PERISCOPE

7 Oct 2025

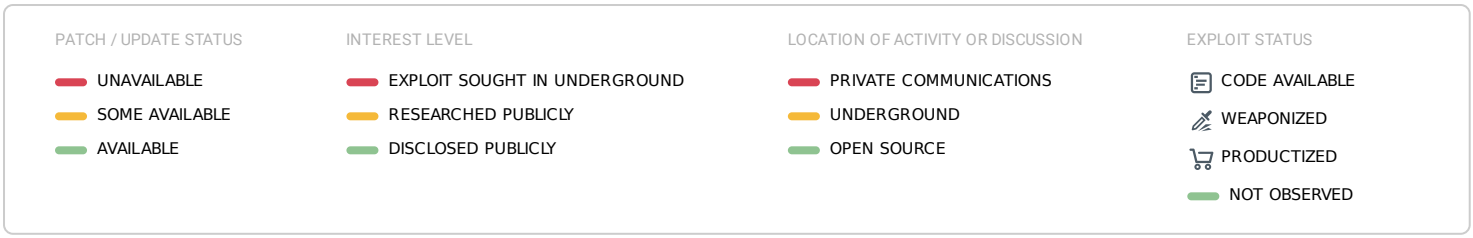
INTEL471

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-2025-10035 New Deserialization of untrusted data	Fortra GoAnywhere MFT	
CVE-2025-20352 New Stack-based buffer overflow	Cisco Multiple	
CVE-2021-39226 New Authentication bypass	Grafana Grafana	
CVE-2025-26399 New Deserialization of untrusted data	SolarWinds Web Help Desk (WHD)	
CVE-2025-54236 New Improper input validation	Adobe Commerce	
CVE-2025-59689 New Command injection	Libraesva Email Security Gateway (ESG)	
CVE-2024-28988 New Deserialization of untrusted data	SolarWinds Web Help Desk (WHD)	
CVE-2023-38941 RCE	Django-sspanel Django-sspanel	
CVE-2025-5086 Deserialization of untrusted data	Dassault DELMIA Apriso	
CVE-2025-52970 Improper handling of parameters	Fortinet FortiWeb	
CVE-2025-3515 Arbitrary file upload	Drop Multiple File Upload for Contact Form 7 WordPress plugin Drop Multiple File Upload for Contact Form 7 WordPress plugin	
CVE-2025-10585 Type confusion	Google Chrome	
CVE-2025-53772 Deserialization of untrusted data	Microsoft IIS Web Deploy	
CVE-2025-55147 CSRF	Ivanti Multiple	



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.