PERISCOPE

April 4, 2023

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-2013-2551	**Use after free**	**New**	**High**	●	●●●	●●	🐞🚀🛒
CVE-2014-6332	**Improper restriction of operations within the bounds of a memory buffer**	**New**	**High**	●	●●	●●	🐞🚀🛒
CVE-2023-27532	**Unspecified**	**New**	**High**	●	●●	●●	🐞🚀
CVE-2023-20963	**Privilege escalation**	**New**	**Medium**	●	●●	●	🚀
CVE-2023-23415	**RCE**	**New**	**Medium**	●	●●	●●	🚀
CVE-2014-8361	OS command injection	Existing	High	●	●●	●●	🐞🚀🛒
CVE-2022-28353	XSS	Existing	Low	●	●●	●●	🐞
CVE-2022-28354	XSS	Existing	Low	●	●●	●●	🐞
CVE-2023-20078	Command Injection	Existing	Low	●	●●	●	●
CVE-2023-20079	Denial of Service	Existing	Low	●	●●	●	●
CVE-2023-23396	Unspecified	Existing	Low	●	●●	●●	🐞
CVE-2023-24033	Memory corruption	Existing	Low	●	●●	●●	●
CVE-2023-26496	Memory corruption	Existing	Low	●	●●	●	●
CVE-2023-26497	Memory corruption	Existing	Low	●	●●	●	●
CVE-2023-26498	Memory corruption	Existing	Low	●	●●	●	●

* 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
			Productized

Details

CVE-2013-2551	Status: New	CVSSv2: 9.3	Risk Level: High
	Type: Use after free	PoC: Observed	Underground: Observed

CVE summary

CVE-2013-2551 is a use after free vulnerability impacting Microsoft Internet Explorer versions 6 through 10. A Metasploit module was observed in open source and subsequently shared in the underground. Security researchers at the Cybersecurity and Infrastructure Security Agency (CISA) claimed the vulnerability was actively exploited in the wild. Additionally, CVE-2013-2551 was likely exploited by RIG Exploit Kit to spread a variety of malware.

Underground activity

CVE-2013-2551 was weaponized and productized. Several actors posted a Metasploit module for CVE-2013-2551 from open source. The actor **jlegend** sought an exploit for CVE-2013-2551 on the Exploit forum. Additionally, the actor **TakeThat** claim the vulnerability was added to the RIG exploit kit.

Countermeasures

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

CVE-2014-6332	Status: New	CVSSv2: 9.3	Risk Level: High
	Type: Improper restriction of operations within the bounds of a memory buffer	PoC: Observed	Underground: Observed

CVE summary

CVE-2014-6332 is an improper restriction of operations within the bounds of a memory buffer vulnerability impacting multiple products and versions of Microsoft Windows. A Metasploit module was observed in open source and subsequently shared in the underground. Security researchers at the Cybersecurity and Infrastructure Security Agency (CISA) claimed the vulnerability was actively exploited in the wild. Additionally, CVE-2014-6332 was likely exploited by RIG Exploit Kit to spread a variety of malware.

Underground activity

CVE-2014-6332 was weaponized and productized. Several actors posted a Metasploit module for CVE-2014-6332 from open source.

Countermeasures

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

CVE-2023-27532	Status: New	CVSSv3: 7.5	Risk Level: High
	Type: Unspecified	PoC: Observed	Underground: Observed

CVE summary

CVE-2023-27532 is an unspecified vulnerability impacting multiple versions of Veeam Backup and Replication. An exploit was observed in open source and a link to an exploit was shared in the underground.

Underground activity

CVE-2023-27532 was weaponized. The actor **bo[e]ss** posted a link to an exploit for CVE-2023-27532 from open source. Additionally, the actor **WWW** shared information from open-source reporting.

Countermeasures

Veeam addressed the vulnerability in a security advisory with updated versions. Available patch resolves both unauthenticated credential dumping and RCE. As a workaround it is recommended to block external connections to port TCP 9401 in the backup server firewall until the patch is installed.

CVE-2023-20963	Status: New	CVSSv3: 7.8	Risk Level: Medium
	Type: Privilege escalation	PoC: Not Observed	Underground: Not Observed

CVE summary

CVE-2023-20963 is a privilege escalation vulnerability impacting multiple versions of Google Android operating system (OS). A proof of concept (PoC) was not observed publicly or in the underground. However, security researchers reported CVE-2023-20963 was actively exploited in the wild with the malicious versions of Pinduoduo application.

Underground activity

Intel 471 has not observed weaponization or productization of CVE-2023-20963 in the underground.

Countermeasures

Google addressed the vulnerability in security advisories with updated versions.

CVE-2023-23415	Status: New	CVSSv3: 9.8	Risk Level: Medium
	Type: RCE	PoC: Not Observed	Underground: Observed

CVE summary

CVE-2023-23415 is a remote code execution (RCE) vulnerability impacting multiple products and versions of Microsoft Windows. A proof of concept (PoC) was not observed publicly or in the underground. However, an exploit toolkit that allegedly exploits CVE-2023-23415 was advertised in the underground.

Underground activity

CVE-2023-23415 was likely weaponized. The actor **angigod** advertised an exploit toolkit that allegedly exploits CVE-2023-23415.

Countermeasures

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

CVE-2014-8361	Status: Existing	CVSSv2: 10	Risk Level: High
	Type: OS command injection	PoC: Observed	Underground: Observed

CVE summary

CVE-2014-8361 is an OS command injection vulnerability impacting multiple versions of Realtek rtl81xx SDK. A Metasploit module was observed in open source and subsequently shared in the underground. Successful exploitation can lead to unauthenticated remote code execution (RCE) with root privileges. Security researchers reported CVE-2014-8361 was exploited in the wild by the HinataBot botnet.

Underground activity

CVE-2014-8361 was weaponized and productized. The actor **Muhammad** posted a Metasploit module for CVE-2014-8361 from open source. Additionally multiple actors shared information from open-source reporting.

Countermeasures

The impacted vendor has not released patching or mitigation information for impacted products or corresponding versions. As a workaround, it is recommended to restrict who can access the device with firewall rules and whiltelisting.

CVE-2022-28353	Status: Existing	CVSSv3: 6.3	Risk Level: Low
	Type: XSS	PoC: Observed	Underground: Observed

CVE summary

CVE-2022-28353 is a cross-site scripting (XSS) vulnerability impacting MyBB External Redirect Warning plugin version 1.3.0. 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-2022-28353 in the underground. The actor **][ak** shared PoC information from open-source reporting.

Countermeasures

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

CVE-2022-28354	Status: Existing	CVSSv3: 6.3	Risk Level: Low
	Type: XSS	PoC: Observed	Underground: Observed

CVE summary

CVE-2022-28354 is a cross-site scripting (XSS) vulnerability impacting MyBB Active Threads Plugin version 1.3.0. 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-2022-28354 in the underground. The actor **][ak** shared PoC information from open-source reporting.

Countermeasures

MyBB Project addressed the vulnerability in Active Threads Plugin version 1.3.1.

CVE-2023-20078	Status: Existing	CVSSv3: 9.8	Risk Level: Low
	Type: Command Injection	PoC: Not Observed	Underground: Not Observed

CVE summary

CVE-2023-20078 is a command injection vulnerability impacting multiple versions of Cisco IP Phone series 6871, 6861, 6851, 6841, 6825, 7861, 7841, 7832, 7821, 7811, 8865, 8861, 8851, 8845, 8841, 8832, and 8811. 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-2023-20078 in the underground.

Countermeasures

Cisco addressed the vulnerability in security advisories with updated versions.

CVE-2023-20079	Status: Existing	CVSSv3: 7.5	Risk Level: Low
	Type: Denial of Service	PoC: Not Observed	Underground: Not Observed

CVE summary

CVE-2023-20079 is a denial of service (DoS) vulnerability impacting Cisco Ip Phone series 6800, 7800, and 8800. A proof of concept (PoC) was not observed publicly or in the underground. Successful exploitation can enable an attacker to reload the device remotely, resulting in DoS condition.

Underground activity

Intel 471 has not observed weaponization or productization of CVE-2023-20079 in the underground.

Countermeasures

Cisco addressed the vulnerability in security advisories with updated versions.

CVE-2023-23396	Status: Existing	CVSSv3: 5.5	Risk Level: Low
	Type: Unspecified	PoC: Observed	Underground: Observed

CVE summary

CVE-2023-23396 is an unspecified vulnerability impacting Microsoft Office Web Apps Server 2013 Service Pack 1 and Microsoft Office Online Server. A proof of concept (PoC) was observed publicly and subsequently shared in the underground.

Underground activity

Intel 471 has not observed weaponization or productization of CVE-2023-23396 in the underground. The actor **denzalgard** shared PoC information from open-source reporting.

Countermeasures

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

CVE-2023-24033	Status: Existing	CVSSv3: 8.6	Risk Level: Low
	Type: Memory corruption	PoC: Not Observed	Underground: Observed

CVE summary

CVE-2023-24033 is a memory corruption vulnerability impacting Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T512 baseband modem chipsets. 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-2023-24033 in the underground. The actor **alexzir** shared information from open-source reporting.

Countermeasures

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

CVE-2023-26496	Status: Existing	CVSSv3: 8.6	Risk Level: Low
	Type: Memory corruption	PoC: Not Observed	Underground: Not Observed

CVE summary

CVE-2023-26496 is a memory corruption vulnerability impacting Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T512 baseband modem chipsets. 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-2023-26496 in the underground.

Countermeasures

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

CVE-2023-26497	Status: Existing	CVSSv3: 8.6	Risk Level: Low
	Type: Memory corruption	PoC: Not Observed	Underground: Not Observed

CVE summary

CVE-2023-26497 is a memory corruption vulnerability impacting Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T512 baseband modem chipsets. 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-2023-26497 in the underground.

Countermeasures

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

CVE-2023-26498	Status: Existing	CVSSv3: 8.6	Risk Level: Low
	Type: Memory corruption	PoC: Not Observed	Underground: Not Observed

CVE summary

CVE-2023-26498 is a memory corruption vulnerability impacting Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T512 baseband modem chipsets. 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-2023-26498 in the underground.

Countermeasures

Samsung addressed the vulnerability in 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.