Daily brief, Friday, January 9, 2026

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

Generated Nov 9, 2026, 12:19 AM ET

0	0	0	16	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

16 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

16

9.8 **CVE-2026-22584** Salesforce uni2ts

Improper Control of Generation of Code ('Code Injection') vulnerability in Salesforce Uni2TS on MacOS, Windows, Linux allows Leverage Executable Code in Non-Executable Files.This issue affects Uni2TS: through 1.2.0.

9.8 **CVE-2025-70161** Edimax br-6208ac firmware DETECTION

EDIMAX BR-6208AC V2_1.02 is vulnerable to Command Injection. This arises because the pppUserName field is directly passed to a shell command via the system() function without proper sanitization. An attacker can exploit this by injecting malicious commands int

9.8 **CVE-2025-69542** Dlink dir-895la1 firmware

A Command Injection Vulnerability has been discovered in the DHCP daemon service of D-Link DIR895LA1 v102b07. The vulnerability exists in the lease renewal processing logic where the DHCP hostname parameter is directly concatenated into a system command withou

9.8 **CVE-2025-15501** Sangfor operation and maintenance security management system

A vulnerability was determined in Sangfor Operation and Maintenance Management System up to 3.0.8. Impacted is the function WriterHandle.getCmd of the file /isomp-protocol/protocol/getCmd. This manipulation of the argument sessionPath causes os command injecti

9.8 **CVE-2025-15500** Sangfor operation and maintenance management system

A vulnerability was found in Sangfor Operation and Maintenance Management System up to 3.0.8. This issue affects some unknown processing of the file /isomp-protocol/protocol/getHis of the component HTTP POST Request Handler. The manipulation of the argument se

10.0 **CVE-2025-69425**

The Ruckus vRIoT IoT Controller firmware versions prior to 3.0.0.0 (GA) expose a command execution service on TCP port 2004 running with root privileges. Authentication to this service relies on a hardcoded Time-based One-Time Password (TOTP) secret and an emb

10.0 **CVE-2025-64093** Zenitel icx500 firmware

Remote Code Execution vulnerability that allows unauthenticated attackers to inject arbitrary commands into the hostname of the device.

9.3 **CVE-2020-36875**

AccessAlly WordPress plugin versions prior to 3.3.2 contain an unauthenticated arbitrary PHP code execution vulnerability in the Login Widget. The plugin processes the login_error parameter as PHP code, allowing an attacker to supply and execute arbitrary PHP

10.0 **CVE-2025-70974**

Fastjson before 1.2.48 mishandles autoType because, when an @type key is in a JSON document, and the value of that key is the name of a Java class, there may be calls to certain public methods of that class. Depending on the behavior of those methods, there ma

9.8 **CVE-2025-14736**

The Frontend Admin by DynamiApps plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 3.28.29. This is due to insufficient validation of user-supplied role values in the 'validate_value', 'pre_update_value', and 'get

9.8 **CVE-2025-14598** Cloudilyaerp bet e-portal

BeeS Software Solutions BET Portal contains an SQL injection vulnerability in the login functionality of affected sites. The vulnerability enables arbitrary SQL commands to be executed on the backend database.

9.3 **CVE-2025-7072**

The firmware in KAON CG3000TC and CG3000T routers contains hard-coded credentials in clear text (shared across all routers of this model) that an unauthenticated remote attacker could use to execute commands with root privileges. This vulnerability has been fi

10.0 **CVE-2025-64090** Zenitel tcis-3 firmware

This vulnerability allows authenticated attackers to execute commands via the hostname of the device.

10.0 **CVE-2025-69426**

The Ruckus vRIoT IoT Controller firmware versions prior to 3.0.0.0 (GA) contain hardcoded credentials for an operating system user account within an initialization script. The SSH service is network-accessible without IP-based restrictions. Although the config

9.8 **CVE-2025-66050** Vivotek ip7137 firmware

Vivotek IP7137 camera with firmware version 0200a by default dos not require to provide any password when logging in as an administrator. While it is possible to set up such a password, a user is not informed about such a need. The vendor has not replied to th

9.1 **CVE-2025-14741**

The Frontend Admin by DynamiApps plugin for WordPress is vulnerable to missing authorization to unauthorized data modification and deletion due to a missing capability check on the 'delete_object' function in all versions up to, and including, 3.28.25. This ma

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.