PERISCOPE

May 3, 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-2018-0798	**Out-of-bounds write**	**New**	**High**				
CVE-2022-29464	**Unrestricted file upload**	**New**	**High**				
CVE-2020-9374	**OS command injection**	**New**	**Medium**				
CVE-2020-9529	**Unspecified**	**New**	**Medium**				
CVE-2022-21449	**Unspecified**	**New**	**Medium**				
CVE-2022-23176	**Improper privilege management**	**New**	**Medium**				
CVE-2022-0706	**XSS**	**New**	**Low**				
CVE-2022-0543	Unspecified	Existing	**High**				
CVE-2022-1364	Type confusion	Existing	**High**				
CVE-2017-12542	Unspecified	Existing	Medium				
CVE-2018-6882	XSS	Existing	Medium				
CVE-2022-21919	Privilege escalation	Existing	Medium				
CVE-2022-22718	Privilege escalation	Existing	Medium				
CVE-2022-22960	Privilege escalation	Existing	Medium				
CVE-2021-39173	Unspecified	Existing	Low				

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

Available · Disclosed publicly · Open source · Not observed

• Mitigation status. • Exploit status. • Underground activity. • CVSSv3 score.	Some available Unavailable	Researched publicly Exploit sought in underground	Underground Private communications	Code available Weaponized Productized

Details

CVE-2018-0798	Status: New	CVSSv3: 8.8	Risk Level: High
	Type: Out-of-bounds write	PoC: Not Observed	Underground: Observed

CVE summary

CVE-2018-0798 is an out-of-bounds write vulnerability impacting Microsoft Office 2007, Microsoft Office 2010, Microsoft Office 2013, and Microsoft Office 2016. A proof of concept (PoC) was not observed publicly. However, an exploitation toolkit was advertised in the underground.

Underground activity

CVE-2018-0798 was likely weaponized and productized. Intel 471 observed the actor **Trillium** advertised an exploitation toolkit dubbed "multisploit tool" that leveraged CVE-2018-0798 and multiple actors have shown interest in acquiring the tool. Additionally, several actors advertised an exploit builder on various forums.

Countermeasures

Microsoft addressed the vulnerability by removing Equation Editor functionality.

CVE-2022-29464	Status: New	CVSSv3: 9.8	Risk Level: High
	Type: Unrestricted file upload	PoC: Observed	Underground: Observed

CVE summary

CVE-2022-29464 is an unrestricted file upload vulnerability impacting multiple versions of WSO2 API Manager, WSO2 Identity Server, WSO2 Identity Server Analytics, WSO2 Identity Server as Key Manager, and WSO2 Enterprise Integrator. An exploit was observed in open source and a link to an exploit was shared in the underground. Additionally, security researchers claimed threat actors were actively scanning endpoints vulnerable to CVE-2022-29464 and there were attempts to exploit this vulnerability in the wild.

Underground activity

CVE-2022-29464 was weaponized. The actor **MassiveAttack** posted a link to an exploit for CVE-2022-29464 from open source.

Countermeasures

WSO2 addressed the vulnerability in a security advisory with updated versions.

CVE-2020-9374	Status: New	CVSSv3: 9.8	Risk Level: Medium
	Type: OS command injection	PoC: Observed	Underground: Observed

CVE summary

CVE-2020-9374 is an OS command injection vulnerability impacting TP-Link TL-WR849N Firmware version 0.9.1 4.16. An exploit was observed in open source and subsequently shared in the underground.

Underground activity

CVE-2020-9374 was weaponized. The actors **THROOT** and **][ak** posted an exploit for CVE-2020-9374 from open source.

Countermeasures

TP-Link addressed the vulnerability in a security advisory with updated versions.

CVE-2020-9529	Status: New	CVSSv3: 9.8	Risk Level: Medium
	Type: Unspecified	PoC: Observed	Underground: Observed

CVE summary

CVE-2020-9529 is an unspecified vulnerability impacting multiple versions of Shenzhen Hichip Vision Technology Firmware. An exploit was observed in open source and a link to an exploit was shared in the underground.

Underground activity

CVE-2020-9529 was weaponized. The actor **shatter** posted a link to an exploit for CVE-2020-9529 from open source.

Countermeasures

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

CVE-2022-21449	Status: New	CVSSv3: 7.8	Risk Level: Medium
	Type: Unspecified	PoC: Observed	Underground: Observed

CVE summary

CVE-2022-21449 is an unspecified vulnerability impacting multiple versions of Oracle Java SE and Oracle GraalVM Enterprise Edition. A proof of concept (PoC) was observed in open source and a link to a PoC was shared in the underground. Additionally, a tool that identifies JAR/WAR archives vulnerable to CVE-2022-21449 was observed in open source.

Underground activity

Intel 471 has not observed weaponization or productization of CVE-2022-21449 in the underground. Several actors shared a link to PoC information from open-source reporting.

Countermeasures

Oracle addressed the vulnerability in a critical patch update advisory with updated versions.

CVE-2022-23176	Status: New	CVSSv3: 8.8	Risk Level: Medium
	Type: Improper privilege management	PoC: Not Observed	Underground: Observed

CVE summary

CVE-2022-23176 is an improper privilege management vulnerability impacting multiple versions of WatchGuard Fireware OS. 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-2022-23176 in the underground. Several actors shared information from open-source reporting.

Countermeasures

WatchGuard Technologies addressed the vulnerability in a security advisory with updated versions.

CVE-2022-0706	Status: New	CVSSv3: 4.8	Risk Level: Low
	Type: XSS	PoC: Observed	Underground: Observed

CVE summary

CVE-2022-0706 is a cross-site scripting (XSS) vulnerability impacting Easy Digital Downloads WordPress plugin versions 2.11.5 and earlier. A proof of concept (PoC) was observed in open source and a link to a PoC was shared in the underground.

Underground activity

Intel 471 has not observed weaponization or productization of CVE-2022-0706 in the underground. The actor **EX** shared a link to PoC information from open-source reporting.

Countermeasures

Sandhills Development addressed the vulnerability in an Easy Digital Downloads version 2.11.6.

CVE-2022-0543	Status: Existing	CVSSv3: 10	Risk Level: High
	Type: Unspecified	PoC: Observed	Underground: Observed

CVE summary

CVE-2022-0543 is an unspecified vulnerability impacting Redis running on Debian-based distros due to a packaging issue. An exploit was observed in open source. 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-2022-0543 in the underground. Several actors shared information from open-source reporting.

Countermeasures

The vendors running Redis on their distribution addressed the vulnerability in security advisories with a patch.

CVE-2022-1364	Status: Existing	CVSS: NA	Risk Level: High
	Type: Type confusion	PoC: Not Observed	Underground: Observed

CVE summary

CVE-2022-1364 is a type confusion vulnerability impacting Google Chrome versions 100.0.4896.88 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.

Underground activity

Intel 471 has not observed weaponization or productization of CVE-2022-1364 in the underground. The actors **EvZen** and **WWW** shared information from open-source reporting.

Countermeasures

Google addressed the vulnerability in a stable channel update by releasing Chrome version 100.0.4896.127.

CVE-2017-12542	Status: Existing	CVSSv3: 10	Risk Level: Medium
	Type: Unspecified	PoC: Observed	Underground: Observed

CVE summary

CVE-2017-12542 is an unspecified vulnerability impacting multiple versions of HPE Integrated Lights-out (iLO 4), Moonshot, and NonStop Systems. An exploit was observed in open source and a link to an exploit was shared in the underground.

Underground activity

CVE-2017-12542 was weaponized. Several actors posted a link to an exploit for CVE-2017-12542 from open source. Additionally, the actor **Desconocido** sought an exploit for CVE-2017-12542 on the XSS forum.

Countermeasures

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

CVE-2018-6882	Status: Existing	CVSSv3: 6.1	Risk Level: Medium
	Type: XSS	PoC: Observed	Underground: Observed

CVE summary

CVE-2018-6882 is a cross-site scripting (XSS) vulnerability impacting Synacor Zimbra Collaboration Suite (ZCS) versions 8.7 through 8.8.6. A proof of concept (PoC) was observed in open source. Additionally, security researchers at Computer Emergency Response Team for Ukraine (CERT-UA) claimed the vulnerability was used to target Ukrainian government organizations.

Underground activity

Intel 471 has not observed weaponization or productization of CVE-2018-6882 in the underground. The actors **GG44bb** and **WWW** shared information from open-source reporting.

Countermeasures

Synacor addressed the vulnerability in Zimbra Collaboration Suite (ZCS) version 8.8.7.

CVE-2022-21919	Status: Existing	CVSSv3: 7	Risk Level: Medium
	Type: Privilege escalation	PoC: Not Observed	Underground: Observed

CVE summary

CVE-2022-21919 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. This vulnerability exists because of an incomplete fix for CVE-2021-34484.

Underground activity

Intel 471 has not observed weaponization or productization of CVE-2022-21919 in the underground. The actors **Soules** and **AXCESS** shared information from open-source reporting.

Countermeasures

On January 11, 2022, Microsoft released a security advisory which reportedly addressed this vulnerability. However, according to security researchers these security updates were incomplete and CVE-2022-21919 can be exploited with a patch bypass.

CVE-2022-22718	Status: Existing	CVSSv3: 7.8	Risk Level: Medium
	Type: Privilege escalation	PoC: Not Observed	Underground: Observed

CVE summary

CVE-2022-22718 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. 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-2022-22718 in the underground. Several actors shared information from open-source reporting.

Countermeasures

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

CVE-2022-22960	Status: Existing	CVSSv3: 7.8	Risk Level: Medium
	Type: Privilege escalation	PoC: Not Observed	Underground: Not Observed

CVE summary

CVE-2022-22960 is a privilege escalation vulnerability impacting multiple versions of VMware Workspace ONE Access, VMware Identity Manager and VMware vRealize Automation. A proof of concept (PoC) was not observed publicly or in the underground.

Additionally, VMware and security researchers at the Cybersecurity and Infrastructure Security Agency (CISA) claimed the vulnerability was actively exploited in the wild.

Underground activity

Intel 471 did not observe weaponization or productization of CVE-2022-22960 in the underground.

Countermeasures

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

CVE-2021-39173	Status: Existing	CVSSv3: 8.8	Risk Level: Low
	Type: Unspecified	PoC: Not Observed	Underground: Observed

CVE summary

CVE-2021-39173 is an unspecified vulnerability impacting CachetHQ Cachet versions 2.5.0 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-2021-39173 in the underground. The actor **___user___** sought help with exploiting CVE-2021-39173 on the Breached forum.

Countermeasures

The vulnerability was addressed in a CachetHQ Cachet version 2.5.1.

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.