Daily brief, Thursday, March 5, 2026

Mar 4, 7:00 PM to Mar 5, 7:00 PM ET

Generated Nov 7, 2026, 2:34 PM ET

0	5	0	72	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

5 newly exploited, 72 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

5

9.8 **CVE-2021-22681** Rockwell Multiple Products CISA KEV

Attacker can discover a key verifying Logix controller communication with Rockwell design software in Studio 5000 Logix Designer and other Rockwell products.

9.8 **CVE-2017-7921** Hikvision Multiple Products CISA KEV DETECTION

Improper authentication in multiple Hikvision products lets an attacker escalate privileges and access sensitive information.

8.8 **CVE-2021-30952** Apple Multiple Products CISA KEV

An integer overflow in Apple tvOS, macOS, Safari, iPadOS and watchOS lets an attacker execute arbitrary code via maliciously crafted web content.

8.8 **CVE-2023-43000** Apple Multiple Products CISA KEV

Crafted web content triggers a use-after-free in Apple macOS, iOS, iPadOS, and Safari 16.6, causing memory corruption.

7.8 **CVE-2023-41974** Apple iOS and iPadOS CISA KEV

A use-after-free flaw in Apple iOS and iPadOS lets an app execute arbitrary code with kernel privileges.

New public exploit code

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

New critical CVEs

72

9.8 **CVE-2017-7921** Hikvision Multiple Products KEV EXPLOIT CODE DETECTION

Improper authentication in multiple Hikvision products lets an attacker escalate privileges and access sensitive information.

9.8 **CVE-2021-22681** Rockwell Multiple Products KEV EXPLOIT CODE

Attacker can discover a key verifying Logix controller communication with Rockwell design software in Studio 5000 Logix Designer and other Rockwell products.

9.8 **CVE-2026-27944** Nginxui nginx ui DETECTION

Nginx UI is a web user interface for the Nginx web server. Prior to version 2.3.3, the /api/backup endpoint is accessible without authentication and discloses the encryption keys required to decrypt the backup in the X-Backup-Security response header. This all

9.1 **CVE-2026-2835** Cloudflare pingora

An HTTP Request Smuggling vulnerability (CWE-444) has been found in Pingora's parsing of HTTP/1.0 and Transfer-Encoding requests. The issue occurs due to improperly allowing HTTP/1.0 request bodies to be close-delimited and incorrect handling of multiple Trans

9.1 **CVE-2026-2833** Cloudflare pingora

An HTTP request smuggling vulnerability (CWE-444) was found in Pingora's handling of HTTP/1.1 connection upgrades. The issue occurs when a Pingora proxy reads a request containing an Upgrade header, causing the proxy to pass through the rest of the bytes on th

9.8 **CVE-2026-21536** Microsoft devices pricing program

Microsoft Devices Pricing Program Remote Code Execution Vulnerability

9.8 **CVE-2026-2743** Seppmail seppmail DETECTION

Arbitrary File Write via Path Traversal upload to Remote Code Execution in SeppMail User Web Interface. The affected feature is the large file transfer (LFT). This issue affects SeppMail: 15.0.2.1 and before

9.8 **CVE-2025-70230** Dlink dir-513 firmware

Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formSetDDNS.

10.0 **CVE-2026-0848** Nltk nltk

NLTK versions <=3.9.2 are vulnerable to arbitrary code execution due to improper input validation in the StanfordSegmenter module. The module dynamically loads external Java .jar files without verification or sandboxing. An attacker can supply or replace the J

9.8 **CVE-2025-70231** Dlink dir-513 firmware

D-Link DIR-513 version 1.10 contains a critical-level vulnerability. When processing POST requests related to verification codes in /goform/formLogin, it enters /goform/getAuthCode but fails to filter the value of the FILECODE parameter, resulting in a path tr

9.8 **CVE-2025-70229** Dlink dir-513 firmware

Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formSchedule.

9.8 **CVE-2025-70232** Dlink dir-513 firmware

Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formSetMACFilter.

9.8 **CVE-2025-70233** Dlink dir-513 firmware

Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formSetEnableWizard.

9.4 **CVE-2026-28446** Openclaw openclaw

OpenClaw versions prior to 2026.2.1 with the voice-call extension installed and enabled contain an authentication bypass vulnerability in inbound allowlist policy validation that accepts empty caller IDs and uses suffix-based matching instead of strict equalit

9.8 **CVE-2025-29165** Dlink dir-1253 firmware

An issue in D-Link DIR-1253 MESH V1.6.1684 allows an attacker to escalate privileges via the etc/shadow.sample component

9.1 **CVE-2026-24457** Eclipse openmq

An unsafe parsing of OpenMQ's configuration in OpenMQ versions <6.5.2 and <6.9.0, allows a remote attacker to read arbitrary files from a MQ Broker's server. A full exploitation could read unauthorized files of the OpenMQ's host OS. In some scenarios RCE could

9.1 **CVE-2025-40931** Chorny apache\

Apache::Session::Generate::MD5 versions through 1.94 for Perl create insecure session id. Apache::Session::Generate::MD5 generates session ids insecurely. The default session id generator returns a MD5 hash seeded with the built-in rand() function, the epoch t

9.8 **CVE-2026-3381** Pmqs compress\

Compress::Raw::Zlib versions through 2.219 for Perl use potentially insecure versions of zlib. Compress::Raw::Zlib includes a copy of the zlib library. Compress::Raw::Zlib version 2.220 includes zlib 1.3.2, which addresses findings fron the 7ASecurity audit of

9.8 **CVE-2026-2599**

The Database for Contact Form 7, WPforms, Elementor forms plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.4.7 via deserialization of untrusted input in the 'download_csv' function. This makes it possible for u

9.8 **CVE-2025-54001**

Deserialization of Untrusted Data vulnerability in ThemeREX Classter classter allows Object Injection.This issue affects Classter: from n/a through <= 2.5.

52 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.