Daily brief, Monday, December 8, 2025

Dec 7, 7:00 PM to Dec 8, 7:00 PM ET

Generated Nov 9, 2026, 5:26 AM ET

0	2	0	11	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 newly exploited, 11 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

2

9.8 **CVE-2022-37055** D-Link Routers CISA KEV DETECTION

A buffer overflow in D-Link routers gives an attacker high-impact compromise of confidentiality, integrity, and availability; affected products are end-of-life and end-of-service.

7.2 **CVE-2025-66644** Array Networks ArrayOS AG CISA KEV

An attacker can execute arbitrary OS commands on Array Networks ArrayOS AG through an OS command injection flaw.

New public exploit code

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

New critical CVEs

11

9.8 **CVE-2022-37055** D-Link Routers KEV DETECTION

A buffer overflow in D-Link routers gives an attacker high-impact compromise of confidentiality, integrity, and availability; affected products are end-of-life and end-of-service.

9.8 **CVE-2025-48626** Google android

In multiple locations, there is a possible way to launch an application from the background due to a precondition check failure. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed fo

9.1 **CVE-2025-61318** Emlog emlog

Emlog Pro 2.5.20 has an arbitrary file deletion vulnerability. This vulnerability stems from the admin/template.php component and the admin/plugin.php component. They fail to perform path verification and dangerous code filtering for deletion parameters, allow

9.8 **CVE-2025-27020** Nokia infinera mtc-9 firmware

Improper configuration of the SSH service in Infinera MTC-9 allows an unauthenticated attacker to execute arbitrary commands and access data on file system . This issue affects MTC-9: from R22.1.1.0275 before R23.0.

9.8 **CVE-2025-27019** Nokia infinera mtc-9 firmware

Remote shell service (RSH) in Infinera MTC-9 version R22.1.1.0275 allows an attacker to utilize password-less user accounts and obtain system access by activating a reverse shell.This issue affects MTC-9: from R22.1.1.0275 before R23.0.

9.8 **CVE-2025-40320**

In the Linux kernel, the following vulnerability has been resolved: smb: client: fix potential cfid UAF in smb2_query_info_compound When smb2_query_info_compound() retries, a previously allocated cfid may have been freed in the first attempt. Because cfid wasn

9.1 **CVE-2025-65548** Cashu nutshell

NUT-14 allows cashu tokens to be created with a preimage hash. However, nutshell (cashubtc/nuts) before 0.18.0 do not validate the size of preimage when the token is spent. The preimage is stored by the mint and attacker can exploit this vulnerability to fill

9.8 **CVE-2023-53751**

In the Linux kernel, the following vulnerability has been resolved: cifs: fix potential use-after-free bugs in TCP_Server_Info::hostname TCP_Server_Info::hostname may be updated once or many times during reconnect, so protect its access outside reconnect path

9.8 **CVE-2025-64081** Pamzey patients waiting area queue management system

SQL injection vulnerability in /php/api_patient_schedule.php in SourceCodester Patients Waiting Area Queue Management System v1 allows attackers to execute arbitrary SQL commands via the appointmentID parameter.

9.1 **CVE-2025-65849**

A cryptanalytic break in Altcha Proof-of-Work obfuscation mode version 0.8.0 and later allows for remote visitors to recover the Proof-of-Work nonce in constant time via mathematical deduction. NOTE: this is disputed by the Supplier because the product's objec

9.3 **CVE-2023-53769**

In the Linux kernel, the following vulnerability has been resolved: virt/coco/sev-guest: Double-buffer messages The encryption algorithms read and write directly to shared unencrypted memory, which may leak information as well as permit the host to tamper with

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.