Daily brief, Friday, December 19, 2025

Dec 18, 7:00 PM to Dec 19, 7:00 PM ET

Generated Nov 9, 2026, 3:46 AM ET

0	1	0	13	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 13 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

9.3 **CVE-2025-14733** WatchGuard Firebox CISA KEV

Unauthenticated remote attacker gets code execution via out-of-bounds write in WatchGuard Fireware OS iked, hitting IKEv2 mobile user and branch office VPNs.

New public exploit code

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

New critical CVEs

13

9.3 **CVE-2025-14733** WatchGuard Firebox KEV EXPLOIT CODE

Unauthenticated remote attacker gets code execution via out-of-bounds write in WatchGuard Fireware OS iked, hitting IKEv2 mobile user and branch office VPNs.

9.3 **CVE-2025-34433**

AVideo versions 14.3.1 prior to 20.1 contain an unauthenticated remote code execution vulnerability caused by predictable generation of an installation salt using PHP uniqid(). The installation timestamp is exposed via a public endpoint, and a derived hash ide

9.8 **CVE-2025-14964** Totolink t10 firmware

A vulnerability has been found in TOTOLINK T10 4.1.8cu.5083_B20200521. This affects the function sprintf of the file /cgi-bin/cstecgi.cgi. Such manipulation of the argument loginAuthUrl leads to stack-based buffer overflow. The attack may be performed from rem

9.8 **CVE-2023-53948**

Lilac-Reloaded for Nagios 2.0.8 contains a remote code execution vulnerability in the autodiscovery feature that allows attackers to inject arbitrary commands. Attackers can exploit the lack of input filtering in the nmap_binary parameter to execute a reverse

9.8 **CVE-2023-53959** Filezilla-Project filezilla client

FileZilla Client 3.63.1 contains a DLL hijacking vulnerability that allows attackers to execute malicious code by placing a crafted TextShaping.dll in the application directory. Attackers can generate a reverse shell payload using msfvenom and replace the miss

9.8 **CVE-2023-53950**

InnovaStudio WYSIWYG Editor 5.4 contains an unrestricted file upload vulnerability that allows attackers to bypass file extension restrictions through filename manipulation. Attackers can upload malicious ASP shells by using null byte techniques and alternate

9.8 **CVE-2023-53957** Kimai kimai

Kimai 1.30.10 contains a SameSite cookie vulnerability that allows attackers to steal user session cookies through malicious exploitation. Attackers can trick victims into executing a crafted PHP script that captures and writes session cookie information to a

9.6 **CVE-2025-66580** Openagentplatform dive

Dive is an open-source MCP Host Desktop Application that enables integration with function-calling LLMs. A critical Stored Cross-Site Scripting (XSS) vulnerability exists in versions prior to 0.11.1 in the Mermaid diagram rendering component. The application a

9.8 **CVE-2025-63665** Gtedge gt edge ai

An issue in GT Edge AI Community Edition Versions before v2.0.12 allows attackers to execute arbitrary code via injecting a crafted JSON payload into the Prompt window.

9.1 **CVE-2025-1928** Restajet online food delivery system

Improper Restriction of Excessive Authentication Attempts vulnerability in Restajet Information Technologies Inc. Online Food Delivery System allows Password Recovery Exploitation. This issue affects Online Food Delivery System: through 19122025. NOTE: The ven

9.8 **CVE-2023-53951**

Ever Gauzy v0.281.9 contains a JWT authentication vulnerability that allows attackers to exploit weak HMAC secret key implementation. Attackers can leverage the exposed JWT token to authenticate and gain unauthorized access with administrative permissions.

9.1 **CVE-2024-49587**

Glutton V1 service endpoints were exposed without any authentication on Gotham stacks, this could have allowed users that did not have any permission to hit glutton backend directly and read/update/delete data. The affected service has been patched and automat

9.8 **CVE-2025-58053** Galette galette

Galette is a membership management web application for non profit organizations. Prior to version 1.2.0, while updating any existing account with a self forged POST request, one can gain higher privileges. Version 1.2.0 fixes the issue.

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.