Daily brief, Tuesday, November 11, 2025

Nov 10, 7:00 PM to Nov 11, 7:00 PM ET

Generated Nov 9, 2026, 9:43 AM ET

0	0	0	15	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

15 new critical CVEs.

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

15

9.8 **CVE-2025-60724** Microsoft 365 copilot

Heap-based buffer overflow in Microsoft Graphics Component allows an unauthorized attacker to execute code over a network.

9.8 **CVE-2025-13021** Mozilla firefox

+1 more CVEs in the same release

Incorrect boundary conditions in the Graphics: WebGPU component. This vulnerability was fixed in Firefox 145 and Thunderbird 145.

9.8 **CVE-2025-13023** Mozilla firefox

+1 more CVEs in the same release

Sandbox escape due to incorrect boundary conditions in the Graphics: WebGPU component. This vulnerability was fixed in Firefox 145 and Thunderbird 145.

9.8 **CVE-2025-13024** Mozilla firefox

JIT miscompilation in the JavaScript Engine: JIT component. This vulnerability was fixed in Firefox 145 and Thunderbird 145.

9.8 **CVE-2025-8324**

Zohocorp ManageEngine Analytics Plus versions 6170 and below are vulnerable to Unauthenticated SQL Injection due to the improper filter configuration.

10.0 **CVE-2025-12539**

The TNC Toolbox: Web Performance plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.4.2. This is due to the plugin storing cPanel API credentials (hostname, username, and API key) in files within the we

9.8 **CVE-2025-12813**

The Holiday class post calendar plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 7.1 via the 'contents' parameter. This is due to a lack of sanitization of user-supplied data when creating a cache file. This mak

9.8 **CVE-2025-11170**

The WP????????? for CPI plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the Cpiwm_Import_Controller::import function in all versions up to, and including, 1.0.2. This makes it possible for unauthenticated att

10.0 **CVE-2025-42890**

SQL Anywhere Monitor (Non-GUI) baked credentials into the code,exposing the resources or functionality to unintended users and providing attackers with the possibility of arbitrary code execution.This could cause high impact on confidentiality integrity and av

9.9 **CVE-2025-42887**

Due to missing input sanitation, SAP Solution Manager allows an authenticated attacker to insert malicious code when calling a remote-enabled function module. This could provide the attacker with full control of the system hence leading to high impact on confi

9.8 **CVE-2025-11457**

The EasyCommerce – AI-Powered, Fast & Beautiful WordPress Ecommerce Plugin plugin for WordPress is vulnerable to Privilege Escalation in versions 0.9.0-beta2 to 1.8.2. This is due to the /easycommerce/v1/orders REST API endpoint not properly restricting the ab

9.8 **CVE-2017-20210** Qnap photo station

Photo Station 5.4.1 & 5.2.7 include the security fix for the vulnerability related to the XMR mining programs identified by internal research.

9.9 **CVE-2025-13032** Avast antivirus

Double fetch in sandbox kernel driver in Avast/AVG Antivirus <25.3 on windows allows local attacker to escalate privelages via pool overflow.

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.