PERISCOPE

March 1, 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-2020-27937	**Unspecified**	**New**	**Medium**	🟢	🟢🟡	🟢	🚀
CVE-2021-30970	**Unspecified**	**New**	**Medium**	🟢	🟢🟡	🟢	🚀
CVE-2022-23131	**Authentication bypass**	**New**	**Medium**	🟢	🟢🟡	🟢🟡	🐞🚀
CVE-2022-24087	**Improper input validation**	**New**	**Medium**	🟢	🟢🟡	🟢🟡	🟢
CVE-2021-44142	**Out-of-bounds write**	**New**	**Low**	🟢	🟢🟡	🟢🟡	🟢
CVE-2022-0609	Use after free	Existing	**High**	🟢	🟢🟡	🟢🟡	🚀
CVE-2022-22536	HTTP request smuggling	Existing	**High**	🟢	🟢🟡	🟢🟡	🐞
CVE-2022-24086	Improper input validation	Existing	**High**	🟢	🟢🟡🔴	🟢🟡	🚀
CVE-2022-21999	Privilege escalation	Existing	Medium	🟢	🟢🟡	🟢🟡	🐞🚀
CVE-2022-22532	HTTP request smuggling	Existing	Medium	🟢	🟢🟡	🟢	🟢
CVE-2022-22533	Unspecified	Existing	Medium	🟢	🟢🟡	🟢	🟢
CVE-2022-22620	Use after free	Existing	Medium	🟢	🟢🟡	🟢🟡	🚀

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

* 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.

Details

CVE-2020-27937	Status: New	CVSSv3: 5.5	Risk Level: Medium
	Type: Unspecified	PoC: Not Observed	Underground: Not Observed

CVE summary

CVE-2020-27937 is an unspecified vulnerability impacting Apple macOS Big Sur version 11.0 and Apple macOS Big Sur versions 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave. A proof of concept (PoC) was not observed publicly or in the underground. A security researcher reported the vulnerability was exploited in the wild in conjunction with CVE-2022-0609 to achieve elevated privileges on the host. If executed correctly this exploit chain would allow an attacker to remotely execute arbitrary code on the vulnerable system with root level privileges.

Underground activity

Intel 471 has not observed weaponization or productization of CVE-2020-27937 in the underground.

Countermeasures

Apple addressed the vulnerability in multiple security advisories with updated versions.

CVE-2021-30970	Status: New	CVSSv3: 5.5	Risk Level: Medium
	Type: Unspecified	PoC: Not Observed	Underground: Not Observed

CVE summary

CVE-2021-30970 is an unspecified vulnerability impacting Apple Monterey versions 12.0.1 and earlier and Apple macOS Big Sur 11.6.1 and earlier. A proof of concept (PoC) was not observed publicly or in the underground. A security researcher reported the vulnerability was exploited in the wild in conjunction with CVE-2022-0609 to achieve elevated privileges on the host. If executed correctly this exploit chain would allow an attacker to remotely execute arbitrary code on the vulnerable system with root level privileges.

Underground activity

Intel 471 has not observed weaponization or productization of CVE-2021-30970 in the underground.

Countermeasures

Apple addressed the vulnerability in multiple security advisories with updated versions.

CVE-2022-23131	Status: New	CVSSv3: 9.8	Risk Level: Medium
	Type: Authentication bypass	PoC: Observed	Underground: Observed

CVE summary

CVE-2022-23131 is an authentication bypass vulnerability impacting Zabbix versions 5.4.7 and earlier. An exploit was observed in open source and a link to an exploit was shared in the underground. Additionally, a walk through demo of an exploit was shared via YouTube.

Underground activity

CVE-2022-23131 was weaponized. The actor **Trikster** posted a link to an exploit for CVE-2022-23131 from open source.

Countermeasures

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

CVE-2022-24087	Status: New	CVSSv3: 9.8	Risk Level: Medium
	Type: Improper input validation	PoC: Not Observed	Underground: Not Observed

CVE summary

CVE-2022-24087 is an improper input validation vulnerability impacting Adobe Commerce and Magento Open Source versions 2.3.7 p2 and earlier and Adobe Commerce and Magento Open Source versions 2.4.3 p1 and earlier. A proof of concept (PoC) was not observed publicly or in the underground. This vulnerability exists because of an incomplete fix for CVE-2022-24086.

Underground activity

Intel 471 has not observed weaponization or productization of CVE-2022-24087 in the underground.

Countermeasures

Adobe addressed the vulnerability in a security bulletin with updated versions.

CVE-2021-44142	Status: New	CVSSv3: 9.9	Risk Level: Low
	Type: Out-of-bounds write	PoC: Not Observed	Underground: Observed

CVE summary

CVE-2021-44142 is an out-of-bounds write vulnerability impacting Samba versions 4.13.16 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-2021-44142 in the underground. The actor **EthicX** sought a working PoC for CVE-2021-44142 on the XSS forum. Additionally, several actors shared information from open-source reporting.

Countermeasures

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

CVE-2022-0609	Status: Existing	CVSS: NA	Risk Level: High
	Type: Use after free	PoC: Not Observed	Underground: Observed

CVE summary

CVE-2022-0609 is a use after free vulnerability impacting Google Chrome versions 98.0.4758.80 and earlier. A proof of concept (PoC) was not observed publicly or in the underground. Google claimed to be aware of the vulnerability being actively exploited in the wild. A security researcher reported the vulnerability was exploited in the wild in conjunction with CVE-2021-30970 and CVE-2020-27937 to achieve elevated privileges on the host. If executed correctly this exploit chain would allow an attacker to remotely execute arbitrary code on the vulnerable system with root level privileges.

Underground activity

Intel 471 has not observed weaponization or productization of CVE-2022-0609 in the underground. Several actors shared information from open-source reporting.

Countermeasures

Google addressed the vulnerability in a stable channel update by releasing Chrome version 98.0.4758.102.

CVE-2022-22536	Status: Existing	CVSSv3: 10	Risk Level: High
	Type: HTTP request smuggling	PoC: Observed	Underground: Observed

CVE summary

CVE-2022-22536 is an HTTP request smuggling vulnerability impacting multiple versions of SAP NetWeaver, SAP Content Server and SAP Web Dispatcher. A proof of concept (PoC) was observed in open source and a link to a PoC was shared in the underground. Successful exploitation of this vulnerability would allow an attacker to remotely execute arbitrary code on a vulnerable host and fully compromise any unpatched SAP applications. Security researchers at Onapsis released a Python script which can be used to detect CVE-2022-22536.

Underground activity

Intel 471 has not observed weaponization or productization of CVE-2022-22536 in the underground. The actor **shrinbaba** shared a link to PoC information from open-source reporting.

Countermeasures

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

CVE-2022-24086	Status: Existing	CVSSv3: 9.8	Risk Level: High
	Type: Improper input validation	PoC: Not Observed	Underground: Observed

CVE summary

CVE-2022-24086 is an improper input validation vulnerability impacting Adobe Commerce and Magento Open Source versions 2.3.7 p2 and earlier and Adobe Commerce and Magento Open Source versions 2.4.3 p1 and earlier. A proof of concept (PoC) was not observed publicly or in the underground. Adobe claimed to be aware of the vulnerability being actively exploited in the wild.

Underground activity

Intel 471 has not observed weaponization or productization of CVE-2022-24086 in the underground. The actor **g3tty** sought technical details or an example of how to exploit CVE-2022-24086. Additionally, several actors shared information from open-source reporting.

Countermeasures

Adobe addressed the vulnerability in a security bulletin with updated versions. When it was reported that the patch released on February 13, 2022 was ineffective, Adobe issued another security update to address an improper input validation vulnerability tracked as CVE-2022-24087.

CVE-2022-21999	Status: Existing	CVSSv3: 7.8	Risk Level: Medium
	Type: Privilege escalation	PoC: Observed	Underground: Observed

CVE summary

CVE-2022-21999 is a privilege escalation vulnerability impacting multiple products and versions of Microsoft Windows. An exploit was observed in open source and a link to an exploit was shared in the underground.

Underground activity

CVE-2022-21999 was weaponized. Several actors posted a link to an exploit for CVE-2022-21999 from open source.

Countermeasures

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

CVE-2022-22532	Status: Existing	CVSSv3: 8.1	Risk Level: Medium
	Type: HTTP request smuggling	PoC: Not Observed	Underground: Not Observed

CVE summary

CVE-2022-22532 is a HTTP request smuggling vulnerability impacting multiple versions of SAP NetWeaver Application Server Java. 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-2022-22532 in the underground.

Countermeasures

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

CVE-2022-22533	Status: Existing	CVSS: NA	Risk Level: Medium
	Type: Unspecified	PoC: Not Observed	Underground: Not Observed

CVE summary

CVE-2022-22533 is an unspecified vulnerability impacting multiple versions of SAP NetWeaver Application Server Java. 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-2022-22533 in the underground.

Countermeasures

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

CVE-2022-22620	Status: Existing	CVSS: NA	Risk Level: Medium
	Type: Use after free	PoC: Not Observed	Underground: Observed

CVE summary

CVE-2022-22620 is a use after free vulnerability impacting Apple macOS Monterey versions 12.2 and earlier, Apple iOS versions 15.3 and iPadOS 15.3 and earlier, and Apple Safari versions 15.3 and earlier. A proof of concept (PoC) was not observed publicly or in the underground. Apple claimed to be aware of the vulnerability being actively exploited in the wild.

Underground activity

Intel 471 has not observed weaponization or productization of CVE-2022-22620 in the underground. The actor **el_cesar** and **AXCESS** shared information from open-source reporting.

Countermeasures

Apple addressed the vulnerability in multiple security advisories 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.