PERISCOPE

June 7, 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-2017-9822	**Improper input validation**	**New**	**High**	●	●●	●●	
CVE-2011-2505	**Code injection**	**New**	**Medium**	●	●●	●●	
CVE-2017-3169	**Null pointer dereference**	**New**	**Medium**	●	●●●	●●	
CVE-2021-0920	**Use after free**	**New**	**Medium**	●	●●	●●	
CVE-2021-43008	**Improper access control**	**New**	**Medium**	●	●●	●●	
CVE-2022-20821	**Information Disclosure**	**New**	**Medium**	●	●●	●●	
CVE-2016-7103	**XSS**	**New**	**Low**	●	●●●	●●	
CVE-2016-7409	**Exposure of sensitive information to an unauthorized actor**	**New**	**Low**	●	●●●	●●	●
CVE-2017-15944	Unspecified	Existing	**High**	●	●●	●●	
CVE-2022-22947	Code injection	Existing	**High**	●	●●	●●	
CVE-2022-28810	OS command injection	Existing	**High**	●	●●	●●	
CVE-2022-30525	OS command injection	Existing	**High**	●	●●	●●	
CVE-2021-23450	Prototype pollution	Existing	Medium	●	●●	●●●	
CVE-2022-24707	SQLi	Existing	Medium	●	●●	●●	
CVE-2022-24734	Code injection	Existing	Medium	●	●●	●●	

CVE-2019-11507	XSS	Existing	Low	●	●●	●●	🐞
CVE-2019-11538	Improper link resolution before file access	Existing	Low	●	●●	●●	●
CVE-2019-11540	Unspecified	Existing	Low	●	●●	●●	🐞
CVE-2019-11542	Out-of-bounds write	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-2017-9822	Status: New	CVSSv3: 8.8	Risk Level: High
	Type: Improper input validation	PoC: Observed	Underground: Observed

CVE summary

CVE-2017-9822 is an improper input validation vulnerability impacting DNN DotNetNuke versions 9.1.0 and earlier. A Metasploit module was observed in open source and subsequently shared 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

CVE-2017-9822 was weaponized and productized. Several actors posted a Metasploit module for CVE-2017-9822 from open source. Additionally, the actor **djebbaranon** shared a tutorial on how to exploit CVE-2017-9822 and received positive comments from multiple users.

Countermeasures

DNN addressed the vulnerability in a security advisory with updated version.

CVE-2011-2505	Status: New	CVSSv2: 6.4	Risk Level: Medium
	Type: Code injection	PoC: Observed	Underground: Observed

CVE summary

CVE-2011-2505 is a code injection vulnerability impacting phpMyAdmin versions 3.0 through 3.3.10.1, 3.4.0 through 3.4.3. An exploit was observed in open source and subsequently shared in the underground.

Underground activity

CVE-2011-2505 was weaponized. The actors **xaren** and **Nytro** posted an exploit for CVE-2011-2505 from open source.

Countermeasures

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

CVE-2017-3169	Status: New	CVSSv3: 9.8	Risk Level: Medium
	Type: Null pointer dereference	PoC: Observed	Underground: Observed

CVE summary

CVE-2017-3169 is a null pointer dereference vulnerability impacting Apache HTTP Server versions 2.2.0 through 2.2.32 and 2.4.0 through 2.4.25. An exploit was observed in open source and a link to an exploit was shared in the underground.

Underground activity

CVE-2017-3169 was weaponized. The actors **GLXBX** and **Desoxyn** posted a link to an exploit for CVE-2017-3169 from open source. Additionally, the actor **Fresh777** sought an exploit for CVE-2017-3169 on the XSS forum.

Countermeasures

Apache addressed the vulnerability in HTTP Server versions 2.2.33 and 2.4.26.

CVE-2021-0920	Status: New	CVSSv3: 6.4	Risk Level: Medium
	Type: Use after free	PoC: Not Observed	Underground: Observed

CVE summary

CVE-2021-0920 is a use after free vulnerability impacting Google Android. 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-2021-0920 in the underground. The actor **Dragora** shared information from open-source reporting.

Countermeasures

Google addressed the vulnerability in an Android security bulletin with updated versions.

CVE-2021-43008	Status: New	CVSSv3: 7.5	Risk Level: Medium
	Type: Improper access control	PoC: Observed	Underground: Observed

CVE summary

CVE-2021-43008 is an improper access control vulnerability impacting Adminer versions 1.12.0 through 4.6.2. An exploit was observed in open source and subsequently shared in the underground.

Underground activity

CVE-2021-43008 was weaponized. The actor **SenjorZeroday** posted a link to an exploit for CVE-2021-43008 from open source.

Countermeasures

The vulnerability was addressed in Adminer version 4.6.3.

CVE-2022-20821	Status: New	CVSSv3: 6.5	Risk Level: Medium
	Type: Information Disclosure	PoC: Not Observed	Underground: Observed

CVE summary

CVE-2022-20821 is an information disclosure vulnerability impacting Cisco IOS XR version 7.3.3. A proof of concept (PoC) was not observed publicly or in the underground. Cisco claimed the vulnerability was actively exploited in the wild.

Underground activity

Intel 471 has not observed weaponization or productization of CVE-2022-20821 in the underground. The actor **WWW** shared information from open-source reporting.

Countermeasures

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

CVE-2016-7103	Status: New	CVSSv3: 6.1	Risk Level: Low
	Type: XSS	PoC: Observed	Underground: Observed

CVE summary

CVE-2016-7103 is a cross-site scripting (XSS) vulnerability impacting jQuery UI versions 1.10.0 through 1.11.4. A proof of concept (PoC) was observed in open source.

Underground activity

Intel 471 has not observed weaponization or productization of CVE-2016-7103 in the underground. The actor **pervanusluge** sought help with exploiting CVE-2016-7103 and offered to pay US $5,000.

Countermeasures

jQuery addressed the vulnerability in jQuery UI version 1.12.0.

CVE-2016-7409	Status: New	CVSSv3: 5.5	Risk Level: Low
	Type: Exposure of sensitive information to an unauthorized actor	PoC: Not Observed	Underground: Observed

CVE summary

CVE-2016-7409 is an exposure of sensitive information to an unauthorized actor vulnerability impacting Dropbear SSH versions before 2016.74. 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-2016-7409 in the underground. The actor **İnterestHacker** sought help with downloading exploit code for CVE-2016-7409.

Countermeasures

Dropbear SSH addressed the vulnerability in a security advisory with updated version.

CVE-2017-15944	Status: Existing	CVSSv3: 9.8	Risk Level: High
	Type: Unspecified	PoC: Observed	Underground: Observed

CVE summary

CVE-2017-15944 is an unspecified vulnerability impacting Palo Alto Networks PAN-OS versions 6.1.18 and earlier, 7.0.0 through 7.0.18, 7.1.0 through 7.1.13 and 8.0.0 through 8.0.5. A Metasploit module was observed in open source and a proof of concept (PoC) was shared in the underground.

Underground activity

Intel 471 has not observed weaponization or productization of CVE-2017-15944 in the underground. The actors **weaver** and **neopaket** shared PoC information from open-source reporting.

Countermeasures

Palo Alto Networks addressed the vulnerability in a security advisory with updated versions.

CVE-2022-22947	Status: Existing	CVSSv3: 10	Risk Level: High
	Type: Code injection	PoC: Observed	Underground: Observed

CVE summary

CVE-2022-22947 is a code injection vulnerability impacting VMware Spring Cloud Gateway versions 3.0.0 through 3.0.6 and earlier and version 3.1.0. An exploit was observed in open source. 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-2022-22947 in the underground. The actors **WWW** and **fenix** shared information from open-source reporting.

Countermeasures

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

CVE-2022-28810	Status: Existing	CVSSv3: 6.8	Risk Level: High
	Type: OS command injection	PoC: Observed	Underground: Observed

CVE summary

CVE-2022-28810 is an OS command injection vulnerability impacting Zoho ManageEngine ADSelfService Plus versions 6121 and earlier. A Metasploit module was observed in open source and subsequently shared in the underground. Security researchers claimed the vulnerability was actively exploited in the wild.

Underground activity

CVE-2022-28810 was weaponized and productized. The actor **Kev** posted a Metasploit module for CVE-2022-28810 from open source.

Countermeasures

Zoho addressed the vulnerability in ManageEngine ADSelfService Plus version 6122.

CVE-2022-30525	Status: Existing	CVSSv3: 9.8	Risk Level: High
	Type: OS command injection	PoC: Observed	Underground: Observed

CVE summary

CVE-2022-30525 is an OS command injection vulnerability impacting multiple versions of Zyxel USG FLEX 100(W), USG FLEX 200, USG FLEX 500, USG FLEX 700, USG FLEX 50(W), USG20(W)-VPN, ATP series, and VPN series firmware. A Metasploit module was observed in open source and subsequently shared in the underground. Further, a walk through demo of an exploit was shared via YouTube. Additionally, security researchers claimed threat actors actively were scanning for vulnerable firewall instances and there were attempts to exploit this vulnerability in the wild.

Underground activity

CVE-2022-30525 was weaponized and productized. The actor **Kev** posted a Metasploit module and the actor **web_corp** posted a link to a Metasploit module for CVE-2022-30525 from open source. Additionally, the actor **XOPALEHA** advertised an exploit for sale on the Exploit forum priced at US $70,000 and offered to work through an escrow.

Countermeasures

Zyxel Networks addressed the vulnerability in a security advisory with updated versions.

CVE-2021-23450	Status: Existing	CVSSv3: 9.8	Risk Level: Medium
	Type: Prototype pollution	PoC: Not Observed	Underground: Observed

CVE summary

CVE-2021-23450 is a prototype pollution vulnerability impacting OpenJS Dojo versions 1.16.5 and earlier. A proof of concept (PoC) was not observed in open source. However, a web shell access was sold in the underground.

Underground activity

CVE-2021-23450 was likely weaponized. The actor **ChoiMu** allegedly leveraged CVE-2021-23450 to obtain a web shell on the vulnerable subdomain. Additionally, the actor **ChoiMu's** associate, actor **d4rk0wl**, allegedly sold a web shell to the **LAPSUS$** threat group.

Countermeasures

OpenJS Foundation addressed the vulnerability in Dojo version 1.17.0.

CVE-2022-24707	Status: Existing	CVSSv3: 8.8	Risk Level: Medium
	Type: SQLi	PoC: Observed	Underground: Observed

CVE summary

CVE-2022-24707 is a structured query language injection (SQLi) vulnerability impacting Anuko Time Tracker versions 1.20.0.5640 and prior. An exploit was observed in open source and a link to an exploit was shared in the underground.

Underground activity

CVE-2022-24707 was weaponized. The actor **beybala** posted a link to an exploit for CVE-2022-24707 from open source.

Countermeasures

The vendor addressed the vulnerability in GitHub software development platform saved commit change with a patch.

CVE-2022-24734	Status: Existing	CVSSv3: 7.2	Risk Level: Medium
	Type: Code injection	PoC: Observed	Underground: Observed

CVE summary

CVE-2022-24734 is a code injection vulnerability impacting MyBB versions 1.2.0 through 1.8.29. An exploit was observed in open source and subsequently shared in the underground.

Underground activity

CVE-2022-24734 was weaponized. The actor **DarckSol** posted an exploit for CVE-2022-24734 from open source.

Countermeasures

MyBB addressed the vulnerability in MyBB version 1.8.30.

CVE-2019-11507	Status: Existing	CVSSv3: 6.1	Risk Level: Low
	Type: XSS	PoC: Observed	Underground: Observed

CVE summary

CVE-2019-11507 is a cross-site scripting (XSS) vulnerability impacting multiple versions of Pulse Secure Pulse Connect Secure. 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-2019-11507 in the underground. The actor **weaver** shared a link to PoC information from open-source reporting.

Countermeasures

Pulse Secure addressed the vulnerability in a security advisory with updated versions.

CVE-2019-11538	Status: Existing	CVSSv3: 7.7	Risk Level: Low
	Type: Improper link resolution before file access	PoC: Not Observed	Underground: Observed

CVE summary

CVE-2019-11538 is an improper link resolution before file access vulnerability impacting multiple versions of Pulse Secure Pulse Connect Secure. 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-2019-11538 in the underground. The actor **weaver** shared information from open-source reporting.

Countermeasures

Pulse Secure addressed the vulnerability in a security advisory with updated versions.

CVE-2019-11540	Status: Existing	CVSSv3: 9.8	Risk Level: Low
	Type: Unspecified	PoC: Observed	Underground: Observed

CVE summary

CVE-2019-11540 is an unspecified vulnerability impacting multiple versions of Pulse Secure Pulse Connect Secure and Pulse Policy Secure. 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-2019-11540 in the underground. The actor **weaver** shared a link to PoC information from open-source reporting.

Countermeasures

Pulse Secure addressed the vulnerability in a security advisory with updated versions.

CVE-2019-11542	Status: Existing	CVSSv3: 8	Risk Level: Low
	Type: Out-of-bounds write	PoC: Observed	Underground: Observed

CVE summary

CVE-2019-11542 is an out-of-bounds write vulnerability impacting multiple versions of Pulse Secure Pulse Connect Secure and Pulse Policy Secure. 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-2019-11542 in the underground. The actor **weaver** shared a link to PoC information from open-source reporting.

Countermeasures

Pulse Secure 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.