Daily brief, Tuesday, January 6, 2026

Jan 5, 7:00 PM to Jan 6, 7:00 PM ET

Generated Nov 9, 2026, 12:40 AM ET

0	0	0	14	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

14 new critical CVEs, 1 new breaches.

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

14

9.8 **CVE-2025-65212** Njhyst hy511 firmware

An issue was discovered in NJHYST HY511 POE core before 2.1 and plugins before 0.1. The vulnerability stems from the device's insufficient cookie verification, allowing an attacker to directly request the configuration file address and download the core config

9.8 **CVE-2020-36923** Sony bravia signage

Sony BRAVIA Digital Signage 1.7.8 contains an insecure direct object reference vulnerability that allows attackers to bypass authorization controls. Attackers can access hidden system resources like '/#/content-creation' by manipulating client-side access rest

9.8 **CVE-2020-36925**

Arteco Web Client DVR/NVR contains a session hijacking vulnerability with insufficient session ID complexity that allows remote attackers to bypass authentication. Attackers can brute force session IDs within a specific numeric range to obtain valid sessions a

9.8 **CVE-2025-60534** Blueaccesstech cobalt x1

Blue Access Cobalt v02.000.195 suffers from an authentication bypass vulnerability, which allows an attacker to selectively proxy requests in order to operate functionality on the web application without the need to authenticate with legitimate credentials.

9.8 **CVE-2025-60262** H3c mc102-g firmware

An issue in H3C M102G HM1A0V200R010 wireless controller and BA1500L SWBA1A0V100R006 wireless access point, there is a misconfiguration vulnerability about vsftpd. Through this vulnerability, all files uploaded anonymously via the FTP protocol is automatically

9.9 **CVE-2025-30996**

Unrestricted Upload of File with Dangerous Type vulnerability in Themify Themify Sidepane WordPress Theme, Themify Themify Newsy, Themify Themify Folo, Themify Themify Edmin, Themify Bloggie, Themify Photobox, Themify Wigi, Themify Rezo, Themify Slide allows U

9.8 **CVE-2026-21675** Color iccdev

iccDEV provides a set of libraries and tools for working with ICC color management profiles. Versions 2.3.1 and below contain a Use After Free vulnerability in the CIccXform::Create() function, where it deletes the hint. This issue is fixed in version 2.3.1.1.

9.8 **CVE-2020-36912**

Plexus anblick Digital Signage Management 3.1.13 contains an open redirect vulnerability in the 'PantallaLogin' script that allows attackers to manipulate the 'pagina' GET parameter. Attackers can craft malicious links that redirect users to arbitrary websites

9.8 **CVE-2025-15001**

The FS Registration Password plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 1.0.1. This is due to the plugin not properly validating a user's identity prior to updating their password. This

9.8 **CVE-2025-14942** Wolfssh wolfssh

wolfSSH’s key exchange state machine can be manipulated to leak the client’s password in the clear, trick the client to send a bogus signature, or trick the client into skipping user authentication. This affects client applications with wolfSSH version 1.4.21

9.8 **CVE-2025-14996**

The AS Password Field In Default Registration Form plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 2.0.0. This is due to the plugin not properly validating a user's identity prior to updatin

9.8 **CVE-2025-39477**

Missing Authorization vulnerability in Sfwebservice InWave Jobs allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects InWave Jobs: from n/a through 3.5.8.

9.8 **CVE-2025-15444** Iamb crypt\

Crypt::Sodium::XS module versions prior to 0.000042, for Perl, include a vulnerable version of libsodium libsodium <= 1.0.20 or a version of libsodium released before December 30, 2025 contains a vulnerability documented as CVE-2025-69277 https://www.cve.org/C

9.8 **CVE-2025-15385** Tecno boomplay

Insufficient Verification of Data Authenticity vulnerability in TECNO Mobile com.Afmobi.Boomplayer allows Authentication Bypass.This issue affects com.Afmobi.Boomplayer: 7.4.63.

Ransomware

No leak-site posts collected.

New data breaches 1

WhiteDate whitedate.net 20,363 accounts

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.