Daily brief, Tuesday, December 9, 2025

Dec 8, 7:00 PM to Dec 9, 7:00 PM ET

Generated Nov 9, 2026, 5:12 AM ET

0	2	0	38	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 newly exploited, 38 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

2

7.8 **CVE-2025-62221** Microsoft Windows CISA KEV

A local attacker with authorization on Microsoft Windows can exploit a use-after-free in the Cloud Files Mini Filter Driver to elevate privileges.

7.8 **CVE-2025-6218** RARLAB WinRAR CISA KEV DETECTION

A path traversal flaw in RARLAB WinRAR lets an attacker execute code in the context of the current user.

New public exploit code

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

New critical CVEs

38

9.6 **CVE-2025-10573** Ivanti endpoint manager DETECTION

Stored XSS in Ivanti Endpoint Manager prior to version 2024 SU4 SR1 allows a remote unauthenticated attacker to execute arbitrary JavaScript in the context of an administrator session. User interaction is required.

9.8 **CVE-2025-59719** Fortinet fortiweb

An improper verification of cryptographic signature vulnerability in Fortinet FortiWeb 8.0.0, FortiWeb 7.6.0 through 7.6.4, FortiWeb 7.4.0 through 7.4.9 may allow an unauthenticated attacker to bypass the FortiCloud SSO login authentication via a crafted SAML

9.8 **CVE-2025-66631** Cslanet csla .net

CSLA .NET is a framework designed for the development of reusable, object-oriented business layers for applications. Versions 5.5.4 and below allow the use of WcfProxy. WcfProxy uses the now-obsolete NetDataContractSerializer (NDCS) and is vulnerable to remote

9.8 **CVE-2025-14321** Mozilla firefox

Use-after-free in the WebRTC: Signaling component. This vulnerability was fixed in Firefox 146, Firefox ESR 140.6, Thunderbird 146, and Thunderbird 140.6.

9.8 **CVE-2025-14324** Mozilla firefox

JIT miscompilation in the JavaScript Engine: JIT component. This vulnerability was fixed in Firefox 146, Firefox ESR 115.31, Firefox ESR 140.6, Thunderbird 146, and Thunderbird 140.6.

9.8 **CVE-2025-14330** Mozilla firefox

JIT miscompilation in the JavaScript Engine: JIT component. This vulnerability was fixed in Firefox 146, Firefox ESR 140.6, Thunderbird 146, and Thunderbird 140.6.

9.8 **CVE-2025-14326** Mozilla firefox

Use-after-free in the Audio/Video: GMP component. This vulnerability was fixed in Firefox 146 and Thunderbird 146.

9.1 **CVE-2025-42928**

Under certain conditions, a high privileged user could exploit a deserialization vulnerability in SAP jConnect to launch remote code execution. The system may be vulnerable when specially crafted input is used to exploit the vulnerability resulting in high imp

9.9 **CVE-2025-42880**

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-2025-66039** Sangoma freepbx DETECTION

FreePBX Endpoint Manager is a module for managing telephony endpoints in FreePBX systems. Versions are vulnerable to authentication bypass when the authentication type is set to "webserver." When providing an Authorization header with an arbitrary value, a ses

9.8 **CVE-2021-47728** Selea izero box full firmware

Selea Targa IP OCR-ANPR Camera contains an unauthenticated command injection vulnerability in utils.php that allows remote attackers to execute arbitrary shell commands. Attackers can exploit the 'addr' and 'port' parameters to inject commands and gain www-dat

9.1 **CVE-2025-14306** Robocode robocode

A directory traversal vulnerability exists in the CacheCleaner component of Robocode version 1.9.3.6. The recursivelyDelete method fails to properly sanitize file paths, allowing attackers to traverse directories and delete arbitrary files on the system. This

9.8 **CVE-2023-53771** Minidvblinux minidvblinux

MiniDVBLinux 5.4 contains an authentication bypass vulnerability that allows remote attackers to change the root password without authentication. Attackers can send crafted POST requests to the system setup endpoint with modified SYSTEM_PASSWORD parameters to

9.3 **CVE-2025-34414**

Entrust Instant Financial Issuance (IFI) On Premise software (formerly referred to as CardWizard) versions 5.x, prior to 6.10.5, and prior to 6.11.1 contain an insecure .NET Remoting exposure in the Legacy Remoting Service that is enabled by default. The servi

9.8 **CVE-2023-53774** Minidvblinux minidvblinux

MiniDVBLinux 5.4 contains a remote code execution vulnerability in the SVDRP protocol that allows remote attackers to send commands to manipulate TV systems. Attackers can send crafted SVDRP commands through the svdrpsend.sh script to execute messages and pote

9.8 **CVE-2025-67489**

@vitejs/plugin-rs provides React Server Components (RSC) support for Vite. Versions 0.5.5 and below are vulnerable to arbitrary remote code execution on the development server through unsafe dynamic imports in server function APIs (loadServerAction, decodeRepl

9.8 **CVE-2022-50666**

In the Linux kernel, the following vulnerability has been resolved: RDMA/siw: Fix QP destroy to wait for all references dropped. Delay QP destroy completion until all siw references to QP are dropped. The calling RDMA core will free QP structure after successf

9.8 **CVE-2025-40343**

In the Linux kernel, the following vulnerability has been resolved: nvmet-fc: avoid scheduling association deletion twice When forcefully shutting down a port via the configfs interface, nvmet_port_subsys_drop_link() first calls nvmet_port_del_ctrls() and then

9.8 **CVE-2025-65882** Openmptcprouter openmptcprouter

An issue was discovered in openmptcprouter thru 0.64 in file common/package/utils/sys-upgrade-helper/src/tools/sysupgrade.c in function create_xor_ipad_opad allowing attackers to potentially write arbitrary files or execute arbitrary commands.

9.9 **CVE-2023-53739**

Tinycontrol LAN Controller v3 LK3 version 1.58a contains an unauthenticated vulnerability that allows remote attackers to download configuration backup files containing sensitive credentials. Attackers can retrieve the lk3_settings.bin file and extract base64-

18 more critical CVEs in this window: see the dashboard

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.