Daily brief, Monday, April 27, 2026

Apr 26, 8:00 PM to Apr 27, 8:00 PM ET

Generated Nov 7, 2026, 5:00 AM ET

0	0	0	29	0	2
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

29 new critical CVEs, 2 new breaches.

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

29

10.0 **CVE-2026-33453** Apache camel DETECTION

Improperly Controlled Modification of Dynamically-Determined Object Attributes vulnerability in Apache Camel Camel-Coap component. Apache Camel's camel-coap component is vulnerable to Camel message header injection, leading to remote code execution when routes

9.9 **CVE-2026-40453** Apache camel

The fix for CVE-2025-27636 added setLowerCase(true) to HttpHeaderFilterStrategy so that case-variant header names such as 'CAmelExecCommandExecutable' are filtered out alongside 'CamelExecCommandExecutable'. The same setLowerCase(true) call was not applied to

9.8 **CVE-2026-40860** Apache camel

JmsBinding.extractBodyFromJms() in camel-jms, and the equivalent JmsBinding class in camel-sjms, deserialized the payload of incoming JMS ObjectMessage values via javax.jms.ObjectMessage.getObject() without applying any ObjectInputFilter, class allowlist or cl

9.8 **CVE-2026-41635** Apache mina

Apache MINA's AbstractIoBuffer.resolveClass() contains two branches, one of them (for static classes or primitive types) does not check the class at all, bypassing the classname allowlist and allowing arbitrary code to be executed. The fix checks if the class

9.8 **CVE-2026-41409** Apache mina

The fix for CVE-2024-52046 in Apache MINA AbstractIoBuffer.getObject() was incomplete. The classname allowlist of classes allowed to be deserialized was applied too late after a static initializer in a class to be read might already have been executed. Affecte

9.8 **CVE-2026-22337**

Incorrect Privilege Assignment vulnerability in Directorist Directorist Social Login allows Privilege Escalation.This issue affects Directorist Social Login: from n/a before 2.1.4.

9.8 **CVE-2026-7121**

A flaw has been found in Totolink A8000RU 7.1cu.643_b20200521. This affects the function setWizardCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. This manipulation of the argument wizard causes os command injection. It is possible to initiat

9.8 **CVE-2026-7122**

A vulnerability has been found in Totolink A8000RU 7.1cu.643_b20200521. This impacts the function setUPnPCfg 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 possible t

9.8 **CVE-2026-7123**

A vulnerability was found in Totolink A8000RU 7.1cu.643_b20200521. Affected is the function setIptvCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Performing a manipulation of the argument setIptvCfg results in os command injection. The atta

9.8 **CVE-2026-7124**

A vulnerability was determined in Totolink A8000RU 7.1cu.643_b20200521. Affected by this vulnerability is the function setIpv6LanCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Executing a manipulation of the argument addrPrefixLen can lead

9.8 **CVE-2026-7125**

A vulnerability was identified in Totolink A8000RU 7.1cu.643_b20200521. Affected by this issue is the function setWiFiEasyCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument merge leads to os command injection. T

9.8 **CVE-2026-30352**

A remote code execution (RCE) vulnerability in the /devserver/start endpoint of leonvanzyl autocoder commit 79d02a allows attackers to execute arbitrary code via providing a crafted command parameter.

9.8 **CVE-2026-41462**

ProjeQtor versions 7.0 through 12.4.3 contain an unauthenticated SQL injection vulnerability in the login functionality where the login variable is directly concatenated into a SQL query without parameterization or sanitization. Attackers can inject arbitrary

9.8 **CVE-2026-7136**

A weakness has been identified in Totolink A8000RU 7.1cu.643_b20200521. Affected by this issue is the function setDmzCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Executing a manipulation of the argument wanIdx can lead to os command injec

9.8 **CVE-2026-7137**

A security vulnerability has been detected in Totolink A8000RU 7.1cu.643_b20200521. This affects the function setStorageCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument sambaEnabled leads to os command injecti

9.8 **CVE-2026-7138**

A vulnerability was detected in Totolink A8000RU 7.1cu.643_b20200521. This vulnerability affects the function setNtpCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument tz results in os command injection. The atta

9.8 **CVE-2026-7139**

A flaw has been found in Totolink A8000RU 7.1cu.643_b20200521. This issue affects the function setWiFiAclRules of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. This manipulation of the argument mode causes os command injection. The attack is poss

9.8 **CVE-2026-7140**

A vulnerability has been found in Totolink A8000RU 7.1cu.643_b20200521. Impacted is the function CsteSystem of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Such manipulation of the argument HTTP leads to os command injection. The attack may be p

9.8 **CVE-2026-31255** Tenda ac18 firmware

A command injection vulnerability exists in Tenda AC18 V15.03.05.05_multi. The vulnerability is located in the /goform/SetSambaCfg interface, where improper handling of the guestuser parameter allows attackers to execute arbitrary system commands.

9.8 **CVE-2026-35903** Mercurycom mipc252w firmware

MERCURY MIPC252W IP camera 1.0.5 Build 230306 Rel.79931n contains an improper authentication vulnerability in the RTSP service. After successful Digest authentication in an initial DESCRIBE request, the device does not verify the Digest response parameter in s

9 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 2

Pitney Bowes pitneybowes.com	8,243,989 accounts
ADT adt.com	5,488,888 accounts

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.