Daily brief, Wednesday, December 10, 2025

Dec 9, 7:00 PM to Dec 10, 7:00 PM ET

Generated Nov 9, 2026, 5:00 AM ET

0	0	0	33	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

33 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

No CVEs added to CISA's known-exploited list.

New public exploit code

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

New critical CVEs

33

9.8 **CVE-2025-34392** Barracuda rmm DETECTION

Barracuda Service Center, as implemented in the RMM solution, in versions prior to 2025.1.1, does not verify the URL defined in an attacker-controlled WSDL that is later loaded by the application. This can lead to arbitrary file write and remote code execution

9.8 **CVE-2025-13184** Totolink x5000r firmware DETECTION

Unauthenticated Telnet enablement via cstecgi.cgi (auth bypass) leading to unauthenticated root login with a blank password on factory/reset X5000R V9.1.0u.6369_B20230113 (arbitrary command execution). Earlier versions that share the same implementation, may a

9.1 **CVE-2025-61808** Adobe coldfusion

ColdFusion versions 2025.4, 2023.16, 2021.22 and earlier are affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could lead to arbitrary code execution by a high priviledged attacker. Exploitation of this issue does not require us

9.8 **CVE-2025-67506** Pipeshub pipeshub

PipesHub is a fully extensible workplace AI platform for enterprise search and workflow automation. Versions prior to 0.1.0-beta expose POST /api/v1/record/buffer/convert through missing authentication. The endpoint accepts a file upload and converts it to PDF

9.8 **CVE-2025-65294** Aqara hub m2 firmware

Aqara Hub devices including Camera Hub G3 4.1.9_0027, Hub M2 4.3.6_0027, and Hub M3 4.3.6_0025 contain an undocumented remote access mechanism enabling unrestricted remote command execution.

9.1 **CVE-2020-36898** Howfor qihang media web digital signage

QiHang Media Web Digital Signage 3.0.9 contains an unauthenticated file deletion vulnerability in the QH.aspx endpoint that allows remote attackers to delete files without authentication. Attackers can exploit the 'data' parameter by sending a POST request wit

9.8 **CVE-2020-36897** Howfor qihang media web digital signage

QiHang Media Web Digital Signage 3.0.9 contains an unauthenticated remote code execution vulnerability in the QH.aspx file that allows attackers to upload malicious ASPX scripts. Attackers can exploit the file upload functionality by using the 'remotePath' and

9.8 **CVE-2020-36885** Sony snc-dh120t firmware

Sony IPELA Network Camera 1.82.01 contains a stack buffer overflow vulnerability in the ftpclient.cgi endpoint that allows remote attackers to execute arbitrary code. Attackers can exploit the vulnerability by sending a crafted POST request with oversized data

9.1 **CVE-2025-61811** Adobe coldfusion

ColdFusion versions 2025.4, 2023.16, 2021.22 and earlier are affected by an Improper Access Control vulnerability that could result in arbitrary code execution in the context of the current user. A high privileged attacker could leverage this vulnerability to

9.8 **CVE-2020-36902** Medivision medivision digital signage firmware

UBICOD Medivision Digital Signage 1.5.1 contains an authorization bypass vulnerability that allows normal users to escalate privileges by manipulating the 'ft[grp]' parameter. Attackers can send a GET request to /html/user with 'ft[grp]' set to integer value '

9.8 **CVE-2020-36892** Eibiz i-media server digital signage

Eibiz i-Media Server Digital Signage 3.8.0 contains an unauthenticated privilege escalation vulnerability in the updateUser object that allows attackers to modify user roles. Attackers can exploit the /messagebroker/amf endpoint to elevate privileges and take

9.8 **CVE-2023-53740** Dbbroadcast sft dab 015\/c firmware

Screen SFT DAB 1.9.3 contains an authentication bypass vulnerability that allows attackers to change the admin password without providing the current credentials. Attackers can exploit the userManager.cgx endpoint by sending a crafted JSON request with a new M

9.4 **CVE-2025-13607**

A malicious actor can access camera configuration information, including account credentials, without authenticating when accessing a vulnerable URL.

9.3 **CVE-2025-64537** Adobe experience manager

+2 more CVEs in the same release

Adobe Experience Manager versions 6.5.23 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could lead to arbitrary code execution. An attacker could exploit this vulnerability by injecting malicious scripts into a web page t

9.8 **CVE-2025-34393** Barracuda rmm

Barracuda Service Center, as implemented in the RMM solution, in versions prior to 2025.1.1, does not correctly verify the name of an attacker-controlled WSDL service, leading to insecure reflection. This can result in remote code execution through either invo

9.8 **CVE-2025-34394** Barracuda rmm

Barracuda Service Center, as implemented in the RMM solution, in versions prior to 2025.1.1, exposes a .NET Remoting service that is insufficiently protected against deserialization of arbitrary types. This can lead to remote code execution.

9.1 **CVE-2025-61809** Adobe coldfusion

ColdFusion versions 2025.4, 2023.16, 2021.22 and earlier are affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized

9.3 **CVE-2025-13953**

Bypass vulnerability in the authentication method in the GTT Tax Information System application, related to the Active Directory (LDAP) login method. Authentication is performed through a local WebSocket, but the web application does not properly validate the

9.8 **CVE-2025-65602** Chancms chancms

A template injection vulnerability in the /vip/v1/file/save component of ChanCMS v3.3.4 allows attackers to execute arbitrary code via a crafted POST request.

9.1 **CVE-2025-65792** Datagear datagear

DataGear v5.5.0 is vulnerable to Arbitrary File Deletion.

11 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.