PERISCOPE

12 Aug 2025

INTEL471

TLP: AMBER

CVE WEAPONIZATION REPORT

For more information on our Vulnerability Intelligence see https://intel471.com/titan/vulnerability-intelligence

CVE Prioritized by Intel 471	VENDOR / PRODUCT	PATCH / INTEREST / LOCATION / EXPLOIT
CVE-2025-6218 New Directory traversal	RARLab WinRAR	
CVE-2024-51568 New OS command injection	CyberPanel CyberPanel	
CVE-2023-37941 New Deserialization of untrusted data	Apache Superset	
CVE-2023-39265 New Improper input validation	Apache Superset	
CVE-2020-4429 New Use of hard-coded credentials	IBM Data Risk Manager	
CVE-2020-4428 New OS command injection	IBM Data Risk Manager	
CVE-2023-36661 New SSRF	Shibboleth XMLTooling	
CVE-2025-32462 New Incorrect authorization	Sudo Project Sudo	
CVE-2025-47175 New Use after free	Microsoft Multiple	
CVE-2024-6235 New Improper authentication	Citrix NetScaler Console	
CVE-2023-2533 New CSRF	PaperCut Software NG / MF	
CVE-2025-5287 New SQLi	The Likes and Dislikes The Likes and Dislikes	

CVE Prioritized by Intel 471	VENDOR / PRODUCT	PATCH / INTEREST / LOCATION / EXPLOIT
CVE-2025-31125 New Exposure of sensitive information to an unauthorized actor	ViteJS Vite	
CVE-2025-40599 New Arbitrary file upload	SonicWall SMA 100	
CVE-2025-0133 New XSS	Palo Alto Networks PAN-OS	
CVE-2025-49706 Improper authentication	Microsoft Multiple	
CVE-2025-53771 Path traversal	Microsoft Multiple	
CVE-2025-54309 Unprotected alternate channel	CrushFTP CrushFTP	
CVE-2025-49704 Code injection	Microsoft Multiple	
CVE-2025-53770 Deserialization of untrusted data	Microsoft SharePoint	
CVE-2025-20282 Improper privilege management	Cisco Identity Services Engine (ISE)	
CVE-2025-20337 Injection	Cisco Multiple	
CVE-2025-8044 Improper restriction of operations within the bounds of a memory buffer	Mozilla Firefox	

PATCH / UPDATE STATUS
- UNAVAILABLE
- SOME AVAILABLE
- AVAILABLE

INTEREST LEVEL
- EXPLOIT SOUGHT IN UNDERGROUND
- RESEARCHED PUBLICLY
- DISCLOSED PUBLICLY

LOCATION OF ACTIVITY OR DISCUSSION
- PRIVATE COMMUNICATIONS
- UNDERGROUND
- OPEN SOURCE

EXPLOIT STATUS
- CODE AVAILABLE
- WEAPONIZED
- PRODUCTIZED
- NOT OBSERVED

Intel 471 assesses vulnerabilities using a weighted calculation across the following criteria (in descending order of criticality):

- Mitigation status
- Exploit status
- Underground activity
- CVSSv3 score

FAQ

What is the purpose of this report?

The Common Vulnerabilities and Exposures (CVE) Weaponization Report is a quick reference tool designed to assist patch prioritization and vulnerability management decision-making. This regularly updated report tracks the life cycle of significant vulnerabilities observed in the underground from initial disclosure to exploit weaponization and productization.

What vulnerabilities are included in this report?

To help track vulnerabilities likely to impact you, our approach is to prioritize and monitor vulnerabilities once any of the following criteria have been met:

- A significant CVE is discussed actively in the underground.
- Requests for exploits are observed.
- The CVE is weaponized or productized.

How often is the CVE report sent?

The CVE Weaponization Report will be sent out when underground state changes are observed for new and existing CVEs.

How are CVEs phased out of this report over time?

To keep the report current and concise, a vulnerability is phased out once any of the following criteria is met:

- An existing CVE is weaponized or productized in a previous report.
- An existing CVE was patched or updated with no significant underground discussion and no weaponization.
- An existing CVE has been in the report matrix two times.

What do the different “Interest Level” indicators mean?

- Disclosed publicly – This will apply to CVEs that have been publicly disclosed.
- Researched publicly – This will apply to CVEs when they are observed in research publications (blogs, whitepaper, etc.).
- Exploit sought in underground – This will apply to CVEs when a threat actor is looking for exploits in the underground.

*Note: These are not based on the number of observed underground discussions.

What do the different “Exploit Status” indicators mean?

- Not observed — no exploit code observed.
- Code available — exploit proof-of-concept (PoC) code has been published or shared.
- Weaponized — integrated into malicious code for use by sophisticated actors (i.e., exploit kits, malvertising).
- Productized — available for use in mass production by unsophisticated actors (i.e., incorporating exploit into Armitage or Metasploit).

What does “patch or update” mean?

The impacted vendor released mitigation information such as software updates or patching details to address the vulnerability.