Daily brief, Thursday, November 27, 2025

Nov 26, 7:00 PM to Nov 27, 7:00 PM ET

Generated Nov 9, 2026, 7:09 AM ET

0	0	0	9	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

9 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

No CVEs added to CISA's known-exploited list.

New public exploit code

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

New critical CVEs 9

9.3 **CVE-2025-8890**

Firmware in SDMC NE6037 routers prior to version 7.1.12.2.44 has a network diagnostics tool vulnerable to a shell command injection attacks. In order to exploit this vulnerability, an attacker has to log in to the router's administrative portal, which by defau

9.8 **CVE-2025-13539**

The FindAll Membership plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 1.0.4. This is due to the plugin not properly logging in a user with the data that was previously verified through the 'findall_membership_

9.9 **CVE-2025-12421** Mattermost mattermost server

Mattermost versions 11.0.x <= 11.0.2, 10.12.x <= 10.12.1, 10.11.x <= 10.11.4, 10.5.x <= 10.5.12 fail to to verify that the token used during the code exchange originates from the same authentication flow, which allows an authenticated user to perform account t

9.3 **CVE-2025-12140**

The application contains an insecure 'redirectToUrl' mechanism that incorrectly processes the value of the 'redirectUrlParameter' parameter. The application interprets the entered string of characters as a Java expression, allowing an unauthenticated attacer t

9.8 **CVE-2025-13538**

The FindAll Listing plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.0.5. This is due to the 'findall_listing_user_registration_additional_params' function not restricting what user roles a user can register wi

9.8 **CVE-2025-13540**

The Tiare Membership plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.2. This is due to the 'tiare_membership_init_rest_api_register' function not restricting what user roles a user can register with. This make

9.8 **CVE-2025-13675**

The Tiger theme for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 101.2.1. This is due to the 'paypal-submit.php' file not restricting what user roles a user can register with. This makes it possible for unauthenticated

9.9 **CVE-2025-12419** Mattermost mattermost server

Mattermost versions 10.12.x <= 10.12.1, 10.11.x <= 10.11.4, 10.5.x <= 10.5.12, 11.0.x <= 11.0.3 fail to properly validate OAuth state tokens during OpenID Connect authentication which allows an authenticated attacker with team creation privileges to take over

9.2 **CVE-2024-5539**

The Access Control Bypass vulnerability found in ALC WebCTRL and Carrier i-Vu in versions up to and including 8.5 allows a malicious actor to bypass intended access restrictions and expose sensitive information via the web based building automation server.

Ransomware

No leak-site posts collected.

New data breaches 1

China Software Developer Network csdn.net 6,414,990 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.