Daily brief, Wednesday, April 8, 2026

Apr 7, 8:00 PM to Apr 8, 8:00 PM ET

Generated Nov 7, 2026, 8:27 AM ET

0	1	0	27	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 27 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

9.8 **CVE-2026-1340** Ivanti Endpoint Manager Mobile (EPMM) CISA KEV DETECTION

An attacker gains arbitrary code execution and access to sensitive information in Ivanti Endpoint Manager Mobile (EPMM) through code injection.

New public exploit code

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

New critical CVEs

27

9.8 **CVE-2026-1340** Ivanti Endpoint Manager Mobile (EPMM) KEV EXPLOIT CODE DETECTION

An attacker gains arbitrary code execution and access to sensitive information in Ivanti Endpoint Manager Mobile (EPMM) through code injection.

9.8 **CVE-2026-27143** Golang go

Arithmetic over induction variables in loops were not correctly checked for underflow or overflow. As a result, the compiler would allow for invalid indexing to occur at runtime, potentially leading to memory corruption.

9.8 **CVE-2026-5902** Google chrome

Race in Media in Google Chrome on Android prior to 147.0.7727.55 allowed a remote attacker who had compromised the renderer process to corrupt media stream metadata via a crafted HTML page. (Chromium security severity: Low)

9.6 **CVE-2026-5874** Google chrome

Use after free in PrivateAI in Google Chrome prior to 147.0.7727.55 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)

9.8 **CVE-2026-3296** DETECTION

The Everest Forms plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.4.3 via deserialization of untrusted input from form entry metadata. This is due to the html-admin-page-entries-view.php file calling PHP's nat

9.8 **CVE-2026-3535**

The DSGVO Google Web Fonts GDPR plugin for WordPress is vulnerable to arbitrary file upload due to missing file type validation in the `DSGVOGWPdownloadGoogleFonts()` function in all versions up to, and including, 1.1. The function is exposed via a `wp_ajax_no

9.8 **CVE-2026-4003**

The Users manager – PN plugin for WordPress is vulnerable to Privilege Escalation via Arbitrary User Meta Update in all versions up to and including 1.1.15. This is due to a flawed authorization logic check in the userspn_ajax_nopriv_server() function within t

9.8 **CVE-2026-25776** Sixapart movable type

Movable Type provided by Six Apart Ltd. contains a code injection vulnerability which may allow an attacker to execute arbitrary Perl script.

9.8 **CVE-2026-2942**

The ProSolution WP Client plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'proSol_fileUploadProcess' function in all versions up to, and including, 1.9.9. This makes it possible for unauthenticated attack

9.8 **CVE-2026-31040** Statamcp stata-mcp

A vulnerability was identified in stata-mcp prior to v1.13.0 where insufficient validation of user-supplied Stata do-file content can lead to command execution.

9.8 **CVE-2026-33229** Xwiki xwiki

XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Prior to 17.4.8 and 17.10.1, an improperly protected scripting API allows any user with script right to bypass the sandboxing of the Velocity scripting API

9.8 **CVE-2025-52221** Tenda ac6 firmware

Tenda AC6 15.03.05.16_multi is vulnerable to Buffer Overflow in the formSetCfm function via the funcname, funcpara1, and funcpara2 parameters.

9.8 **CVE-2026-33088** Sixapart movable type

Movable Type provided by Six Apart Ltd. contains an SQL Injection vulnerability which may allow an attacker to execute an arbitrary SQL statement.

9.1 **CVE-2023-46945** Qd-Today qd

QD 20230821 is vulnerable to Server-side request forgery (SSRF) via a crafted request

9.1 **CVE-2026-31017** Frappe erpnext

A Server-Side Request Forgery (SSRF) vulnerability exists in the Print Format functionality of ERPNext v16.0.1 and Frappe Framework v16.1.1, where user-supplied HTML is insufficiently sanitized before being rendered into PDF. When generating PDFs from user-con

9.3 **CVE-2026-1346** Ibm security verify access

IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 and IBM Verify Identity Access 11.0 through 11.0.2 and IBM Security Verify Access 10.0 through 10.0.9.1 could allow a locally authenticated

9.6 **CVE-2026-39617**

Cross-Site Request Forgery (CSRF) vulnerability in priyanshumittal Bluestreet bluestreet allows Cross Site Request Forgery.This issue affects Bluestreet: from n/a through <= 1.7.3.

9.6 **CVE-2026-39619**

Cross-Site Request Forgery (CSRF) vulnerability in priyanshumittal Busiprof busiprof allows Upload a Web Shell to a Web Server.This issue affects Busiprof: from n/a through <= 2.5.2.

9.6 **CVE-2026-39620**

Cross-Site Request Forgery (CSRF) vulnerability in priyanshumittal Appointment appointment allows Upload a Web Shell to a Web Server.This issue affects Appointment: from n/a through <= 3.5.5.

9.6 **CVE-2026-39640**

Cross-Site Request Forgery (CSRF) vulnerability in mndpsingh287 Theme Editor theme-editor allows Code Injection.This issue affects Theme Editor: from n/a through <= 3.2.

7 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

My Lovely AI mylovely.ai 106,271 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.