Daily brief, Friday, April 10, 2026

Apr 9, 8:00 PM to Apr 10, 8:00 PM ET

Generated Nov 7, 2026, 8:03 AM ET

0	0	0	28	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

28 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

28

9.9 **CVE-2026-5412** Canonical juju

In Juju versions prior to 2.9.57 and 3.6.21, an authorization issue exists in the Controller facade. An authenticated user can call the CloudSpec API method to extract the cloud credentials used to bootstrap the controller. This allows a low-privileged user to

9.8 **CVE-2026-5993**

A vulnerability was identified in Totolink A7100RU 7.4cu.2313_b20191024. This vulnerability affects the function setWiFiGuestCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Such manipulation of the argument wifiOff leads to os command inject

9.8 **CVE-2026-5994**

A security flaw has been discovered in Totolink A7100RU 7.4cu.2313_b20191024. This issue affects the function setTelnetCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Performing a manipulation of the argument telnet_enabled results in os com

9.8 **CVE-2026-5995**

A weakness has been identified in Totolink A7100RU 7.4cu.2313_b20191024. Impacted is the function setMiniuiHomeInfoShow of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Executing a manipulation of the argument lan_info can lead to os command inje

9.8 **CVE-2026-5996**

A security vulnerability has been detected in Totolink A7100RU 7.4cu.2313_b20191024. The affected element is the function setAdvancedInfoShow of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument tty_server leads to os

9.8 **CVE-2026-5997**

A vulnerability was detected in Totolink A7100RU 7.4cu.2313_b20191024. The impacted element is the function setLoginPasswordCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument admpass results in os command inject

9.8 **CVE-2026-6025**

A vulnerability was identified in Totolink A7100RU 7.4cu.2313_b20191024. This affects the function setSyslogCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Such manipulation of the argument enable leads to os command injection. It is possibl

9.8 **CVE-2026-6026**

A security flaw has been discovered in Totolink A7100RU 7.4cu.2313_b20191024. This vulnerability affects the function setPortalConfWeChat of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Performing a manipulation of the argument enable results in

9.8 **CVE-2026-6027**

A weakness has been identified in Totolink A7100RU 7.4cu.2313_b20191024. This issue affects the function setUrlFilterRules of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Executing a manipulation of the argument enable can lead to os command inj

9.8 **CVE-2026-6028**

A security vulnerability has been detected in Totolink A7100RU 7.4cu.2313_b20191024. Impacted is the function setPptpServerCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument enable leads to os command injection.

9.8 **CVE-2026-6029**

A vulnerability was detected in Totolink A7100RU 7.4cu.2313_b20191024. The affected element is the function setVpnAccountCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument User results in os command injection. T

9.8 **CVE-2026-6057**

FalkorDB Browser 1.9.3 contains an unauthenticated path traversal vulnerability in the file upload API that allows remote attackers to write arbitrary files and achieve remote code execution.

9.8 **CVE-2025-44560**

owntone-server 2ca10d9 is vulnerable to Buffer Overflow due to lack of recursive checking.

9.8 **CVE-2026-29861**
PHP-MYSQL-User-Login-System v1.0 was discovered to contain a SQL injection vulnerability via the username parameter at login.php.

9.8 **CVE-2026-36232** Itsourcecode online student enrollment system
A SQL injection vulnerability was found in the instructorClasses.php file of itsourcecode Online Student Enrollment System v1.0. The reason for this issue is that the 'classId' parameter from $_GET['classId'] is directly concatenated into the SQL query without

9.8 **CVE-2026-36233** Itsourcecode online student enrollment system
A SQL injection vulnerability was found in the assignInstructorSubjects.php file of itsourcecode Online Student Enrollment System v1.0. The reason for this issue is that attackers can inject malicious code via the parameter "subjcode" and use it directly in SQ

9.8 **CVE-2026-36234** Itsourcecode online student enrollment system
itsourcecode Online Student Enrollment System v1.0 is vulnerable to SQL Injection in newCourse.php via the 'coursename' parameter.

9.8 **CVE-2026-36235** Itsourcecode online student enrollment system
A SQL injection vulnerability was found in the scheduleSubList.php file of itsourcecode Online Student Enrollment System v1.0. The reason for this issue is that the 'subjcode' parameter is directly embedded into the SQL query via string interpolation without a

9.8 **CVE-2026-36236** Janobe engineers online portal
SourceCodester Engineers Online Portal v1.0 is vulnerable to SQL Injection in update_password.php via the new_password parameter.

9.8 **CVE-2026-23781** Bmc control-m\/managed file transfer
An issue was discovered in BMC Control-M/MFT 9.0.20 through 9.0.22. A set of default debug user credentials is hardcoded in cleartext within the application package. If left unchanged, these credentials can be easily obtained and may allow unauthorized access

8 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.