Daily brief, Monday, May 25, 2026

May 24, 8:00 PM to May 25, 8:00 PM ET

Generated Nov 6, 2026, 11:17 PM ET

0	0	0	22	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

22 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

No CVEs added to CISA's known-exploited list.

New public exploit code

No new Nuclei templates, Metasploit modules, Exploit-DB or VulnCheck XDB entries.

New critical CVEs

22

9.8 **CVE-2026-9405**

A security flaw has been discovered in Totolink A8000RU 7.1cu.643_b20200521. This impacts the function setGameSpeedCfg of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. Performing a manipulation of the argument enable results in os co

9.8 **CVE-2026-9406**

A weakness has been identified in Totolink A8000RU 7.1cu.643_b20200521. Affected is the function setRemoteCfg of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. Executing a manipulation of the argument enable can lead to os command inj

9.8 **CVE-2026-9407**

A security vulnerability has been detected in Totolink A8000RU 7.1cu.643_b20200521. Affected by this vulnerability is the function setFirewallType of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. The manipulation of the argument fire

9.8 **CVE-2026-9408**

A vulnerability was detected in Totolink A8000RU 7.1cu.643_b20200521. Affected by this issue is the function setStaticDhcpRules of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. The manipulation of the argument enable results in os co

9.8 **CVE-2026-9432**

A security flaw has been discovered in Totolink A8000RU 7.1cu.643_b20200521. This vulnerability affects the function setWiFiAdvancedCfg of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. The manipulation of the argument bgProtection re

9.8 **CVE-2026-9433**

A weakness has been identified in Totolink A8000RU 7.1cu.643_b20200521. This issue affects the function setMacFilterRules of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. This manipulation of the argument enable causes os command inj

9.8 **CVE-2026-9434**

A security vulnerability has been detected in Totolink A8000RU 7.1cu.643_b20200521. Impacted is the function setWiFiWpsCfg of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. Such manipulation of the argument wscDisabled leads to os com

9.8 **CVE-2026-9435**

A vulnerability was detected in Totolink A8000RU 7.1cu.643_b20200521. The affected element is the function setQosCfg of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. Performing a manipulation of the argument enable results in os comm

9.8 **CVE-2026-9436**

A flaw has been found in Totolink A8000RU 7.1cu.643_b20200521. The impacted element is the function setL2tpServerCfg of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. Executing a manipulation of the argument enable can lead to os comm

9.8 **CVE-2026-9454**

A flaw has been found in Totolink A8000RU 7.1cu.643_b20200521. This vulnerability affects the function setOpenVpnCertGenerationCfg of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. Executing a manipulation of the argument servername c

9.8 **CVE-2026-9455**

A vulnerability has been found in Totolink A8000RU 7.1cu.643_b20200521. This issue affects the function UploadOpenVpnCert of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. The manipulation of the argument FileName leads to os command

9.8 **CVE-2026-9456**

A vulnerability was found in Totolink A8000RU 7.1cu.643_b20200521. Impacted is the function setOpenVpnCfg of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. The manipulation of the argument enabled results in os command injection. The

9.8 **CVE-2026-9457**

A vulnerability was determined in Totolink A8000RU 7.1cu.643_b20200521. The affected element is the function UploadFirmwareFile of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. This manipulation of the argument FileName causes os com

9.8 **CVE-2026-9458**

A vulnerability was identified in Totolink A8000RU 7.1cu.643_b20200521. The impacted element is the function setWanCfg of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. Such manipulation of the argument enabled leads to os command inj

9.8 **CVE-2026-9475**

A vulnerability was determined in Totolink A8000RU 7.1cu.643_b20200521. This affects the function setIpQosRules of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. This manipulation of the argument Comment causes os command injection. R

9.8 **CVE-2026-9476**

A vulnerability was identified in Totolink A8000RU 7.1cu.643_b20200521. This vulnerability affects the function setPasswordCfg of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. Such manipulation of the argument admpass leads to os com

9.8 **CVE-2026-9477**

A security flaw has been discovered in Totolink A8000RU 7.1cu.643_b20200521. This issue affects the function setAccessDeviceCfg of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. Performing a manipulation of the argument mac results in

9.8 **CVE-2026-9478**

A weakness has been identified in Totolink A8000RU 7.1cu.643_b20200521. Impacted is the function setParentalRules of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. Executing a manipulation of the argument enable can lead to os command

9.3 **CVE-2026-9058**

For untrusted certificates that contain the "Authority Information Access - calssuers URI" extension, Szafir SDK will automatically download the parent CA certificate from the specified URL and will import it to its trust store as a "nonqualified" certificate.

9.3 **CVE-2026-42773**

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in eMagicOne eMagicOne Store Manager allows Blind SQL Injection. This issue affects eMagicOne Store Manager: from n/a through 1.3.2.

2 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches

No new breaches published.

Watch Floor collects CVE records, CISA KEV, exploit indexes, official advisories, security news and chatter. CVSS is the headline score. Ransomware posts are criminal groups' claims, not confirmed by the victims. Leak-site data: RansomLook (ransomlook.io), CC BY 4.0; sectors grouped and countries mapped by Watch Floor. CVE IDs link to the full record on Watch Floor.