Daily brief, Monday, April 13, 2026

Apr 12, 8:00 PM to Apr 13, 8:00 PM ET

Generated Nov 7, 2026, 7:25 AM ET

0	7	0	21	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

7 newly exploited, 21 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

7

9.1 **CVE-2026-21643** Fortinet FortiClient EMS CISA KEV DETECTION

SQL injection in Fortinet FortiClient EMS lets an attacker gain unauthorized access to sensitive data and administrative privileges.

8.8 **CVE-2023-21529** Microsoft Exchange Server CISA KEV

An attacker gains arbitrary code execution on Microsoft Exchange Server through deserialization of untrusted data.

8.6 **CVE-2026-34621** Adobe Acrobat and Reader CISA KEV

Adobe Acrobat and Reader prototype pollution flaw lets an attacker execute arbitrary code.

7.8 **CVE-2020-9715** Adobe Acrobat CISA KEV

A use-after-free flaw in Adobe Acrobat lets an attacker execute arbitrary code.

7.8 **CVE-2023-36424** Microsoft Windows CISA KEV

An out-of-bounds read in the Microsoft Windows Common Log File System Driver lets an attacker escalate privileges on Windows.

7.8 **CVE-2025-60710** Microsoft Windows CISA KEV

Microsoft Windows link following flaw (CWE-59) allows privilege escalation; the input does not state authentication or user interaction requirements.

7.8 **CVE-2012-1854** Microsoft Visual Basic for Applications (VBA) CISA KEV

Insecure library loading in Microsoft Visual Basic for Applications (VBA) lets an attacker achieve remote code execution.

New public exploit code

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

New critical CVEs 21

9.1 **CVE-2026-21643** Fortinet FortiClient EMS KEV EXPLOIT CODE DETECTION
SQL injection in Fortinet FortiClient EMS lets an attacker gain unauthorized access to sensitive data and administrative privileges.

9.8 **CVE-2026-31414** Linux linux kernel
In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_conntrack_expect: use expect->helper Use expect->helper in ctnetlink and /proc to dump the helper name. Using nfct_help() without holding a reference to the master conntrack is u

9.1 **CVE-2026-0234** Palo Alto Networks cortex xsiam
An improper verification of cryptographic signature vulnerability exists in Cortex XSOAR and Cortex XSIAM platforms during integration of Microsoft Teams that enables an unauthenticated user to access and modify protected resources.

9.8 **CVE-2026-6154** Totolink A7100RU
A security flaw has been discovered in Totolink A7100RU 7.4cu.2313_b20191024. The affected element is the function setWizardCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Performing a manipulation of the argument wizard results in os comman

9.8 **CVE-2026-6155** Totolink A7100RU
A weakness has been identified in Totolink A7100RU 7.4cu.2313. The impacted element is the function setWanCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Executing a manipulation of the argument pppoeServiceName can lead to os command inject

9.8 **CVE-2026-40044** Pachno Pachno
Pachno 1.0.6 contains a deserialization vulnerability that allows unauthenticated attackers to execute arbitrary code by injecting malicious serialized objects into cache files. Attackers can write PHP object payloads to world-writable cache files with predict

9.8 **CVE-2026-6138**
A flaw has been found in Totolink A7100RU 7.4cu.2313_b20191024. The impacted element is the function setAccessDeviceCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. This manipulation of the argument mac causes os command injection. The attack

9.8 **CVE-2026-6139**
A vulnerability has been found in Totolink A7100RU 7.4cu.2313_b20191024. This affects the function UploadOpenVpnCert of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Such manipulation of the argument FileName leads to os command injection. The at

9.8 **CVE-2026-6140**
A vulnerability was found in Totolink A7100RU 7.4cu.2313_b20191024. This impacts the function UploadFirmwareFile of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Performing a manipulation of the argument FileName results in os command injection.

9.8 **CVE-2026-6156**

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

9.8 **CVE-2026-31282**

Totara LMS v19.1.5 and before is vulnerable to Incorrect Access Control. The login page code can be manipulated to reveal the login form. An attacker can chain that with missing rate-limit on the login form to launch a brute force attack. NOTE: this is dispute

9.8 **CVE-2026-31283**

In Totara LMS v19.1.5 and before, the forgot password API does not implement rate limiting for the target email address. which can be used for an Email Bombing attack. NOTE: the Supplier's position is that the pwresettime configuration defaults to 30 minutes,

9.8 **CVE-2026-6195** DETECTION

A security vulnerability has been detected in Totolink A7100RU 7.4cu.2313_b20191024. Affected by this issue is the function setPasswordCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Such manipulation of the argument admpass leads to os comm

9.8 **CVE-2026-40042**

Pachno 1.0.6 contains an XML external entity injection vulnerability that allows unauthenticated attackers to read arbitrary files by exploiting unsafe XML parsing in the TextParser helper. Attackers can inject malicious XML entities through wiki table syntax

9.8 **CVE-2026-31048**

An issue in the <code>pickle</code> protocol of Pyro v3.x allows attackers to execute arbitrary code via supplying a crafted pickled string message.

9.8 **CVE-2026-22562**

A malicious actor with access to the UniFi Play network could exploit a Path Traversal vulnerability found in the device firmware to write files on the system that could be used for a remote code execution (RCE). Affected Products: UniFi Play PowerAmp (Version

9.8 **CVE-2026-22563**

A series of Improper Input Validation vulnerabilities could allow a Command Injection by a malicious actor with access to the UniFi Play network. Affected Products: UniFi Play PowerAmp (Version 1.0.35 and earlier) UniFi Play Audio Port (Version 1.0.24 and earl

9.8 **CVE-2026-22564**

An Improper Access Control vulnerability could allow a malicious actor with access to the UniFi Play network to enable SSH to make unauthorized changes to the system. Affected Products: UniFi Play PowerAmp (Version 1.0.35 and earlier) UniFi Play Audio Port (Ve

9.3 **CVE-2026-4810** DETECTION

A Code Injection and Missing Authentication vulnerability in Google Agent Development Kit (ADK) versions 1.7.0 (and 2.0.0a1) through 1.28.1 (and 2.0.0a2) on Python (OSS), Cloud Run, and GKE allows an unauthenticated remote attacker to execute arbitrary code on

9.1 **CVE-2026-34865** Huawei harmonyos

Out-of-bounds write vulnerability in the WEB module.Impact: Successful exploitation of this vulnerability will affect availability and confidentiality.

1 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.