Daily brief, Friday, December 12, 2025

Dec 11, 7:00 PM to Dec 12, 7:00 PM ET

Generated Nov 9, 2026, 4:46 AM ET

0	2	0	11	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 newly exploited, 11 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

2

8.8 **CVE-2025-14174** Google Chromium CISA KEV

Remote attacker gets out-of-bounds memory access in Chromium's ANGLE component via a crafted HTML page, affecting Chrome and other Chromium browsers.

8.8 **CVE-2018-4063** Sierra Wireless AirLink ALEOS CISA KEV

Sierra Wireless AirLink ALEOS contains an unrestricted upload of file with dangerous type vulnerability. A specially crafted HTTP request can upload a file, resulting in executable code being uploaded, and routable, to the webserver. An attacker can make an au

New public exploit code

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

New critical CVEs

11

9.8 **CVE-2024-14010** Typora Typora

Typora 1.7.4 contains a command injection vulnerability in the PDF export preferences that allows attackers to execute arbitrary system commands. Attackers can inject malicious commands into the 'run command' input field during PDF export to achieve remote cod

9.8 **CVE-2024-58299**

PCMan FTP Server 2.0 contains a buffer overflow vulnerability in the 'pwd' command that allows remote attackers to execute arbitrary code. Attackers can send a specially crafted payload during the FTP login process to overwrite memory and potentially gain syst

9.8 **CVE-2025-67728** Shaneisrael fireshare

Fireshare facilitates self-hosted media and link sharing. Versions 1.2.30 and below allow an authenticated user, or unauthenticated user if the Public Uploads setting is enabled, to craft a malicious filename when uploading a video file. The malicious filename

9.1 **CVE-2025-66430** Plesk plesk

Plesk 18.0 has Incorrect Access Control.

9.8 **CVE-2025-14344**

The Multi Uploader for Gravity Forms plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the 'plupload_ajax_delete_file' function in all versions up to, and including, 1.1.7. This makes it possible for unau

9.8 **CVE-2025-65854** Mineadmin mineadmin

Insecure permissions in the scheduled tasks feature of MineAdmin v3.x allows attackers to execute arbitrary commands and execute a full account takeover.

9.8 **CVE-2025-54947** Apache streampark

In Apache StreamPark versions 2.0.0 through 2.1.7, a security vulnerability involving a hard-coded encryption key exists. This vulnerability occurs because the system uses a fixed, immutable key for encryption instead of dynamically generating or securely conf

9.1 **CVE-2025-58130** Apache fineract

Insufficiently Protected Credentials vulnerability in Apache Fineract. This issue affects Apache Fineract: through 1.11.0. The issue is fixed in version 1.12.1. Users are encouraged to upgrade to version 1.13.0, the latest release.

9.8 **CVE-2025-67727** Parseplatform parse-server

Parse Server is an open source backend that can be deployed to any infrastructure that runs Node.js. In versions prior to 8.6.0-alpha.2, a GitHub CI workflow is triggered in a way that grants the GitHub Actions workflow elevated permissions, giving it access t

9.8 **CVE-2024-58311**

Dormakaba Saflok System 6000 contains a predictable key generation algorithm that allows attackers to derive card access keys from a 32-bit unique identifier. Attackers can exploit the deterministic key generation process by calculating valid access keys using

9.8 **CVE-2025-12963**

The LazyTasks – Project & Task Management with Collaboration, Kanban and Gantt Chart plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 1.2.29. This is due to the plugin not properly validating

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.