Daily brief, Wednesday, March 25, 2026

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

Generated Nov 7, 2026, 10:53 AM ET

0	1	0	56	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 56 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

9.3 **CVE-2026-33017** Langflow Langflow CISA KEV DETECTION

Unauthenticated attackers can inject code into Langflow by building public flows, which the summary links to code injection on the server.

New public exploit code

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

New critical CVEs

56

9.3 **CVE-2026-33017** Langflow Langflow KEV EXPLOIT CODE DETECTION

Unauthenticated attackers can inject code into Langflow by building public flows, which the summary links to code injection on the server.

9.8 **CVE-2026-28858** Apple ipados

A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 26.4 and iPadOS 26.4. A remote user may be able to cause unexpected system termination or corrupt kernel memory.

9.3 **CVE-2026-28827** Apple macos

A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to break out of its sandbox.

9.3 **CVE-2026-20688** Apple ipados

A path handling issue was addressed with improved validation. This issue is fixed in iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4, visionOS 26.4. An app may be able to break out of its sandbox.

9.8 **CVE-2026-26831** Dbashford textract

textract through 2.5.0 is vulnerable to OS Command Injection via the file path parameter in multiple extractors. When processing files with malicious filenames, the filePath is passed directly to child_process.exec() in lib/extractors/doc.js, rtf.js, dxf.js, i

9.8 **CVE-2026-26830** Pdf-Image Project pdf-image

pdf-image (npm package) through version 2.0.0 allows OS command injection via the pdfFilePath parameter. The constructGetInfoCommand and constructConvertCommandForPage functions use util.format() to interpolate user-controlled file paths into shell command str

9.8 **CVE-2026-26833** Mmahrous thumbler

thumbler through 1.1.2 allows OS command injection via the input, output, time, or size parameter in the thumbnail() function because user input is concatenated into a shell command string passed to child_process.exec() without proper sanitization or escaping.

9.8 **CVE-2026-26832** Zapolnoch tesseract ocr

node-tesseract-ocr is an npm package that provides a Node.js wrapper for Tesseract OCR. In all versions through 2.2.1, the recognize() function in src/index.js is vulnerable to OS Command Injection. The file path parameter is concatenated into a shell command

9.8 **CVE-2025-59706** N2ws n2w

In N2W before 4.3.2 and 4.4.0 before 4.4.1, improper validation of API request parameters enables remote code execution.

9.8 **CVE-2025-59707** N2ws n2w

In N2W before 4.3.2 and 4.4.x before 4.4.1, there is potential remote code execution and account credentials theft because of a spoofing vulnerability.

9.8 **CVE-2026-27049**

Authentication Bypass Using an Alternate Path or Channel vulnerability in NooTheme Jobica Core jobica-core allows Authentication Abuse.This issue affects Jobica Core: from n/a through <= 1.4.2.

9.8 **CVE-2026-22500**

Deserialization of Untrusted Data vulnerability in axiomthemes m2 | Construction and Tools Store m2-ce allows Object Injection.This issue affects m2 | Construction and Tools Store: from n/a through <= 1.1.2.

9.8 **CVE-2026-22507**

Deserialization of Untrusted Data vulnerability in AncoraThemes Beelove beelove allows Object Injection.This issue affects Beelove: from n/a through <= 1.2.6.

9.8 **CVE-2026-24378**

Deserialization of Untrusted Data vulnerability in Metagauss EventPrime eventprime-event-calendar-management allows Object Injection.This issue affects EventPrime: from n/a through <= 4.2.8.0.

9.8 **CVE-2025-70888** Osslsigncode Project osslsigncode

An issue in mtrojnar Osslsigncode affected at v2.10 and before allows a remote attacker to escalate privileges via the osslsigncode.c component

9.8 **CVE-2026-27084**

Deserialization of Untrusted Data vulnerability in ThemeREX Buisson buisson allows Object Injection.This issue affects Buisson: from n/a through <= 1.1.11.

9.9 **CVE-2026-25345**

Improper Validation of Specified Quantity in Input vulnerability in GalleryCreator SimpLy Gallery simply-gallery-block allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects SimpLy Gallery: from n/a through <= 3.3.2.

9.8 **CVE-2026-25035**

Authentication Bypass Using an Alternate Path or Channel vulnerability in Wasiliy Strecker / ContestGallery developer Contest Gallery contest-gallery allows Authentication Abuse.This issue affects Contest Gallery: from n/a through <= 28.1.2.2.

9.8 **CVE-2026-24968**

Incorrect Privilege Assignment vulnerability in Xagio SEO Xagio SEO xagio-seo allows Privilege Escalation.This issue affects Xagio SEO: from n/a through <= 7.1.0.30.

9.3 **CVE-2026-22484**

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in pebas Lisfinity Core lisfinity-core allows SQL Injection.This issue affects Lisfinity Core: from n/a through <= 1.5.0.

36 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.