Daily brief, Wednesday, November 12, 2025

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

Generated Nov 9, 2026, 9:30 AM ET

0	3	0	15	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

3 newly exploited, 15 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

3

9.3 **CVE-2025-9242** WatchGuard Firebox CISA KEV

A remote unauthenticated attacker can execute arbitrary code through an out-of-bounds write in the iked process of WatchGuard Firebox.

9.1 **CVE-2025-12480** Gladinet Triofox CISA KEV DETECTION

Improper access control in Gladinet Triofox lets an attacker reach initial setup pages after setup is complete, bypassing the intended restriction on those pages.

7.0 **CVE-2025-62215** Microsoft Windows CISA KEV

A local attacker with low-level privileges escalates to SYSTEM in the Microsoft Windows Kernel via a race condition.

New public exploit code

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

New critical CVEs

15

9.1 **CVE-2025-12480** Gladinet Triofox KEV EXPLOIT CODE DETECTION

Improper access control in Gladinet Triofox lets an attacker reach initial setup pages after setup is complete, bypassing the intended restriction on those pages.

9.3 **CVE-2025-9242** WatchGuard Firebox KEV EXPLOIT CODE

A remote unauthenticated attacker can execute arbitrary code through an out-of-bounds write in the iked process of WatchGuard Firebox.

9.3 **CVE-2021-4464**

FiberHome AN5506-04-FA firmware versions up to and including RP2631 and HG6245D prior to RP2602 contain a stack-based buffer overflow, as the HTTP service ('webs') fails to enforce maximum lengths for Cookie header values. When a cookie longer than 511 bytes i

9.8 **CVE-2025-63353** Fiberhome hg6145f1 firmware

A vulnerability in FiberHome GPON ONU HG6145F1 RP4423 allows the device's factory default Wi-Fi password (WPA/WPA2 pre-shared key) to be predicted from the SSID. The device generates default passwords using a deterministic algorithm that derives the router pas

9.8 **CVE-2025-12870** Aenrich a\+hrd

The a+HRD developed by aEnrich has an Authentication Abuse vulnerability, allowing unauthenticated remote attackers to send crafted packets to obtain administrator access tokens and use them to access the system with elevated privileges.

9.8 **CVE-2025-11367** N-Able n-central

The N-central Software Probe < 2025.4 is vulnerable to Remote Code Execution via deserialization

9.8 **CVE-2025-12871** Aenrich a\+hrd

The a+HRD developed by aEnrich has an Authentication Abuse vulnerability, allowing unauthenticated remote attackers to craft administrator access tokens and use them to access the system with elevated privileges.

9.8 **CVE-2025-11366** N-Able n-central

N-central < 2025.4 is vulnerable to authentication bypass via path traversal

9.8 **CVE-2025-63666** Tenda ac15 firmware

Tenda AC15 v15.03.05.18_multi) issues an authentication cookie that exposes the account password hash to the client and uses a short, low-entropy suffix as the session identifier. An attacker with network access or the ability to run JS in a victim browser can

9.8 **CVE-2025-40176**

In the Linux kernel, the following vulnerability has been resolved: tls: wait for pending async decryptions if tls_strp_msg_hold fails Async decryption calls tls_strp_msg_hold to create a clone of the input skb to hold references to the memory it uses. If we f

9.8 **CVE-2025-64281** Centralsquare community development

An Authentication Bypass issue in CentralSquare Community Development 19.5.7 allows attackers to access the admin panel without admin credentials.

9.1 **CVE-2025-46608** Dell data lakehouse

Dell Data Lakehouse, versions prior to 1.6.0.0, contain(s) an Improper Access Control vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Elevation of privileges. This vulnerability is considere

9.8 **CVE-2025-56385** Wellsky harmony

A SQL injection vulnerability exists in the login functionality of WellSky Harmony version 4.1.0.2.83 within the 'xmHarmony.asp' endpoint. User-supplied input to the 'TXTUSERID' parameter is not properly sanitized before being incorporated into a SQL query. Su

9.8 **CVE-2025-64280** Centralsquare community development

A SQL Injection Vulnerability in CentralSquare Community Development 19.5.7 allows attackers to inject SQL via the permit_no field.

9.1 **CVE-2025-63289** Sogexia sogexia

Sogexia Android App Compile Affected SDK v35, Max SDK 32 and fixed in v36, was discovered to contain hardcoded encryption keys in the encryption_helper.dart file

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.