Daily brief, Friday, November 21, 2025

Nov 20, 7:00 PM to Nov 21, 7:00 PM ET

Generated Nov 9, 2026, 8:03 AM ET

0	1	0	10	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 10 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

9.8 **CVE-2025-61757** Oracle Fusion Middleware CISA KEV DETECTION

Unauthenticated remote attackers can take over Oracle Fusion Middleware's Identity Manager by reaching a critical function that lacks authentication checks.

New public exploit code

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

New critical CVEs

10

9.8 **CVE-2025-61757** Oracle Fusion Middleware KEV EXPLOIT CODE DETECTION

Unauthenticated remote attackers can take over Oracle Fusion Middleware's Identity Manager by reaching a critical function that lacks authentication checks.

10.0 **CVE-2025-41115** Grafana grafana DETECTION

SCIM provisioning was introduced in Grafana Enterprise and Grafana Cloud in April to improve how organizations manage users and teams in Grafana by introducing automated user lifecycle management. In Grafana versions 12.x where SCIM provisioning is enabled and

10.0 **CVE-2025-65108**

md-to-pdf is a CLI tool for converting Markdown files to PDF using Node.js and headless Chrome. Prior to version 5.2.5, a Markdown front-matter block that contains JavaScript delimiter causes the JS engine in gray-matter library to execute arbitrary code in th

9.8 **CVE-2025-11456** Elula wsdesk

The ELEX WordPress HelpDesk & Customer Ticketing System plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the eh_crm_new_ticket_post() function in all versions up to, and including, 3.3.1. This makes it possibl

9.8 **CVE-2025-64755** Anthropic claude code

Claude Code is an agentic coding tool. Prior to version 2.0.31, due to an error in sed command parsing, it was possible to bypass the Claude Code read-only validation and write to arbitrary files on the host system. This issue has been patched in version 2.0.3

9.1 **CVE-2025-62608** Ml-Explore mlx

MLX is an array framework for machine learning on Apple silicon. Prior to version 0.29.4, there is a heap buffer overflow in mlx::core::load() when parsing malicious NumPy .npy files. Attacker-controlled file causes 13-byte out-of-bounds read, leading to crash

9.8 **CVE-2025-64310**

EPSON WebConfig and Epson Web Control for SEIKO EPSON Projector Products do not restrict excessive authentication attempts. An administrative user's password may be identified through a brute force attack.

9.1 **CVE-2025-64762** Workos authkit-nextjs

The AuthKit library for Next.js provides convenient helpers for authentication and session management using WorkOS & AuthKit with Next.js. In authkit-nextjs version 2.11.0 and below, authenticated responses do not defensively apply anti-caching headers. In env

9.8 **CVE-2025-11127**

The Mstoreapp Mobile App WordPress plugin through 2.08 and Mstoreapp Mobile Multivendor through 9.0.1 do not properly verify users identify when using an AJAX action, allowing unauthenticated users to retrieve a valid session for arbitrary users by knowing the

9.1 **CVE-2025-64767**

hpke-js is a Hybrid Public Key Encryption (HPKE) module built on top of Web Cryptography API. Prior to version 1.7.5, the public SenderContext Seal() API has a race condition which allows for the same AEAD nonce to be re-used for multiple Seal() calls. This ca

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.