








































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-2025-7775 <small>New</small> Improper restriction of operations within the bounds of a memory buffer	Citrix Multiple	—	— —	—	
CVE-2022-20705 <small>New</small> Out-of-bounds write	Cisco Multiple	—	— —	— —	
CVE-2023-2163 <small>New</small> Incorrect calculation	Linux Kernel Organization Linux Kernel	—	— —	— — —	
CVE-2022-22957 <small>New</small> Deserialization of untrusted data	VMware Multiple	—	— —	— —	
CVE-2025-25256 <small>New</small> OS command injection	Fortinet FortiSIEM	—	— —	— —	
CVE-2022-22956 <small>New</small> Improper authorization	VMware Multiple	—	— —	— —	
CVE-2023-32629 <small>New</small> Incorrect authorization	Canonical Ubuntu Linux	—	— —	— —	
CVE-2025-48384 <small>New</small> Improper link resolution before file access	Git Git	—	— —	—	
CVE-2024-8068 <small>New</small> Improper privilege management	Citrix Session Recording	—	— —	—	
CVE-2024-8069 <small>New</small> Deserialization of untrusted data	Citrix Session Recording	—	— —	—	
CVE-2025-43300 <small>New</small> Out-of-bounds write	Apple Inc. Multiple	—	— —	— —	
CVE-2023-50919 Improper authentication	GL.iNet Multiple	—	— —	— —	

CVE-2023-50445 OS command injection	GL.iNet Multiple		 	 	  
CVE-2020-28188 OS command injection	TerraMaster TerraMaster OS		 	 	  
CVE-2015-5122 Use after free	Adobe Multiple		 	 	  
CVE-2020-35665 OS command injection	TerraMaster TerraMaster OS		 	 	  
CVE-2025-47165 Use after free	Microsoft Excel		 	 	 
CVE-2025-8875 Deserialization of untrusted data	N-able N-central		 		
CVE-2024-23615 Buffer overflow	Broadcom Symantec Messaging Gateway		 	  	
CVE-2025-23320 Information disclosure	NVIDIA Triton Inference Server		 	 	
CVE-2025-47170 Use after free	Microsoft Word		 	 	 
CVE-2025-54135 Prompt injection	Cursor Cursor		 	 	
CVE-2025-23319 Out-of-bounds write	NVIDIA Triton Inference Server		 	 	
CVE-2025-8876 Improper input validation	N-able N-central		 		
CVE-2025-23334 Out-of-bounds read	NVIDIA Triton Inference Server		 	 	

PATCH / UPDATE STATUS	INTEREST LEVEL	LOCATION OF ACTIVITY OR DISCUSSION	EXPLOIT STATUS
 UNAVAILABLE	 EXPLOIT SOUGHT IN UNDERGROUND	 PRIVATE COMMUNICATIONS	 CODE AVAILABLE
 SOME AVAILABLE	 RESEARCHED PUBLICLY	 UNDERGROUND	 WEAPONIZED
 AVAILABLE	 DISCLOSED PUBLICLY	 OPEN SOURCE	 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.