PERISCOPE

July 5, 2022

INTEL471

TLP: AMBER

CVE WEAPONIZATION REPORT

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

CVE	Type	Report Status	Intel 471 Risk Level*	Patch/Update Status	Interest Level	Location(s) of Activity or Discussion	Exploit Status
CVE-2022-29499	**Improper input validation**	**New**	**High**	🟡	🟢🟡	🟢🟡	🐞🚀
CVE-2022-26937	**RCE**	**New**	**Medium**	🟢	🟢🟡	🟢🟡	🐞
CVE-2022-30075	**RCE**	**New**	**Medium**	🔴	🟢🟡	🟢🟡	🐞🚀
CVE-2022-31626	**Buffer overflow**	**New**	**Low**	🟢	🟢🟡	🟢🟡	🐞
CVE-2022-32969	**Unspecified**	**New**	**Low**	🟢	🟢🟡	🟢🟡	🟢
CVE-2022-0995	Out-of-bounds write	Existing	**High**	🟢	🟢🟡	🟢🟡🔴	🐞🚀🛒
CVE-2007-4377	Stack-based buffer overflow	Existing	Medium	🟢	🟢🟡	🟢🟡🔴	🐞🚀
CVE-2017-14079	Unrestricted file upload	Existing	Medium	🟢	🟢🟡	🟢🟡🔴	🚀
CVE-2019-1003029	Unspecified	Existing	Medium	🟢	🟢🟡	🟢	🚀
CVE-2020-0638	Privilege escalation	Existing	Medium	🟢	🟢🟡	🟢🟡	🚀
CVE-2021-35578	Unspecified	Existing	Medium	🟢	🟢🟡	🟢🟡	🚀
CVE-2021-39793	Out-of-bounds write	Existing	Medium	🟢	🟢🟡	🟢	🚀
CVE-2022-26501	Incorrect authorization	Existing	Medium	🟢	🟢🟡	🟢🟡🔴	🚀
CVE-2022-27511	Improper access control	Existing	Medium	🟢	🟢🟡	🟢🟡	🟢
CVE-2022-27512	Improper control of a resource through its lifetime	Existing	Medium	🟢	🟢🟡	🟢🟡	🟢

* 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.

🟢 Available	🟢 Disclosed publicly	🟢 Open source	🟢 Not observed
🟡 Some available	🟡 Researched publicly	🟡 Underground	🐞 Code available
🔴 Unavailable	🔴 Exploit sought in underground	🔴 Private communications	🚀 Weaponized
			🛒 Producticized

Details

CVE-2022-29499	Status: New	CVSSv3: 9.8	Risk Level: High
	Type: Improper input validation	PoC: Observed	Underground: Observed

CVE summary

CVE-2022-29499 is an improper input validation vulnerability impacting Mitel MiVoice Connect versions 19.2 SP3 and earlier and R14.x and earlier. A proof of concept (PoC) was observed in open source and a link to a PoC was shared in the underground. Security researchers at the Cybersecurity and Infrastructure Security Agency (CISA) claimed the vulnerability was actively exploited in the wild. Additionally, open source reports claimed the vulnerability was allegedly used in suspected ransomware deployment operations.

Underground activity

Intel 471 has not observed weaponization or productization of CVE-2022-29499 in the underground. The actor **Nowheretogo** shared a link to PoC information from open-source reporting.

Countermeasures

Mitel released a remediation script for Mitel MiVoice Connect versions 19.2 SP3 and earlier and R14.x and earlier, which mitigate the possibility of exploitation. Further, Mitel claimed remediation will be included in MiVoice Connect version R19.3, forecast for June 2022.

CVE-2022-26937	Status: New	CVSSv3: 9.8	Risk Level: Medium
	Type: RCE	PoC: Observed	Underground: Observed

CVE summary

CVE-2022-26937 is a remote code execution (RCE) vulnerability impacting multiple versions of Microsoft Windows Server. A proof of concept (PoC) was observed in open source and subsequently shared in the underground.

Underground activity

Intel 471 has not observed weaponization or productization of CVE-2022-26937 in the underground. The actor **shrinbaba** shared information and the actor **0xA00** shared a link to PoC from open-source reporting.

Countermeasures

Microsoft addressed the vulnerability in a security advisory with a patch. Additionally, Microsoft also provided a workaround that can be implemented to mitigate the possibility of exploitation.

CVE-2022-30075	Status: New	CVSSv3: 8.8	Risk Level: Medium
	Type: RCE	PoC: Observed	Underground: Observed

CVE summary

CVE-2022-30075 is a remote code execution (RCE) vulnerability impacting TP-Link Archer AX50 firmware versions 210730 and earlier. An exploit was observed in open source and subsequently shared in the underground.

Underground activity

CVE-2022-30075 was weaponized. The actor **danieko** posted an exploit and the actor **syykuno** posted a link to an exploit for CVE-2022-30075 from open source.

Countermeasures

The impacted vendor has not released patching or mitigation information for impacted products or corresponding versions.

CVE-2022-31626	Status: New	CVSSv3: 8.8	Risk Level: Low
	Type: Buffer overflow	PoC: Observed	Underground: Observed

CVE summary

CVE-2022-31626 is a buffer overflow vulnerability impacting PHP versions 7.4.0 through 7.4.29, 8.0.0 through 8.0.19 and 8.1.0 through 8.1.6. A proof of concept (PoC) was observed in open source and subsequently shared in the underground.

Underground activity

Intel 471 has not observed weaponization or productization of CVE-2022-31626 in the underground. The actor **crlf** shared PoC information from open-source reporting.

Countermeasures

The PHP Group addressed the vulnerability in PHP versions 7.4.30, 8.0.20, and 8.1.7.

CVE-2022-32969	Status: New	CVSS: NA	Risk Level: Low
	Type: Unspecified	PoC: Not Observed	Underground: Observed

CVE summary

CVE-2022-32969 is an unspecified vulnerability impacting MetaMask versions 10.11.2 and earlier. A proof of concept (PoC) was not observed publicly or in the underground.

Underground activity

Intel 471 has not observed weaponization or productization of CVE-2022-32969 in the underground. Several actors shared information from open-source reporting.

Countermeasures

MetaMask addressed the vulnerability in MetaMask version 10.11.3.

CVE-2022-0995	Status: Existing	CVSSv3: 7.1	Risk Level: High
	Type: Out-of-bounds write	PoC: Observed	Underground: Observed

CVE summary

CVE-2022-0995 is an out-of-bounds write vulnerability impacting Linux Kernel versions 5.16 through 5.17. A Metasploit module was observed in open source and a link to an exploit was shared in the underground.

Underground activity

CVE-2022-0995 was weaponized. The actor **adhuc** posted a link to an exploit for CVE-2022-0995 from open source. Additionally, the actor **LORD1** advertised an exploitation toolkit on the Exploit forum that leveraged CVE-2022-0995 and offered to work through an escrow.

Countermeasures

Linux Kernel Organization addressed the vulnerability in a software development platform saved commit change with a patch.

CVE-2007-4377	Status: Existing	CVSSv2: 6	Risk Level: Medium
	Type: Stack-based buffer overflow	PoC: Observed	Underground: Observed

CVE summary

CVE-2007-4377 is a stack-based buffer overflow vulnerability impacting NetWin SurgeMail 38k. An exploit was observed in open source. Additionally, an exploitation toolkit was advertised in the underground.

Underground activity

CVE-2007-4377 was likely weaponized. The actor **LORD1** advertised an exploitation toolkit on the Exploit forum that leveraged CVE-2007-4377 and offered to work through an escrow.

Countermeasures

NetWin addressed the vulnerability in a security advisory with an updated version.

CVE-2017-14079	Status: Existing	CVSSv3: 8.8	Risk Level: Medium
	Type: Unrestricted file upload	PoC: Not Observed	Underground: Observed

CVE summary

CVE-2017-14079 is an unrestricted file upload vulnerability impacting Trend Micro Mobile Security versions 9.7 and earlier. A proof of concept (PoC) was not observed publicly or in the underground. However, an exploitation toolkit was advertised in the underground.

Underground activity

CVE-2017-14079 was likely weaponized. The actor **LORD1** advertised an exploitation toolkit on the Exploit forum that leveraged CVE-2017-14079 and offered to work through an escrow.

Countermeasures

Trend Micro addressed the vulnerability in a security advisory with updated versions.

CVE-2019-1003029	Status: Existing	CVSSv3: 9.9	Risk Level: Medium
	Type: Unspecified	PoC: Not Observed	Underground: Not Observed

CVE summary

CVE-2019-1003029 is an unspecified vulnerability impacting Jenkins Script Security Plugin versions 1.53 and earlier. A proof of concept (PoC) was not observed publicly or in the underground. Additionally, security researchers at the Cybersecurity and Infrastructure Security Agency (CISA) claimed the vulnerability was actively exploited in the wild.

Underground activity

Intel 471 has not observed weaponization or productization of CVE-2019-1003029 in the underground.

Countermeasures

Jenkins addressed the vulnerability in a security advisory with updated versions.

CVE-2020-0638	Status: Existing	CVSSv3: 7.8	Risk Level: Medium
	Type: Privilege escalation	PoC: Not Observed	Underground: Observed

CVE summary

CVE-2020-0638 is a privilege escalation vulnerability impacting multiple products and versions of Microsoft Windows. A proof of concept (PoC) was not observed publicly or in the underground. Additionally, security researchers at the Cybersecurity and Infrastructure Security Agency (CISA) claimed the vulnerability was actively exploited in the wild.

Underground activity

Intel 471 has not observed weaponization or productization of CVE-2020-0638 in the underground. The actor **Zer0must2b** shared information from open-source reporting.

Countermeasures

Microsoft addressed the vulnerability in a security advisory with a patch.

CVE-2021-35578	Status: Existing	CVSSv3: 5.3	Risk Level: Medium
	Type: Unspecified	PoC: Not Observed	Underground: Observed

CVE summary

CVE-2021-35578 is an unspecified vulnerability impacting Oracle GraalVM Enterprise Edition versions 20.3.3 and 21.2.0, Oracle Openjdk versions 8, 11.0.12, and 17. A proof of concept (PoC) was not observed publicly or in the underground. However, an exploitation toolkit was advertised in the underground.

Underground activity

CVE-2021-35578 was likely weaponized. The actor **LORD1** advertised an exploitation toolkit on the Exploit forum that leveraged CVE-2021-35578 and offered to work through an escrow.

Countermeasures

Oracle addressed the vulnerability in a security advisory with updated versions.

CVE-2021-39793	Status: Existing	CVSSv3: 7.8	Risk Level: Medium
	Type: Out-of-bounds write	PoC: Not Observed	Underground: Not Observed

CVE summary

CVE-2021-39793 is an out-of-bounds write vulnerability impacting multiple products and versions of Google Pixel devices. A proof of concept (PoC) was not observed publicly or in the underground. Additionally, security researchers at the Cybersecurity and Infrastructure Security Agency (CISA) claimed the vulnerability was actively exploited in the wild.

Underground activity

Intel 471 has not observed weaponization or productization of CVE-2021-39793 in the underground.

Countermeasures

Google addressed the vulnerability in a Pixel update bulletin with a patch.

CVE-2022-26501	Status: Existing	CVSSv3: 9.8	Risk Level: Medium
	Type: Incorrect authorization	PoC: Not Observed	Underground: Observed

CVE summary

CVE-2022-26501 is an incorrect authorization vulnerability impacting Veeam Backup & Replication versions 10.0.0.4442 before 10.0.1.4854 and 11.0.0.825 before 11.0.1.1261. A proof of concept (PoC) was not observed publicly or in the underground. However, an exploitation toolkit was advertised in the underground.

Underground activity

CVE-2022-26501 was likely weaponized. The actor **LORD1** advertised an exploitation toolkit on the Exploit forum that leveraged CVE-2022-26501 and offered to work through an escrow.

Countermeasures

Veeam addressed the vulnerability in a security advisory with updated versions.

CVE-2022-27511	Status: Existing	CVSSv3: 8.1	Risk Level: Medium
	Type: Improper access control	PoC: Not Observed	Underground: Observed

CVE summary

CVE-2022-27511 is an improper access control vulnerability impacting Citrix Application Delivery Management (ADM) versions 13.0 before 13.0-85.19 and 13.1 before 13.1-21.53. A proof of concept (PoC) was not observed publicly or in the underground.

Underground activity

Intel 471 has not observed weaponization or productization of CVE-2022-27511 in the underground. The actor **WWW** shared information from open-source reporting.

Countermeasures

Citrix Systems addressed the vulnerability in a security advisory with updated versions.

CVE-2022-27512	Status: Existing	CVSSv3: 5.3	Risk Level: Medium
	Type: Improper control of a resource through its lifetime	PoC: Not Observed	Underground: Observed

CVE summary

CVE-2022-27512 is an improper control of a resource through its lifetime vulnerability impacting Citrix Application Delivery Management (ADM) versions 13.0 before 13.0-85.19 and 13.1 before 13.1-21.53. A proof of concept (PoC) was not observed publicly or in the underground.

Underground activity

Intel 471 has not observed weaponization or productization of CVE-2022-27512 in the underground. The actor **WWW** shared information from open-source reporting.

Countermeasures

Citrix Systems addressed the vulnerability in a security advisory with updated versions.

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. You will receive a snapshot of the weekly report once every four to six weeks.

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.