# Daily brief, Thursday, December 11, 2025

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

Generated Nov 9, 2026, 4:50 AM ET

| 0 | 1 | 0 | 23 | 0 | 0 |
|---|---|---|---|---|---|
| Breaking | Newly exploited | Exploit code | Critical CVEs | Ransomware posts | New breaches |

1 newly exploited, 23 new critical CVEs.

## Breaking

*Nothing spreading fast in technology large companies run.*

## Newly exploited in the wild

1

8.2 **CVE-2025-58360** OSGeo GeoServer CISA KEV DETECTION

An attacker can define external XML entities in requests to the /geoserver/wms GetMap operation of OSGeo GeoServer, an XML external entity (XXE) reference flaw.

## New public exploit code

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

## New critical CVEs

23

9.8 **CVE-2025-36937** Google android

In AudioDecoder::HandleProduceRequest of audio_decoder.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exp

9.8 **CVE-2025-14534** Utt 512w firmware DETECTION

A vulnerability was determined in UTT ?? 512W up to 3.1.7.7-171114. This impacts the function strcpy of the file /goform/formNatStaticMap of the component Endpoint. Executing manipulation of the argument NatBind can lead to buffer overflow. The attack can be l

9.8 **CVE-2025-14535** Utt 512w firmware DETECTION

A vulnerability was identified in UTT ?? 512W up to 3.1.7.7-171114. Affected is the function strcpy of the file /goform/formConfigFastDirectionW. The manipulation of the argument ssid leads to buffer overflow. The attack may be initiated remotely. The exploit

9.6 **CVE-2025-67511** Aliasrobotics cybersecurity ai

Cybersecurity AI (CAI) is an open-source framework for building and deploying AI-powered offensive and defensive automation. Versions 0.5.9 and below are vulnerable to Command Injection through the run_ssh_command_with_credentials() function, which is availabl

9.3 **CVE-2024-58286**

dizqueTV 1.5.3 contains a remote code execution vulnerability that allows attackers to inject arbitrary commands through the FFMPEG Executable Path settings. Attackers can modify the executable path with shell commands to read system files like /etc/passwd by

9.2 **CVE-2024-58298**

Compuware iStrobe Web 20.13 contains a pre-authentication remote code execution vulnerability that allows unauthenticated attackers to upload malicious JSP files through a path traversal in the file upload form. Attackers can exploit the 'fileName' parameter t

9.1 **CVE-2025-13780** Pgadmin pgadmin 4

pgAdmin versions up to 9.10 are affected by a Remote Code Execution (RCE) vulnerability that occurs when running in server mode and performing restores from PLAIN-format dump files. This issue allows attackers to inject and execute arbitrary commands on the se

10.0 **CVE-2025-64721** Sandboxie-Plus sandboxie

Sandboxie is a sandbox-based isolation software for 32-bit and 64-bit Windows NT-based operating systems. In versions 1.16.6 and below, the SYSTEM-level service SbieSvc.exe exposes SbieIniServer::RC4Crypt to sandboxed processes. The handler adds a fixed header

9.8 **CVE-2025-66043** Libbiosig Project libbiosig

**+5 more CVEs in the same release**

Several stack-based buffer overflow vulnerabilities exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.1. A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger these vu

9.8 **CVE-2024-58308** Opensolution quick cms

Quick.CMS 6.7 contains a SQL injection vulnerability that allows unauthenticated attackers to bypass login authentication by manipulating the login form. Attackers can inject specific SQL payloads like ' or '1'='1 to gain unauthorized administrative access to

9.8 **CVE-2024-58309** Xbtitfm xbtitfm

xbtitFM 4.1.18 contains an unauthenticated SQL injection vulnerability that allows remote attackers to manipulate database queries by injecting malicious SQL code through the msgid parameter. Attackers can send crafted requests to /shoutedit.php with EXTRACTVA

9.1 **CVE-2025-65473** Easyimages2.0 Project easyimages2.0

An arbitrary file rename vulnerability in the /admin/filer.php component of EasyImages 2.0 v2.8.6 and below allows attackers with Administrator privileges to execute arbitrary code via injecting a crafted payload into an uploaded file name.

9.8 **CVE-2025-65474** Easyimages2.0 Project easyimages2.0

An arbitrary file rename vulnerability in the /admin/manager.php component of EasyImages 2.0 v2.8.6 and below allows attackers to execute arbitrary code via renaming a PHP file to a SVG format.

9.1 **CVE-2025-14265** Connectwise screenconnect

In versions of ScreenConnect™ prior to 25.8, server-side validation and integrity checks within the extension subsystem could allow the installation and execution of untrusted or arbitrary extensions by authorized or administrative users. Abuse of this behavio

9.3 **CVE-2024-58290**

Xhibiter NFT Marketplace 1.10.2 contains a SQL injection vulnerability in the collections endpoint that allows attackers to manipulate database queries through the 'id' parameter. Attackers can exploit boolean-based, time-based, and UNION-based SQL injection t

9.1 **CVE-2025-66589** Azeotech daqfactory

In AzeoTech DAQFactory release 20.7 (Build 2555), an Out-of-bounds Read vulnerability can be exploited by an attacker to cause the program to read data past the end of an allocated buffer. This could allow an attacker to disclose information or cause a system

9.8 **CVE-2025-13764**

The WP CarDealer plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.2.16. This is due to the 'WP_CarDealer_User::process_register' function not restricting what user roles a user can register with. This makes it

9.3 **CVE-2024-58301**

Purei CMS 1.0 contains a time-based blind SQL injection vulnerability that allows attackers to manipulate database queries through unfiltered user input parameters. Attackers can exploit vulnerable endpoints like getAllParks.php and events-ajax.php by injectin

## 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.