SA147482 | Debian | Unknown | Moderately Critical | CVE-2025-13042 | 5 | 8.8 | 3.8 | 17 | From Remote Network | Vendor Patched |
| SA148397 | SUSE | Security Bypass | Not Critical | CVE-2025-38616 | 3.3 | 7.1 | 3.8 | 17 | From Local System | Vendor Patched |
| SA147274 | IBM | Security Bypass | Not Critical | CVE-2025-47909 | 3.7 | 7.3 | 3.6 | 2 | From Remote Network | Vendor Patched |
| SA147528 | Red Hat | Exposure of sensitive information | Moderately Critical | CVE-2025-25724 | 7.5 | 4 | 3.5 | 16 | From Remote Network | Vendor Patched |
| SA146860 | Ubuntu | DoS | Moderately Critical | CVE-2025-59362 | 7.5 | 4 | 3.5 | 3 | From Remote Network | Vendor Patched |
| SA147501 | MapServer | Manipulation of data | Moderately Critical | CVE-2025-59431 | 6.5 | 9.8 | 3.3 | 2 | From Remote Network | Vendor Patched |
| SA147364 | Red Hat | Manipulation of data | Less Critical | CVE-2025-47907 | 3.7 | 7 | 3.3 | 17 | From Remote Network | Vendor Patched |
| SA148353 | SUSE | DoS | Moderately Critical | CVE-2025-58183 | 7.5 | 4.3 | 3.2 | 16 | From Remote Network | Vendor Patched |
| SA148420 | Debian | System access | Highly Critical | CVE-2025-59820 | 9.8 | 6.7 | 3.1 | 16 | From Remote Network | Vendor Patched |
| SA147850 | NetApp | Exposure of sensitive information | Not Critical | CVE-2023-5981 | 3.1 | 5.9 | 2.8 | 17 | From Local Network | Vendor Patched |
| SA147960 | Atlassian | Security Bypass | Less Critical | CVE-2022-46175 | 4.3 | 7.1 | 2.8 | 3 | From Remote Network | Partial Fix |
| SA147423 | SUSE | DoS | Moderately Critical | CVE-2025-62594 | 7.5 | 4.7 | 2.8 | 2 | From Remote Network | Vendor Patched |
| SA147661 | SAP | Security Bypass | Not Critical | CVE-2025-42895 | 4.2 | 6.9 | 2.7 | 0 | From Local System | Vendor Patched |
| SA148047 | SUSE | Manipulation of data | Moderately Critical | CVE-2025-64459 | 6.5 | 9.1 | 2.6 | 21 | From Remote Network | Vendor Patched |
| SA146025 | IBM | DoS | Less Critical | CVE-2025-30472 | 6.5 | 9 | 2.5 | 18 | From Local Network | Vendor Patched |
| SA148318 | SUSE | Exposure of sensitive information | Less Critical | CVE-2025-23259 | 8.9 | 6.5 | 2.4 | 2 | From Local Network | Vendor Patched |
| SA148173 | Red Hat | DoS | Moderately Critical | CVE-2025-27832 | 7.5 | 9.8 | 2.3 | 16 | From Remote Network | Vendor Patched |
| SA147294 | SailPoint Technologies, Inc | Cross Site Scripting | Not Critical | CVE-2025-10280 | 4.8 | 7.1 | 2.3 | 2 | From Local Network | Partial Fix |
| SA147652 | SUSE | Exposure of sensitive information | Moderately Critical | CVE-2025-11021 | 5.3 | 7.5 | 2.2 | 16 | From Remote Network | Vendor Patched |
| SA148338 | Gentoo | Exposure of sensitive information | Moderately Critical | CVE-2025-13470 | 5.3 | 7.5 | 2.2 | 15 | From Remote Network | Vendor Patched |
| SA148020 | IBM | Exposure of sensitive information | Less Critical | CVE-2025-36371 | 4.3 | 6.5 | 2.2 | 0 | From Remote Network | Vendor Patched |
| SA148181 | Wazuh | Security Bypass | Not Critical | CVE-2025-54866 | 3.3 | 5.5 | 2.2 | 0 | From Local System | Vendor Patched |
| SA147567 | Red Hat | DoS | Moderately Critical | CVE-2025-59530 | 5.3 | 7.5 | 2.2 | 16 | From Remote Network | Vendor Patched |
| SA147752 | Amazon.com | DoS | Moderately Critical | CVE-2025-61795 | 7.5 | 5.3 | 2.2 | 16 | From Remote Network | Vendor Patched |
| SA148127 | WhatsApp Inc. | Security Bypass | Moderately Critical | CVE-2025-55179 | 7.5 | 5.4 | 2.1 | 15 | From Remote Network | Vendor Patched |
| SA147173 | Ubuntu | System access | Highly Critical | CVE-2025-7425 | 9.8 | 7.8 | 2 | 3 | From Remote Network | Vendor Patched |
| SA147906 | Oracle Corporation | Exposure of sensitive information | Moderately Critical | CVE-2025-11277 | 7.3 | 5.3 | 2 | 16 | From Remote Network | Vendor Patched |

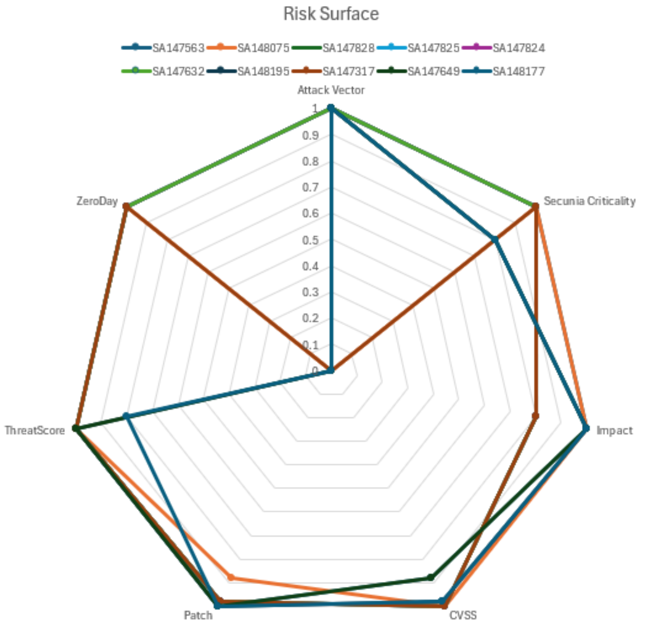
# Risk Scoring Model:

There are many ways to prioritize Software Vulnerabilities ,
a previous article I wrote on LinkedIn : Key Elements of a Balanced Risk Scoring Model I shared some key components that can build a balanced risk scoring model. There is no standard in prioritizing vulnerability remediation , but the goal is to spark some discussion about what's important, and for obvious reasons , I've used the Secunia Research Data to perform the calculation.

My current model is based on 7 variables that have been normalized to a score between 0 and 1 based on custom scaling or just using the score as is (CVSS)

- Attack Vector
- Secunia Criticality Score
- Impact / Consequence
- CVSS Score
- Patch Availability
- Threat Intelligence
- Zero Day

With that the Risk Score will be between 0 – 7 (0 = rejected)



**Top Advisories released this month based on the calculated Risk Score:**

| Advisories | Product Versions | impact or consequence | OS | Secunia Criticality | Impact | CVSS Score | Vendor Patched | Threat Score | Zero Day | Risk Score |
|---|---|---|---|---|---|---|---|---|---|---|
| SA147563 | Microsoft Edge (Chromium-Based) | System access | FALSE | **Extreme Critical** | 1 | 8.8 | Yes | 94 | TRUE | **6.88** |
| SA148075 | Google Chrome 142.x | System access | FALSE | **Extreme Critical** | 1 | 8.8 | Yes | 94 | TRUE | **6.88** |
| SA147828 | Microsoft Windows 10 | System access | TRUE | Highly Critical | 1 | 9.8 | Yes | 99 | TRUE | **6.78** |
| SA147825 | Microsoft Windows Server 2019 & 2022 | System access | TRUE | Highly Critical | 1 | 9.8 | Yes | 99 | TRUE | **6.78** |
| SA147824 | Microsoft Windows 11 | System access | TRUE | Highly Critical | 1 | 9.8 | Yes | 99 | TRUE | **6.78** |
| SA147632 | Microsoft Windows Server 2025 | System access | TRUE | Highly Critical | 1 | 9.8 | Yes | 99 | TRUE | **6.78** |

### Risk Score Thresholds

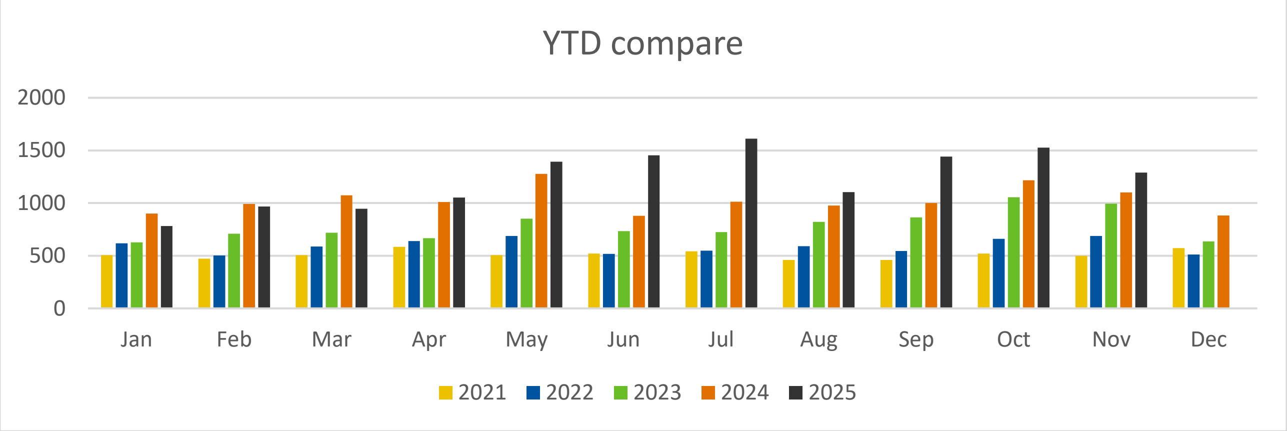
| Attack Vector | Secunia Criticality | Impact Severity |
|---|---|---|
| Remote Network → 1.0<br>Local Network → 0.5<br>Local System → 0.2<br>Unknown → 0.0 | Extreme Critical → 1.0<br>Highly Critical → 0.8<br>Moderately Critical → 0.6<br>Less Critical → 0.4<br>Not Critical → 0.2<br>Rejected → 0.0 | System Access → 1.0<br>Privilege Escalation, Spoofing → 0.9<br>XSS, Hijacking → 0.8<br>Info Exposure, Data Manipulation → 0.7<br>DoS, Security Bypass → 0.6<br>System Info Exposure, Unknown → 0.5 |

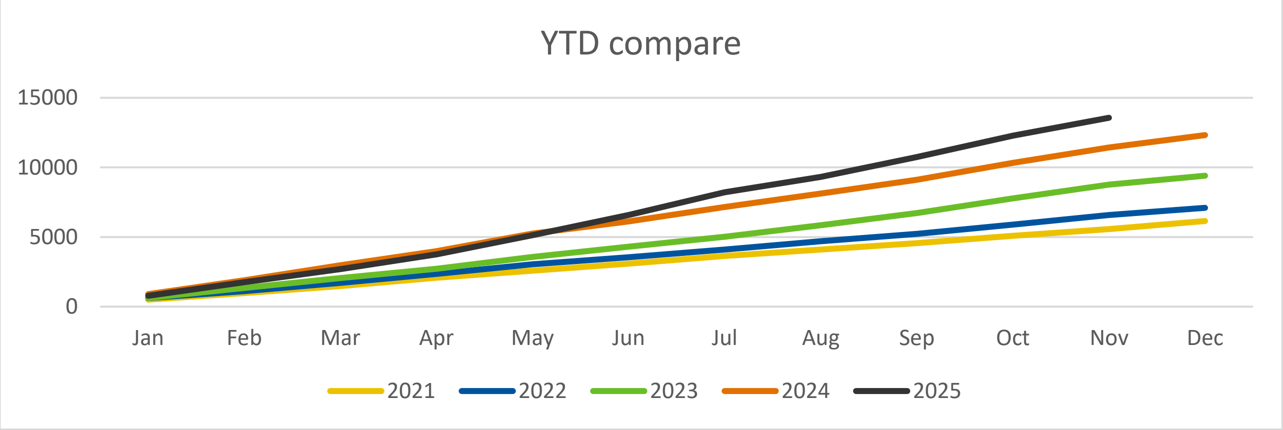
| CVSS Score | Patch Availability | Threat Score |
|---|---|---|
| CVSS v3 ÷ 10 → 0.0 - 1.0 | Vendor Patched → 1.0<br>Partial Fix, Workaround → 0.5<br>No Fix / Unknown → 0.0 | 71+ → 1.0<br>45 - 70 → 0.8<br>24 - 44 → 0.6<br>13 - 23 → 0.4<br>1 - 12 → 0.2<br>0 or unranked → 0.0 |

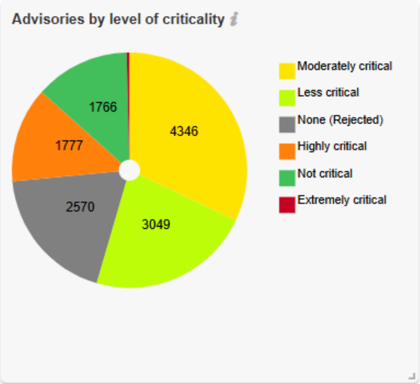
| Zero-Day | Risk Score Formula | |
|---|---|---|
| True → 1.0 | Risk Score = | Sum of all scores |
| False → 0.0 | Higher Score = Higher Risk | Used for prioritization & patching |

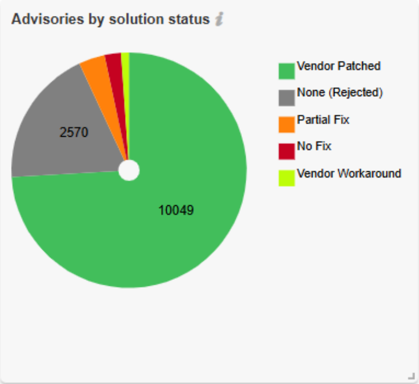
# Year-to-date overview

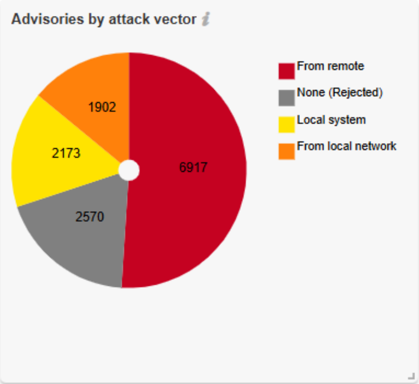
As of **November 30,2025**, the year-to-date total is **13,562** Advisories, which is **18.6%** more than 2024: **11,437** YTD Advisories)

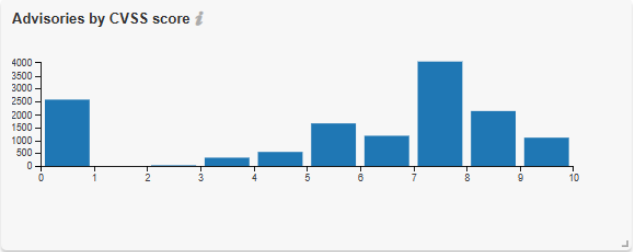


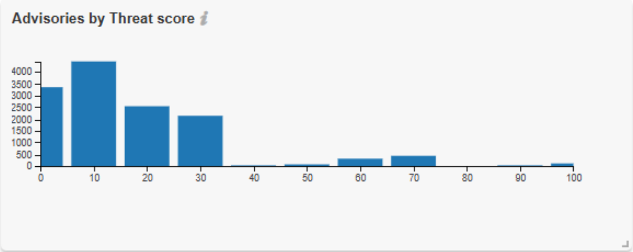












# Monthly data

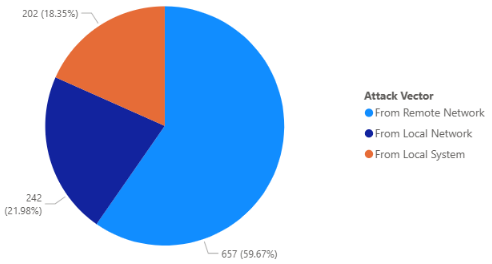
This month, a total of **1,526** ↑ (last month: **1,526**) advisories were reported by the Secunia Research Team.

| This month: | # | Change *(last month):* |
|---|---|---|
| Total # of advisories | **1,289** | ↓ **(1,526)** |
| Unique Vendors | **101** | ↑ **(93)** |
| Unique Products | **284** | ↓ **(336)** |
| Unique Versions | **337** | ↓ **(405)** |
| Rejected Advisories * | **188** | ↓ **(250)** |
| **NEW** Advisories without CVE ID | **36** | ↑ **(20)** |
| Advisories with Threat Score (>0) | **1,289** | ↑ **(1,132)** |
| Total Unique CVE ID's reported | **4,334** | ↑ **(3,236)** |
| | | ↑ increased ↓lower ↔ same |

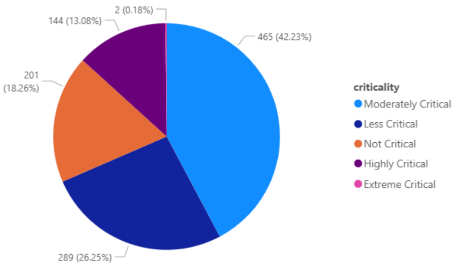
** **188** advisories have received the "rejected" status which means in general that leveraging it would require one or more violations of security best practices (e.g., product not securely configured or not used securely) or that it was "too weak of a gain" (e.g., administrative, local users already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

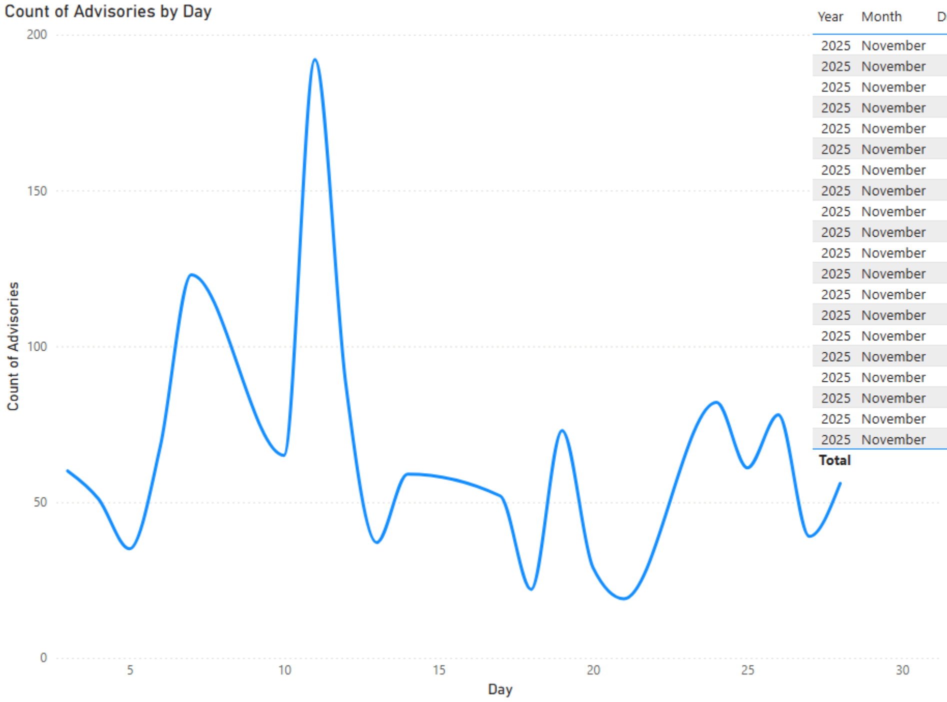


## Advisories by criticality



## Advisories per day

Below an overview of the daily advisory count.



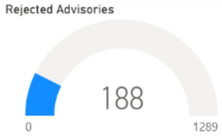
| Year | Month | Day | # of Advisories |
|---|---|---|---|
| 2025 | November | 3 | 60 |
| 2025 | November | 4 | 51 |
| 2025 | November | 5 | 35 |
| 2025 | November | 6 | 68 |
| 2025 | November | 7 | 123 |
| 2025 | November | 10 | 65 |
| 2025 | November | 11 | 192 |
| 2025 | November | 12 | 88 |
| 2025 | November | 13 | 37 |
| 2025 | November | 14 | 59 |
| 2025 | November | 17 | 52 |
| 2025 | November | 18 | 22 |
| 2025 | November | 19 | 73 |
| 2025 | November | 20 | 29 |
| 2025 | November | 21 | 19 |
| 2025 | November | 24 | 82 |
| 2025 | November | 25 | 61 |
| 2025 | November | 26 | 78 |
| 2025 | November | 27 | 39 |
| 2025 | November | 28 | 56 |
| **Total** | | | **1289** |

## Advisories without CVE

| Advisories | Versions | CVSS3 | Criticality | Description | Solution status |
|---|---|---|---|---|---|
| SA147332 | Ubuntu 25.04, Ubuntu Linux 24.04 | 9.80 | Highly Critical | Ubuntu update for keystone | Vendor Patched |
| SA148095 | Debian 12.x, Debian 13.x | 9.80 | Highly Critical | Debian update for keystone | Vendor Patched |
| SA147174 | Confluent Platform 7.x | 8.00 | Less Critical | Confluent Platform Operator Security Bypass Vulnerability | Vendor Patched |
| SA147476 | WibuKey Runtime for Windows 6.x | 7.80 | Less Critical | WibuKey Runtime for Windows Multiple Vulnerabilities | Vendor Patched |
| SA147410 | libarchive 3.x | 7.50 | Moderately Critical | libarchive "find_elf_data_sec()" Out-Of-Bounds Read Memory Access Vulnerability | Vendor Patched |
| SA147538 | Libxml2 | 7.50 | Moderately Critical | Libxml2 "xmlSetTreeDoc()" Denial of Service Vulnerability | Vendor Workaround |
| SA147146 | SUSE Linux Enterprise Server (SLES) 15 SP7 | 6.10 | Moderately Critical | SUSE update for cdi-apiserver-container, cdi-cloner-container, cdi-controller-container, cdi-importer-container, cdi-operator-container, cdi-uploadproxy-container, cdi-uploadserver-container, cont | Vendor Patched |
| SA147373 | Zimbra Collaboration Suite 10.x | 6.10 | Moderately Critical | Zimbra Collaboration Suite Multiple Vulnerabilities | Vendor Patched |
| SA147472 | Zimbra Collaboration Suite 10.x | 6.10 | Moderately Critical | Zimbra Collaboration Suite Multiple Vulnerabilities | Vendor Patched |
| SA147204 | CyberArk Privileged Access Manager 14.x, Privileged Access Manager 14.x | 5.60 | Moderately Critical | CyberArk Privileged Access Manager Multiple Unspecified Vulnerabilities | Vendor Patched |
| SA147250 | Amazon Linux 2023 | 5.60 | Moderately Critical | Amazon Linux update for runc | Vendor Patched |
| SA147486 | Amazon Linux 2 | 5.60 | Moderately Critical | Amazon Linux update for runc | Vendor Patched |
| SA147487 | Amazon Linux 2 | 5.60 | Moderately Critical | Amazon Linux update for runc | Vendor Patched |
| SA147495 | Amazon Linux 2 | 5.60 | Moderately Critical | Amazon Linux update for runc | Vendor Patched |
| SA147915 | Magnolia 6.x | 5.60 | Moderately Critical | Magnolia Multiple Unspecified Vulnerabilities | Vendor Patched |
| SA148031 | SUSE Liberty Linux 8.x | 5.60 | Moderately Critical | SUSE update for idm:client | Vendor Patched |
| SA148032 | SUSE Liberty Linux 8.x | 5.60 | Moderately Critical | SUSE update for idm:DL1 | Vendor Patched |
| SA148141 | CA Aion Business Rules Expert 11.x | 5.60 | Moderately Critical | CA Aion Business Rules Expert for Windows LibXML2 Unspecified Vulnerability | Partial Fix |
| SA148171 | Mattermost 10.x | 5.60 | Moderately Critical | Mattermost Multiple Unspecified Vulnerabilities | Vendor Patched |
| SA148329 | Mattermost 10.x | 5.60 | Moderately Critical | Mattermost Jira Plugin Unspecified Vulnerability | Vendor Patched |
| SA148232 | ZED! Enterprise for Linux 2023.x | 5.50 | Not Critical | ZED! Enterprise for Linux GUI Multi-User Security Bypass Vulnerability | Vendor Patched |
| SA148336 | Debian 12.x, Debian 13.x | 5.40 | Less Critical | Debian update for tryton-sao | Vendor Patched |
| SA147302 | CA Workload Automation 7.x | 5.00 | Less Critical | CA Workload Automation Multiple Unspecified Vulnerabilities | Partial Fix |
| SA147329 | IBM DB2 11.x, IBM DB2 Connect 11.x | 4.30 | Less Critical | IBM Db2 / Db2 Connect FasterXML Jackson Denial of Service Vulnerability | Vendor Patched |
| SA147333 | Pega Platform 8.x | 4.30 | Less Critical | Pega Platform Cross-Site Request Forgery Vulnerability | Vendor Patched |
| SA147339 | IBM DB2 11.x | 4.30 | Less Critical | IBM Db2 Apache Commons Information Disclosure Vulnerability | Vendor Patched |
| SA148419 | Debian 12.x, Debian 13.x | 4.30 | Less Critical | Debian update for tryton-server | Vendor Patched |

# Rejected advisories.

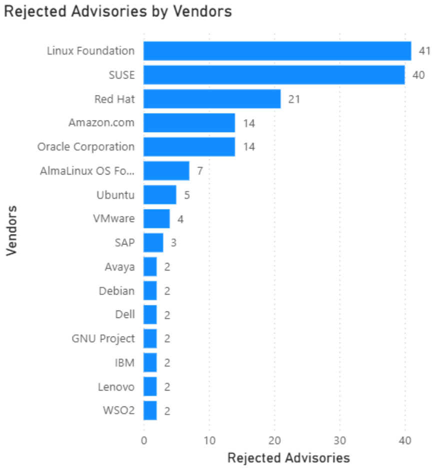
There are many vulnerabilities posted to the National Vulnerability Database (NVD) by a lot of people and companies. They are not always valid, assigned a proper criticality, and in some cases, a vulnerability may be legitimate but not afford the attacker any benefit.

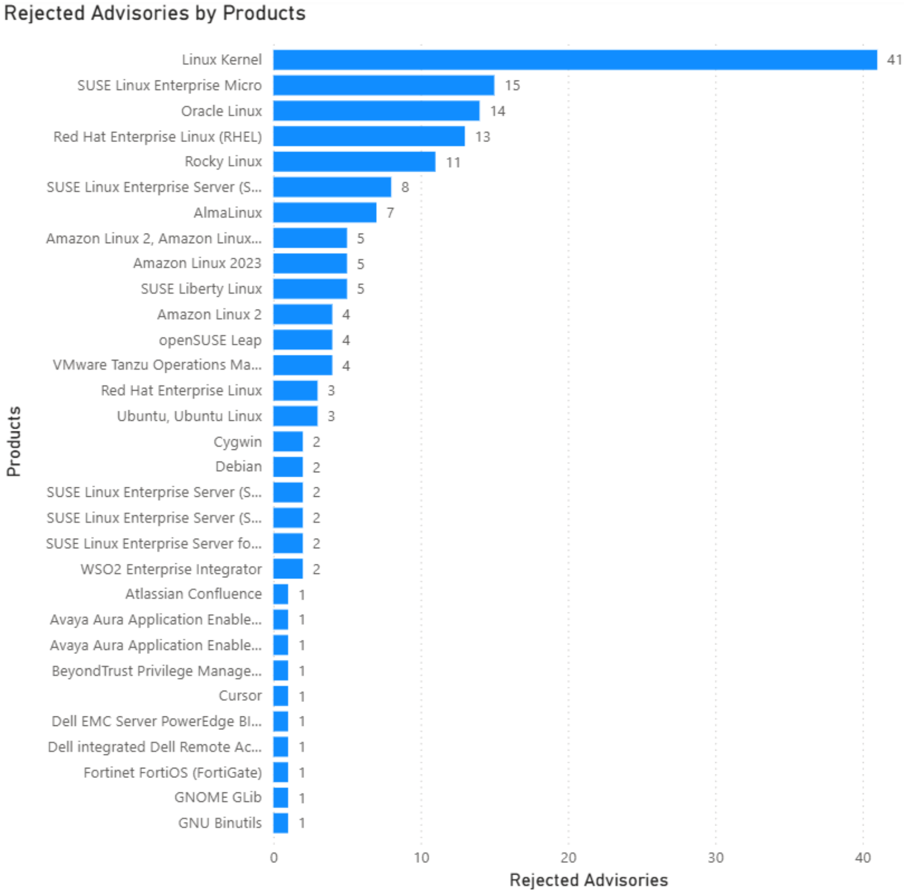


The Secunia Research team at Flexera evaluates vulnerabilities from hundreds of sources, rescores them when necessary and even rejects vulnerabilities not worth your attention. Rejection Advisories help you to reduce the volume of vulnerabilities to be mitigated by helping you focus only on those that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

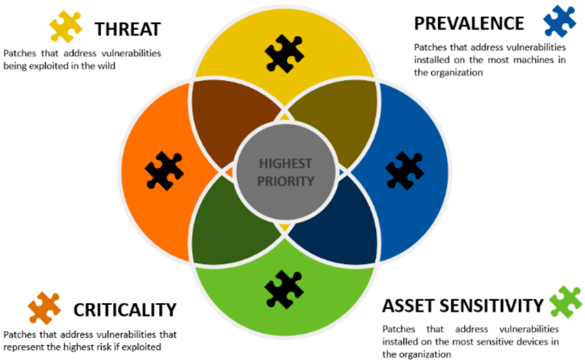
- What systems would result in the most risk if compromised?
- Is it a high-risk device? **Patch**.

**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.

### Take away 1:

Critical vulnerabilities do not necessarily present the most risk.

Leverage threat intelligence to better prioritize what demands your most urgent attention.

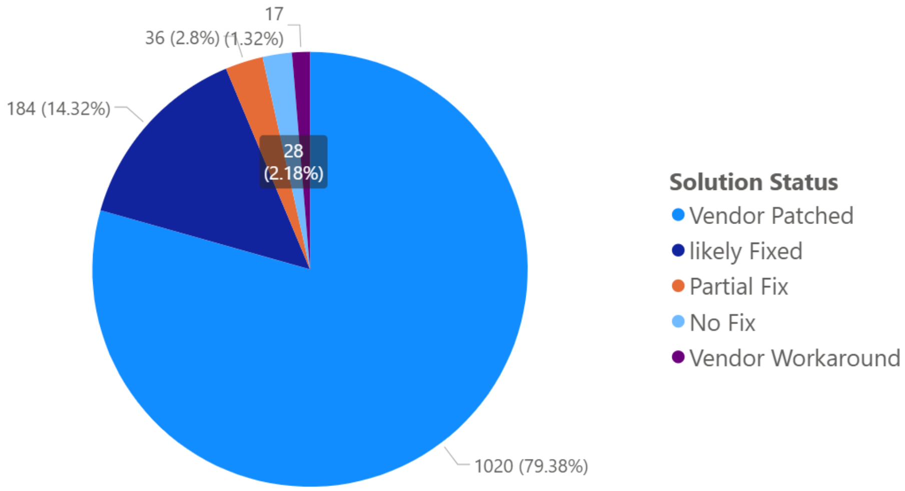
Organizations who do not have Threat Intelligence data should consider implementing this to ensure they have the complete picture.

### 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*

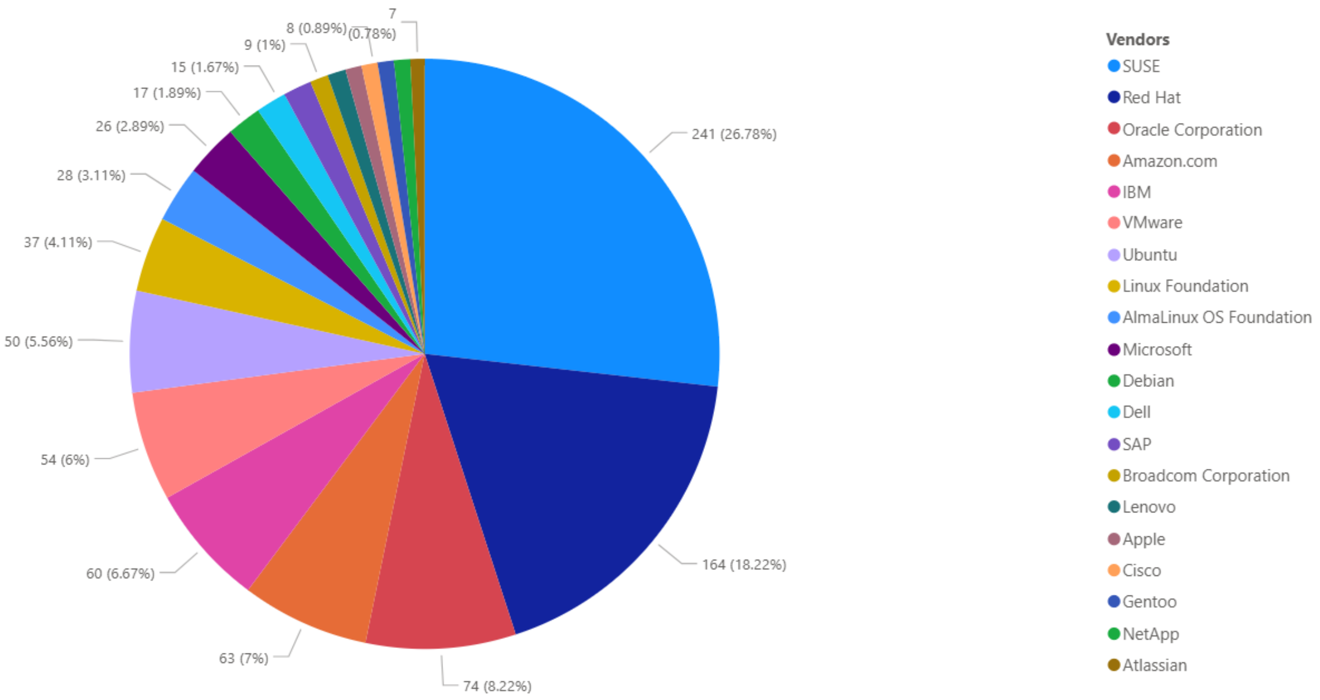
*likely (Possibly) fixed: related to a rejection advisory*



# Vendor view

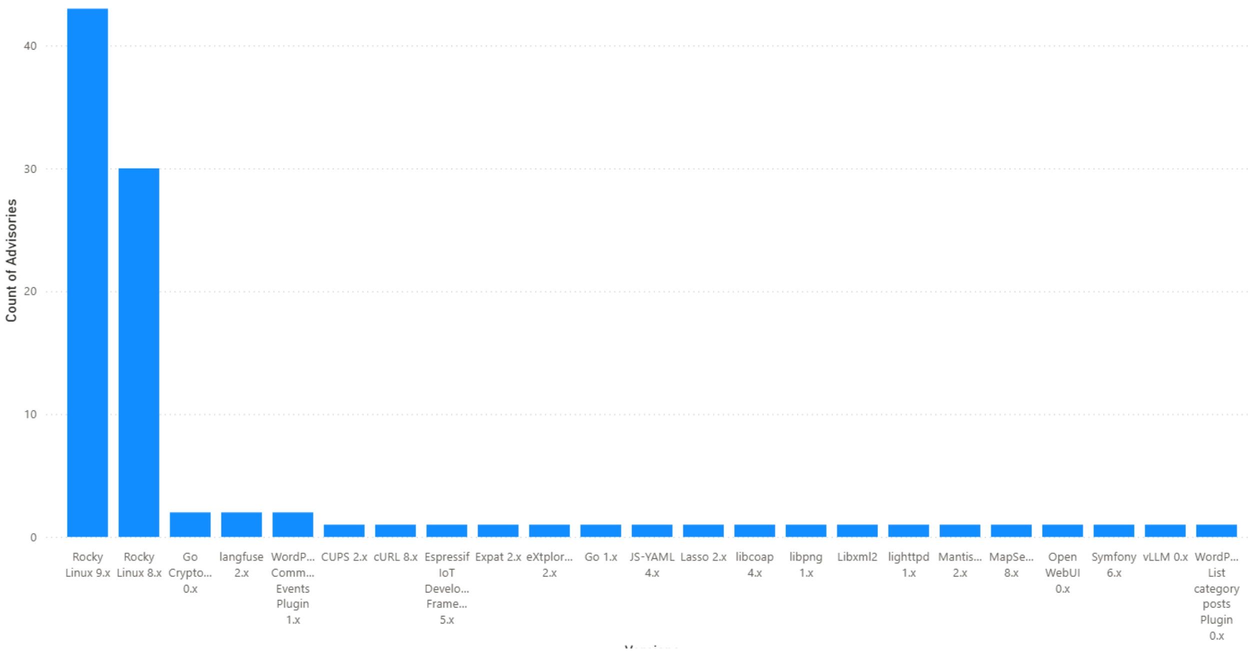
## Top vendors with the most advisories

*(Excl. Rejection Advisories)*

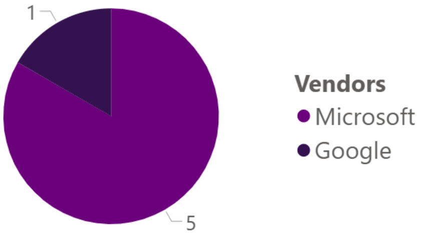


**94 Advisories** this month were open-source products or plugin

## Open-Source Product Versions

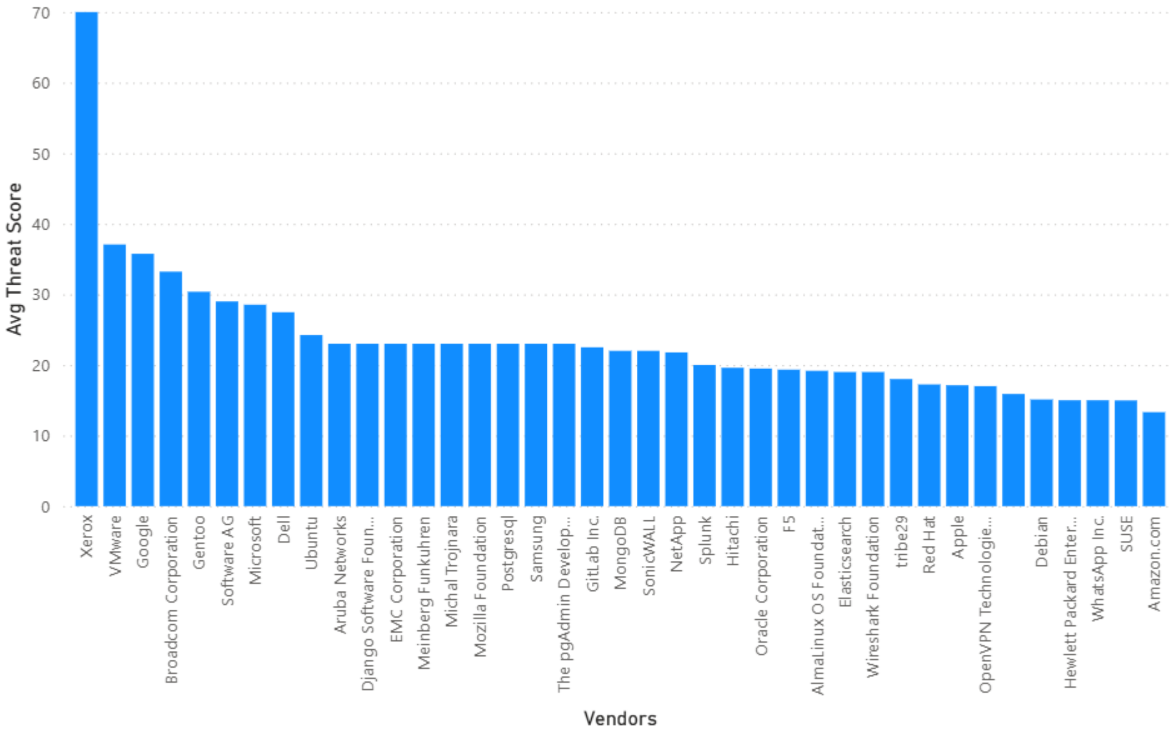


## Top vendors with zero-day



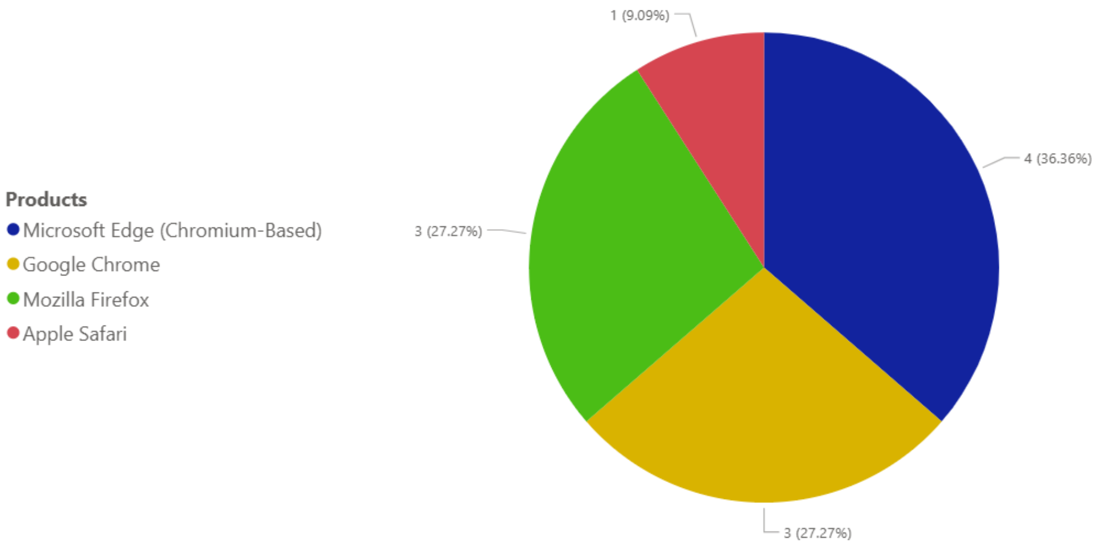
| Advisories | Versions | Threatscore |
|---|---|---|
| SA147828 | Microsoft Windows 10 | 99.00 |
| SA147824 | Microsoft Windows 11 | 99.00 |
| SA147825 | Microsoft Windows Server 2019, Microsoft Windows Server 2022 | 99.00 |
| SA147632 | Microsoft Windows Server 2025 | 99.00 |
| SA148075 | Google Chrome 142.x | 94.00 |
| SA147563 | Microsoft Edge (Chromium-Based) | 94.00 |

## Top Vendors with highest average threat score



# Browser-related advisories

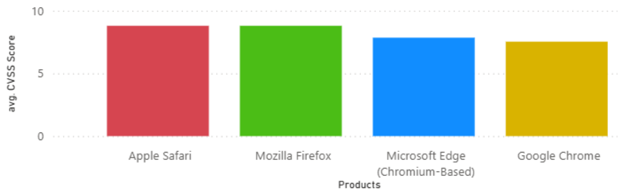
## Advisories per browser



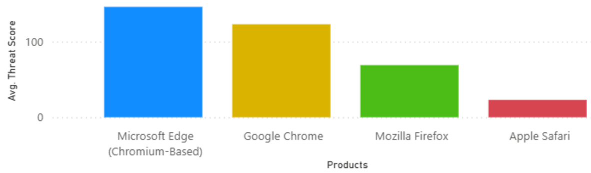
## Browser zero-day vulnerabilities

| Description | Advisories | Cvss3 | ThreatScore | Consequence | ZeroDay |
|---|---|---|---|---|---|
| Microsoft Edge (Chromium-Based) Multiple Arbitrary Code Execution Vulnerabilities | SA147563 | 8.80 | 94.00 | System access | True |
| Google Chrome Multiple Arbitrary Code Execution Vulnerabilities | SA148075 | 8.80 | 94.00 | System access | True |

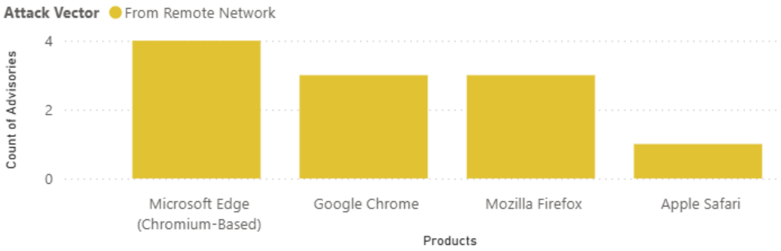
## Average CVSS (criticality) score per browser



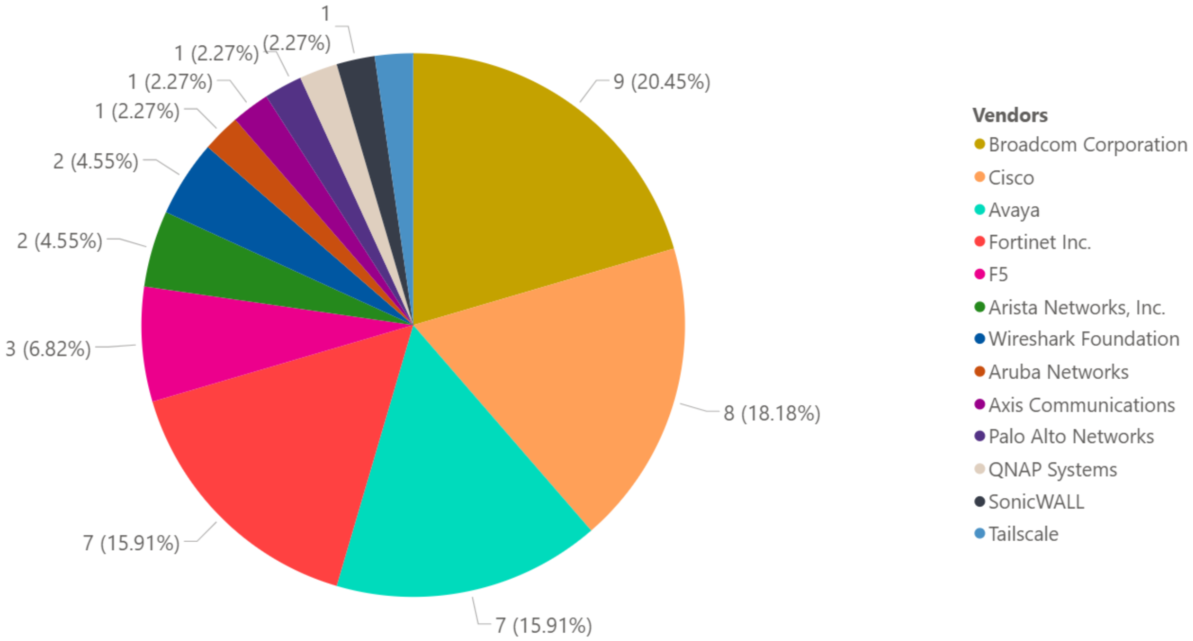
## Average threat score per browser



## What's the Attack Vector?



## Top networking related advisories



# Threat intelligence

In a world where there are more than 40,000 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.

## Threat intelligence data:

| Type of Threat affecting Advisories | # SAIDS | | *Last month* |
|---|---|---|---|
| Penetration Testing Tools | 659 | ↑ | *655* |
| Ransomware Links | 39 | ↑ | *23* |
| Recent Cyber Exploits | 79 | ↓ | *127* |
| Historical Cyber Exploit | 336 | ↑ | *306* |
| Linked to Malware | 382 | ↑ | *307* |

## Threat intelligence advisory statistics

| | |
|---|---|
| SAIDs with a threat score (1+) | **1,021**↓ (1,132*)* |
| SAIDs with no threat score (=0) | **268** ↓ *(394)* |

*SAID: Secunia Advisory Identifier*

| Range | # SAIDS | | *Last month* |
|---|---|---|---|
| Medium-range threat score SAIDs (13-23) | 705 | ↓ | *(902)* |
| Low-range threat score SAIDs (1-12) | 246 | ↑ | *(179 )* |
| **Critical-range threat score SAIDs (45-70)** | **40** | ↑ | *(14)* |
| **Very critical threat score SAIDs (71-99)** | **21** | ↑ | *(17)* |
| **High-range threat score SAIDs (24-44)** | **9** | ↓ | *(20)* |

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

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

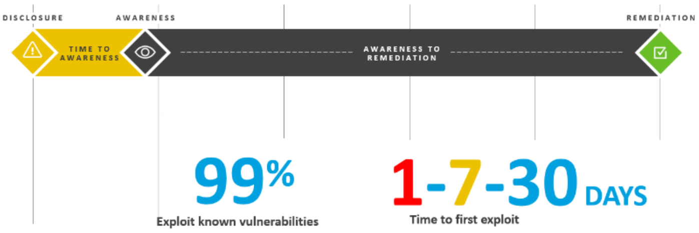
# Patching

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

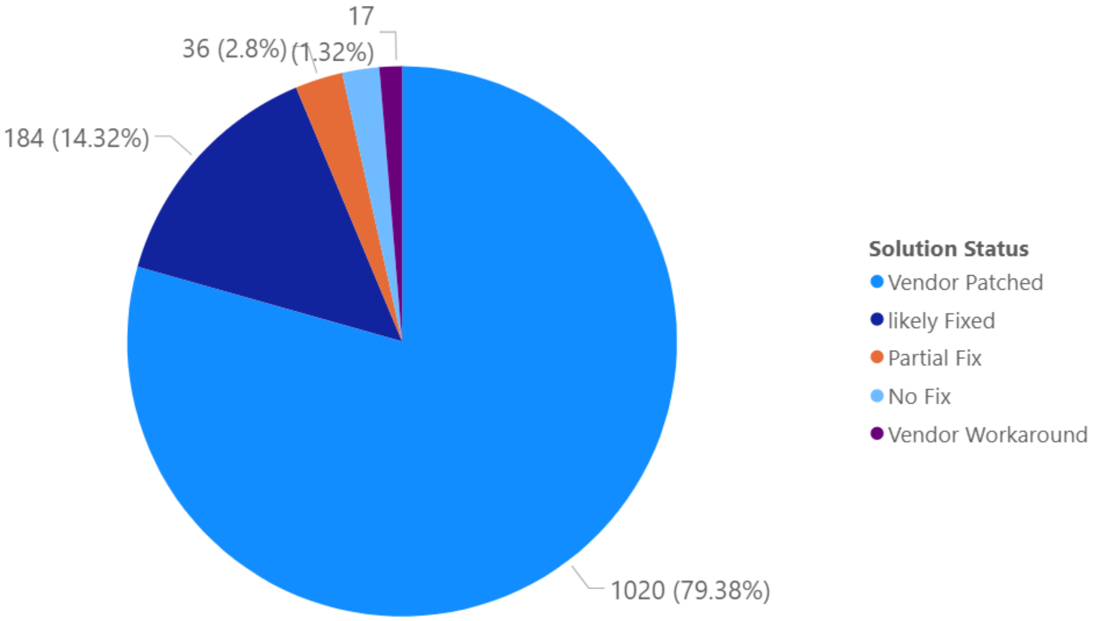
The challenge remains that organizations do not have full visibility or awareness when a vulnerability is disclosed (time to awareness). Another big challenge is the time to remediation (the time from having this information, correlating that with your environment and initiating the process to get the software updated to a secure version).

### The Risk Window

192 DAYS TO REMEDIATION

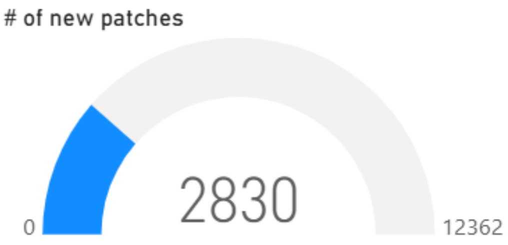


## Vulnerabilities that are vendor patched



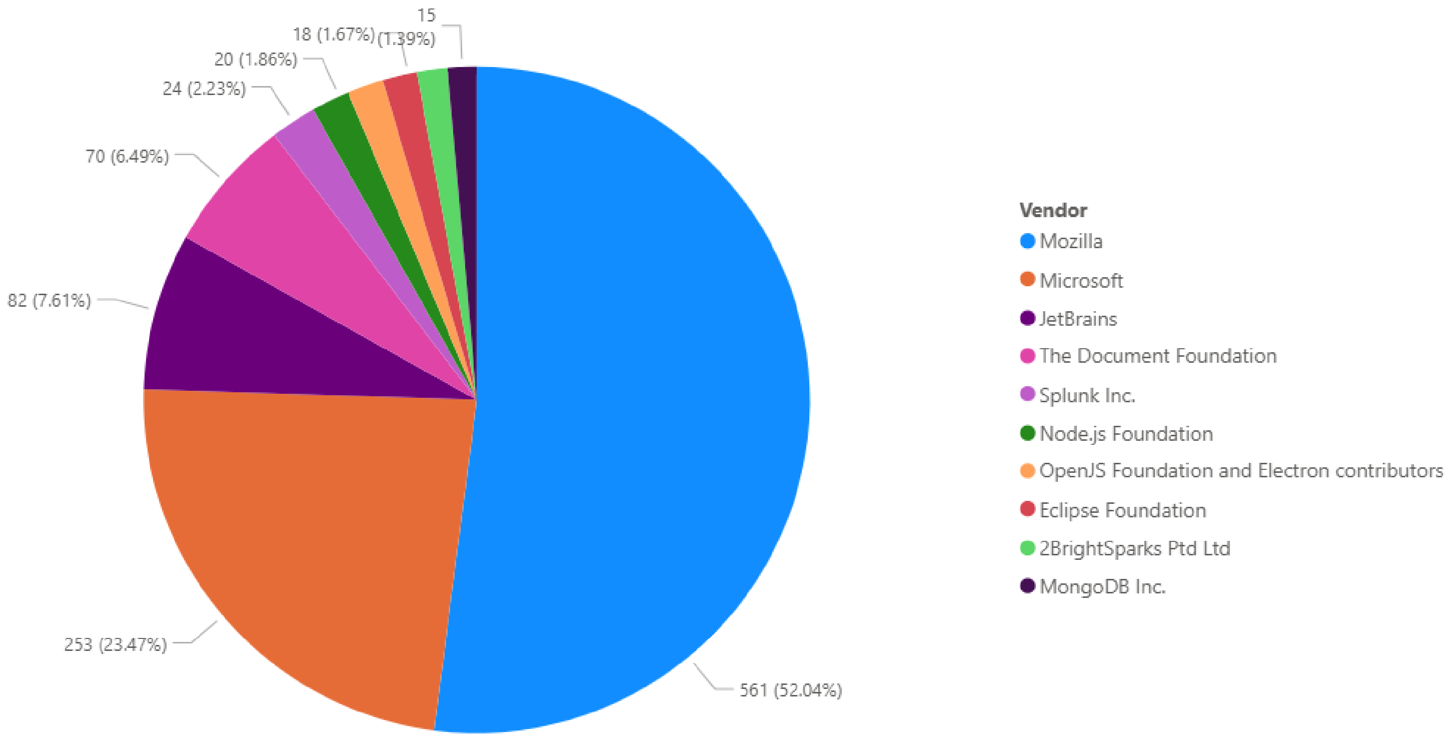
## Flexera's Vendor Patch Module (VPM) statistics

Flexera has the largest third-party patch catalog **(12,000+)** 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 10 vendor patches

(Updated Patches per vendor, NOT including MS Patch Tuesday patches)

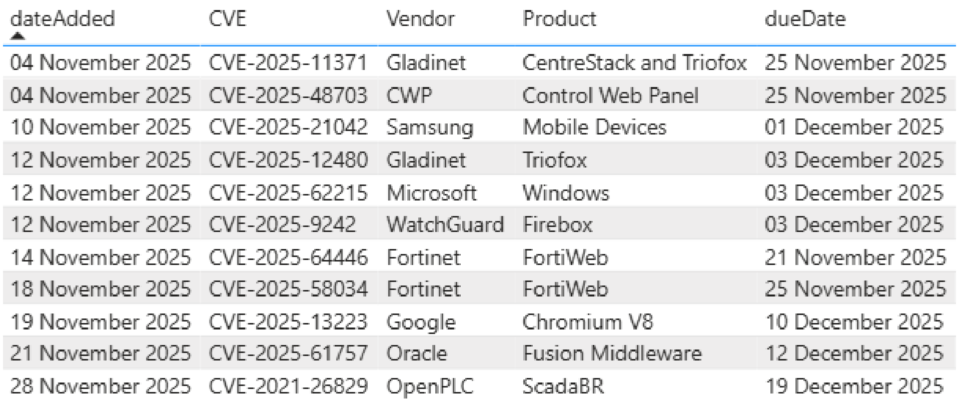


# Other sources

## 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.

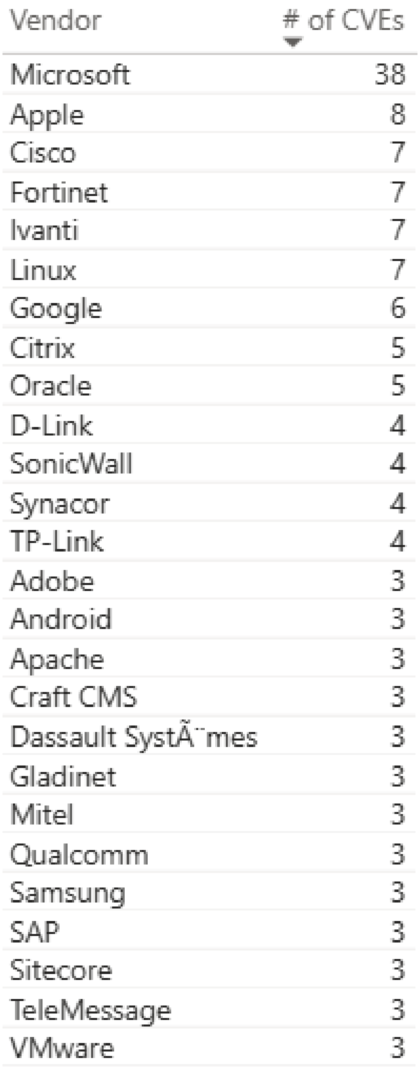
### This months' the additions to the KEV catalog



| dateAdded | CVE | Vendor | Product | dueDate |
|---|---|---|---|---|
| 04 November 2025 | CVE-2025-11371 | Gladinet | CentreStack and Triofox | 25 November 2025 |
| 04 November 2025 | CVE-2025-48703 | CWP | Control Web Panel | 25 November 2025 |
| 10 November 2025 | CVE-2025-21042 | Samsung | Mobile Devices | 01 December 2025 |
| 12 November 2025 | CVE-2025-12480 | Gladinet | Triofox | 03 December 2025 |
| 12 November 2025 | CVE-2025-62215 | Microsoft | Windows | 03 December 2025 |
| 12 November 2025 | CVE-2025-9242 | WatchGuard | Firebox | 03 December 2025 |
| 14 November 2025 | CVE-2025-64446 | Fortinet | FortiWeb | 21 November 2025 |
| 18 November 2025 | CVE-2025-58034 | Fortinet | FortiWeb | 25 November 2025 |
| 19 November 2025 | CVE-2025-13223 | Google | Chromium V8 | 10 December 2025 |
| 21 November 2025 | CVE-2025-61757 | Oracle | Fusion Middleware | 12 December 2025 |
| 28 November 2025 | CVE-2021-26829 | OpenPLC | ScadaBR | 19 December 2025 |

## Top (YTD) KEV vendors

Vendors added this year with Known Exploited Vulnerabilities according to CISA

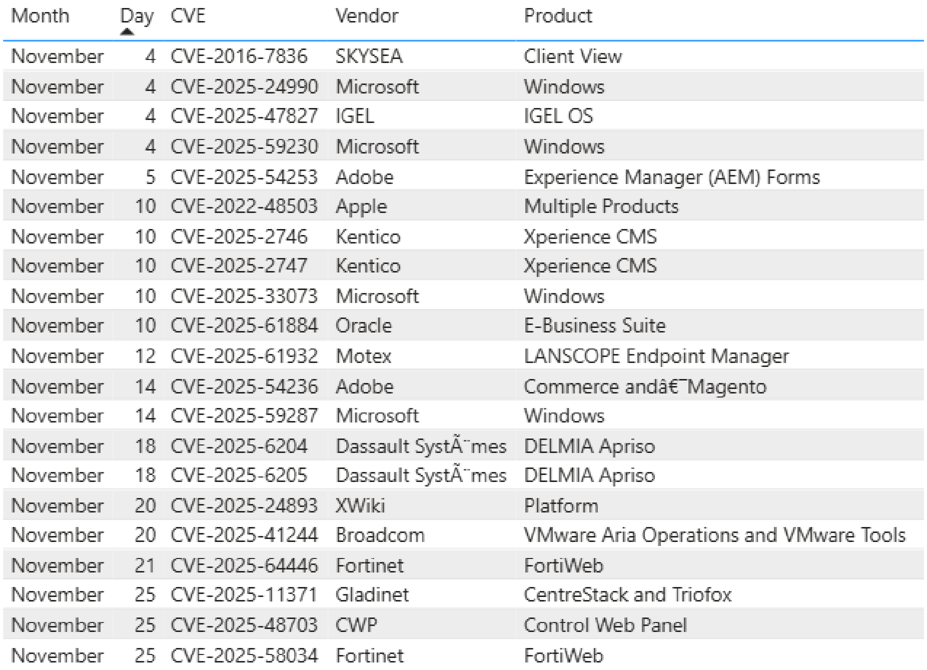


| Vendor | # of CVEs |
|---|---|
| Microsoft | 38 |
| Apple | 8 |
| Cisco | 7 |
| Fortinet | 7 |
| Ivanti | 7 |
| Linux | 7 |
| Google | 6 |
| Citrix | 5 |
| Oracle | 5 |
| D-Link | 4 |
| SonicWall | 4 |
| Synacor | 4 |
| TP-Link | 4 |
| Adobe | 3 |
| Android | 3 |
| Apache | 3 |
| Craft CMS | 3 |
| Dassault SystÃ¨mes | 3 |
| Gladinet | 3 |
| Mitel | 3 |
| Qualcomm | 3 |
| Samsung | 3 |
| SAP | 3 |
| Sitecore | 3 |
| TeleMessage | 3 |
| VMware | 3 |

## 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 |
|---|---|---|---|---|
| November | 4 | CVE-2016-7836 | SKYSEA | Client View |
| November | 4 | CVE-2025-24990 | Microsoft | Windows |
| November | 4 | CVE-2025-47827 | IGEL | IGEL OS |
| November | 4 | CVE-2025-59230 | Microsoft | Windows |
| November | 5 | CVE-2025-54253 | Adobe | Experience Manager (AEM) Forms |
| November | 10 | CVE-2022-48503 | Apple | Multiple Products |
| November | 10 | CVE-2025-2746 | Kentico | Xperience CMS |
| November | 10 | CVE-2025-2747 | Kentico | Xperience CMS |
| November | 10 | CVE-2025-33073 | Microsoft | Windows |
| November | 10 | CVE-2025-61884 | Oracle | E-Business Suite |
| November | 12 | CVE-2025-61932 | Motex | LANSCOPE Endpoint Manager |
| November | 14 | CVE-2025-54236 | Adobe | Commerce andâ€¯Magento |
| November | 14 | CVE-2025-59287 | Microsoft | Windows |
| November | 18 | CVE-2025-6204 | Dassault SystÃ¨mes | DELMIA Apriso |
| November | 18 | CVE-2025-6205 | Dassault SystÃ¨mes | DELMIA Apriso |
| November | 20 | CVE-2025-24893 | XWiki | Platform |
| November | 20 | CVE-2025-41244 | Broadcom | VMware Aria Operations and VMware Tools |
| November | 21 | CVE-2025-64446 | Fortinet | FortiWeb |
| November | 25 | CVE-2025-11371 | Gladinet | CentreStack and Triofox |
| November | 25 | CVE-2025-48703 | CWP | Control Web Panel |
| November | 25 | CVE-2025-58034 | Fortinet | FortiWeb |

# 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 helps organizations understand and maximize the value of their technology, saving billions of dollars in wasted spend. Powered by the Flexera Technology Intelligence Platform, our award-winning IT asset management, FinOps and SaaS management solutions provide comprehensive visibility and actionable insights on an organization's entire IT ecosystem. This intelligence enables IT, finance, procurement and cloud teams to address skyrocketing costs, optimize spend, mitigate risk, and identify opportunities to create positive business outcomes.

More than 50,000 global organizations rely on Flexera and its Technopedia reference library, the largest repository of technology asset data. Learn more at flexera.com.

**Secunia Research** from Flexera is comprised of world-class security specialists dedicated to discovering, testing, verifying, and validating vulnerabilities in a wide range of software products. Since 2002, Secunia Research has provided the most accurate and reliable vulnerability intelligence available. The team's expertise ensures that organizations receive the best vulnerability intelligence for mitigating risks effectively.

This industry-leading vulnerability research forms the foundation for two of Flexera's key products: **Software Vulnerability Management (SVM)** and **Software Vulnerability Research (SVR)**.

**SVM** leverages Secunia Research to help organizations proactively manage software vulnerabilities. Automating the identification, reporting, prioritization, and patching of vulnerabilities, shrinking the risk window and increasing security.

With **SVR**, organizations gain access to real-time, verified vulnerability – and threat intelligence. Covering more than 72,000 products, SVR provides detailed advisories that many valuable datapoints to help security teams prioritize remediation efforts, reduce risk, and stay ahead of potential threats.

www.flexera.com/svm