Daily brief, Monday, December 15, 2025

Dec 14, 7:00 PM to Dec 15, 7:00 PM ET

Generated Nov 9, 2026, 4:24 AM ET

0	2	0	16	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 newly exploited, 16 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

2

8.8 **CVE-2025-43529** Apple Multiple Products CISA KEV

Use-after-free in WebKit across iOS, iPadOS, macOS and other Apple products lets an attacker corrupt memory via maliciously crafted web content.

7.1 **CVE-2025-14611** Gladinet CentreStack and Triofox CISA KEV DETECTION

Hardcoded AES keys in Gladinet CentreStack and Triofox weaken public endpoints and allow arbitrary local file inclusion via crafted input.

New public exploit code

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

New critical CVEs

16

9.8 **CVE-2023-53877** Phpjabbers bus reservation system

Bus Reservation System 1.1 contains a SQL injection vulnerability in the pickup_id parameter that allows attackers to manipulate database queries. Attackers can exploit boolean-based, error-based, and time-based blind SQL injection techniques to steal informat

9.8 **CVE-2025-14706** Sgwbox n3 firmware DETECTION

A vulnerability was identified in Shiguangwu sgwbox N3 2.0.25. This impacts an unknown function of the file /usr/sbin/http_eshell_server of the component NETREBOOT Interface. Such manipulation leads to command injection. The attack can be launched remotely. Th

9.8 **CVE-2025-14707** Sgwbox n3 firmware DETECTION

A security flaw has been discovered in Shiguangwu sgwbox N3 2.0.25. Affected is an unknown function of the file /usr/sbin/http_eshell_server of the component DOCKER Feature. Performing manipulation of the argument params results in command injection. The attac

9.8 **CVE-2025-14705** Sgwbox n3 firmware DETECTION

A vulnerability was determined in Shiguangwu sgwbox N3 2.0.25. This affects an unknown function of the component SHARESERVER Feature. This manipulation of the argument params causes command injection. The attack can be initiated remotely. The exploit has been

9.8 **CVE-2025-14156**

The Fox LMS – WordPress LMS Plugin plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 1.0.5.1. This is due to the plugin not properly validating the 'role' parameter when creating new users via the `/fox-lms/v1/pay

9.8 **CVE-2025-14708** Sgwbox n3 firmware DETECTION

A weakness has been identified in Shiguangwu sgwbox N3 2.0.25. Affected by this vulnerability is an unknown functionality of the file /usr/sbin/http_eshell_server of the component WIREDCFGGET Interface. Executing manipulation of the argument params can lead to

9.8 **CVE-2025-14709** Sgwbox n3 firmware DETECTION

A security vulnerability has been detected in Shiguangwu sgwbox N3 2.0.25. Affected by this issue is some unknown functionality of the file /usr/sbin/http_eshell_server of the component WIRELESSCFGGET Interface. The manipulation of the argument params leads to

9.3 **CVE-2023-53872**

Wp2Fac 1.0 contains an OS command injection vulnerability in the send.php endpoint that allows remote attackers to execute arbitrary system commands. Attackers can inject shell commands through the 'numara' parameter by appending shell commands with '&' operat

9.8 **CVE-2025-65213** Mthreads torch musa

MooreThreads torch_musa through all versions contains an unsafe deserialization vulnerability in torch_musa.utils.compare_tool. The compare_for_single_op() and nan_inf_track_for_single_op() functions use pickle.load() on user-controlled file paths without vali

9.1 **CVE-2025-13888**

A flaw was found in OpenShift GitOps. Namespace admins can create ArgoCD Custom Resources (CRs) that trick the system into granting them elevated permissions in other namespaces, including privileged namespaces. An authenticated attacker can then use these ele

9.8 **CVE-2023-53871** Soosyze soosyze

Soosyze 2.0.0 contains a file upload vulnerability that allows attackers to upload arbitrary HTML files with embedded PHP code to the application. Attackers can exploit the broken file upload mechanism to potentially view sensitive file paths and execute malic

9.8 **CVE-2023-53874** Gomlab gom player

GOM Player 2.3.90.5360 contains a buffer overflow vulnerability in the equalizer preset name input field that allows attackers to crash the application. Attackers can overwrite the preset name with 260 'A' characters to trigger a buffer overflow and cause appl

9.8 **CVE-2025-64725** Weblate weblate

Weblate is a web based localization tool. In versions prior to 5.15, it was possible to accept an invitation opened by a different user. Version 5.15. contains a patch. As a workaround, avoid leaving one's Weblate sessions with an invitation opened unattended.

9.1 **CVE-2025-55895** Totolink a3300r firmware

TOTOLINK A3300R V17.0.0cu.557_B20221024 and N200RE V9.3.5u.6448_B20240521 and V9.3.5u.6437_B20230519 are vulnerable to Incorrect Access Control. Attackers can send payloads to the interface without logging in (remote).

9.0 **CVE-2025-59947** Emqx nanomq

NanoMQ is a messaging broker/bus for IoT Edge & SDV. Versions prior to 0.24.4 have a buffer overflow case while the PUBLISH packets trigger both shared subscription and vanila subscription. This is fixed in version 0.24.4. As a workaround, disable shared subsc

9.1 **CVE-2025-66844** Getgrav grav

In grav <1.7.49.5, a SSRF (Server-Side Request Forgery) vector may be triggered via Twig templates when page content is processed by Twig and the configuration allows undefined PHP functions to be registered

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.