Daily brief, Thursday, January 8, 2026

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

Generated Nov 9, 2026, 12:27 AM ET

0	0	0	34	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

34 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

34

9.0 **CVE-2025-59470** Veeam Backup and Recovery EXPLOIT CODE

Product not on watchlist.

9.0 **CVE-2025-59468** Veeam Backup and Recovery

Product not on watchlist.

9.0 **CVE-2025-59469** Veeam Backup and Recovery

Product not on watchlist.

10.0 **CVE-2026-21858** N8n n8n DETECTION

n8n is an open source workflow automation platform. Versions starting with 1.65.0 and below 1.121.0 enable an attacker to access files on the underlying server through execution of certain form-based workflows. A vulnerable workflow could grant access to an un

9.3 **CVE-2026-21876** Owasp owasp modsecurity core rule set

The OWASP core rule set (CRS) is a set of generic attack detection rules for use with compatible web application firewalls. Prior to versions 4.22.0 and 3.3.8, the current rule 922110 has a bug when processing multipart requests with multiple parts. When the f

9.8 **CVE-2017-20216** DETECTION

FLIR Thermal Camera PT-Series firmware version 8.0.0.64 contains multiple unauthenticated remote command injection vulnerabilities in the controllerFlirSystem.php script. Attackers can execute arbitrary system commands as root by exploiting unsanitized POST pa

9.9 **CVE-2026-21877** N8n n8n DETECTION

n8n is an open source workflow automation platform. In versions 0.121.2 and below, an authenticated attacker may be able to execute malicious code using the n8n service. This could result in full compromise and can impact both self-hosted and n8n Cloud instanc

9.8 **CVE-2025-69258** Trendmicro apex central

A LoadLibraryEX vulnerability in Trend Micro Apex Central could allow an unauthenticated remote attacker to load an attacker-controlled DLL into a key executable, leading to execution of attacker-supplied code under the context of SYSTEM on affected installati

9.4 **CVE-2026-21891** Zimaspace zimaos DETECTION

ZimaOS is a fork of CasaOS, an operating system for Zima devices and x86-64 systems with UEFI. In versions up to and including 1.5.0, the application checks the validity of the username but appears to skip, misinterpret, or incorrectly validate the password wh

9.8 **CVE-2026-21875** Oxygenz clipbucket DETECTION

ClipBucket v5 is an open source video sharing platform. Versions 5.5.2-#187 and below allow an attacker to perform Blind SQL Injection through the add comment section within a channel. When adding a comment within a channel, there is a POST request to the /act

9.8 **CVE-2025-66913** Jeecg jimureport

JimuReport thru version 2.1.3 is vulnerable to remote code execution when processing user-controlled H2 JDBC URLs. The application passes the attacker-supplied JDBC URL directly to the H2 driver, allowing the use of certain directives to execute arbitrary Java

9.8 **CVE-2025-67325** Webkul qloapps

Unrestricted file upload in the hotel review feature in QloApps versions 1.7.0 and earlier allows remote unauthenticated attackers to achieve remote code execution.

9.1 **CVE-2025-56425** Optimal-Systems enaio

An issue was discovered in the AppConnector component version 10.10.0.183 and earlier of enaio 10.10, in the AppConnector component version 11.0.0.183 and earlier of enaio 11.0, and in the AppConnctor component version 11.10.0.183 and earlier of enaio 11.10. T

9.4 **CVE-2025-66916** Dromara ruoyi-vue-plus

The snailjob component in RuoYi-Vue-Plus versions 5.5.1 and earlier, interface /snail-job/workflow/check-node-expression can execute QLExpress expressions, but it does not filter user input, allowing attackers to use the File class to perform arbitrary file re

9.8 **CVE-2026-22034** Jvoisin snuffleupagus

Snuffleupagus is a module that raises the cost of attacks against website by killing bug classes and providing a virtual patching system. On deployments of Snuffleupagus prior to version 0.13.0 with the non-default upload validation feature enabled and configu

9.1 **CVE-2025-68715** Pandawireless pwru01 firmware

An issue was discovered in Panda Wireless PWRU0 devices with firmware 2.2.9 that exposes multiple HTTP endpoints (/goform/setWan, /goform/setLan, /goform/wirelessBasic) that do not enforce authentication. A remote unauthenticated attacker can modify WAN, LAN,

9.8 **CVE-2019-25296**

The WP Cost Estimation plugin for WordPress is vulnerable to arbitrary file uploads and deletion due to missing file type validation in the lfb_upload_form and lfb_removeFile AJAX actions in versions up to, and including, 9.642. This makes it possible for unau

9.4 **CVE-2025-68717** Kaysus ks-wr3600 firmware

KAYSUS KS-WR3600 routers with firmware 1.0.5.9.1 allow authentication bypass during session validation. If any user is logged in, endpoints such as /cgi-bin/system-tool accept unauthenticated requests with empty or invalid session values. This design flaw lets

9.8 **CVE-2025-61548** Edubusinesssolutions print shop pro webdesk

SQL Injection is present on the hfInventoryDistFormID parameter in the /PSP/appNET/Store/CartV12.aspx/GetUnitPrice endpoint in edu Business Solutions Print Shop Pro WebDesk version 18.34 (fixed in 19.69). Unsanitized user input is incorporated directly into SQ

9.1 **CVE-2025-61546** Edubusinesssolutions print shop pro webdesk

There is an issue on the /PSP/appNET/Store/CartV12.aspx/GetUnitPrice endpoint in edu Business Solutions Print Shop Pro WebDesk version 18.34 (fixed in 19.69) that enables remote attacker to create financial discrepancies by purchasing items with a negative qua

14 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.