Daily brief, Wednesday, February 4, 2026

Feb 3, 7:00 PM to Feb 4, 7:00 PM ET

Generated Nov 7, 2026, 7:17 PM ET

0	0	0	18	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

18 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

18

9.9 **CVE-2026-25049** N8n n8n

n8n is an open source workflow automation platform. Prior to versions 1.123.17 and 2.5.2, an authenticated user with permission to create or modify workflows could abuse crafted expressions in workflow parameters to trigger unintended system command execution

9.1 **CVE-2026-25539** B3log siyuan

SiYuan is a personal knowledge management system. Prior to version 3.5.5, the /api/file/copyFile endpoint does not validate the dest parameter, allowing authenticated users to write files to arbitrary locations on the filesystem. This can lead to Remote Code E

9.8 **CVE-2026-25526** Hubspot jinjava

JinJava is a Java-based template engine based on django template syntax, adapted to render jinja templates. Prior to versions 2.7.6 and 2.8.3, JinJava is vulnerable to arbitrary Java execution via bypass through ForTag. This allows arbitrary Java class instant

9.8 **CVE-2026-25505** Bambuddy bambuddy

Bambuddy is a self-hosted print archive and management system for Bambu Lab 3D printers. Prior to version 0.1.7, a hardcoded secret key used for signing JWTs is checked into source code and ManyAPI routes do not check authentication. This issue has been patche

9.6 **CVE-2026-25481** Langroid langroid

Langroid is a framework for building large-language-model-powered applications. Prior to version 0.59.32, there is a bypass to the fix for CVE-2025-46724. TableChatAgent can call pandas_eval tool to evaluate the expression. There is a WAF in langroid/utils/pan

9.8 **CVE-2025-64712** Unstructured unstructured

The unstructured library provides open-source components for ingesting and pre-processing images and text documents, such as PDFs, HTML, Word docs, and many more. Prior to version 0.18.18, a path traversal vulnerability in the partition_msg function allows an

9.9 **CVE-2026-25053** N8n n8n

n8n is an open source workflow automation platform. Prior to versions 1.123.10 and 2.5.0, vulnerabilities in the Git node allowed authenticated users with permission to create or modify workflows to execute arbitrary system commands or read arbitrary files on

10.0 **CVE-2026-1633**

The Synectix LAN 232 TRIO 3-Port serial to ethernet adapter exposes its web management interface without requiring authentication, allowing unauthenticated users to modify critical device settings or factory reset the device.

9.9 **CVE-2026-25115** N8n n8n

n8n is an open source workflow automation platform. Prior to version 2.4.8, a vulnerability in the Python Code node allows authenticated users to break out of the Python sandbox environment and execute code outside the intended security boundary. This issue ha

9.1 **CVE-2026-25139** Riot-Os riot

RIOT is an open-source microcontroller operating system, designed to match the requirements of Internet of Things (IoT) devices and other embedded devices. In version 2025.10 and prior, multiple out-of-bounds read allow any unauthenticated user, with ability t

10.0 **CVE-2025-59818** Zenitel tcis-3 firmware

This vulnerability allows authenticated attackers to execute arbitrary commands on the underlying system using the file name of an uploaded file.

9.8 **CVE-2025-13375**

IBM Common Cryptographic Architecture (CCA) 7.5.52 and 8.4.82 could allow an unauthenticated user to execute arbitrary commands with elevated privileges on the system.

9.2 **CVE-2026-25547**

@isaacs/brace-expansion is a hybrid CJS/ESM TypeScript fork of brace-expansion. Prior to version 5.0.1, @isaacs/brace-expansion is vulnerable to a denial of service (DoS) issue caused by unbounded brace range expansion. When an attacker provides a pattern cont

9.8 **CVE-2025-5329**

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Martcode Software Inc. Delta Course Automation allows SQL Injection. This issue affects Delta Course Automation: through 04022026. NOTE: The vendor was contac

9.8 **CVE-2025-62615** Agpt autogpt platform

+1 more CVEs in the same release

AutoGPT is a platform that allows users to create, deploy, and manage continuous artificial intelligence agents that automate complex workflows. Prior to autogpt-platform-beta-v0.6.34, in RSSFeedBlock, the third-party library urllib.request.urlopen is used dir

9.9 **CVE-2026-25052** N8n n8n

n8n is an open source workflow automation platform. Prior to versions 1.123.18 and 2.5.0, a vulnerability in the file access controls allows authenticated users with permission to create or modify workflows to read sensitive files from the n8n host system. Thi

9.1 **CVE-2026-25160** Alistgo alist

Alist is a file list program that supports multiple storages, powered by Gin and Solidjs. Prior to version 3.57.0, the application disables TLS certificate verification by default for all outgoing storage driver communications, making the system vulnerable to

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.