Daily brief, Thursday, January 22, 2026

Jan 21, 7:00 PM to Jan 22, 7:00 PM ET

Generated Nov 7, 2026, 9:11 PM ET

0	3	0	44	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

3 newly exploited, 44 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild 3

9.2 **CVE-2025-34026** Versa Concerto CISA KEV DETECTION

Attacker reaches Versa Concerto admin endpoints and Actuator heap dumps and trace logs through an authentication flaw in the Traefik reverse proxy configuration.

7.5 **CVE-2025-54313** Prettier eslint-config-prettier CISA KEV

Prettier eslint-config-prettier contains an embedded malicious code vulnerability. Installing an affected package executes an install.js file that launches the node-gyp.dll malware on Windows.

5.3 **CVE-2025-31125** Vite Vitejs CISA KEV DETECTION

Attacker reads non-allowed files via ?inline&import or ?raw?import in Vite dev servers exposed to the network with --host or server.host.

1 older CVE (published more than 7 days earlier) added to KEV, below the bar (CVSS under 9, not widely used enterprise tech): CVE-2025-68645 (8.8)

New public exploit code

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

New critical CVEs 44

9.2 **CVE-2025-34026** Versa Concerto KEV EXPLOIT CODE DETECTION

Attacker reaches Versa Concerto admin endpoints and Actuator heap dumps and trace logs through an authentication flaw in the Traefik reverse proxy configuration.

9.3 **CVE-2026-24307** Microsoft 365 copilot

Improper validation of specified type of input in M365 Copilot allows an unauthorized attacker to disclose information over a network.

9.8 **CVE-2026-24306** Microsoft azure front door

Improper access control in Azure Front Door (AFD) allows an unauthorized attacker to elevate privileges over a network.

9.8 **CVE-2026-24124** Linuxfoundation dragonfly

Dragonfly is an open source P2P-based file distribution and image acceleration system. In versions 2.4.1-rc.0 and below, the Job API endpoints (/api/v1/jobs) lack JWT authentication middleware and RBAC authorization checks in the routing configuration. This al

9.3 **CVE-2026-24305** Microsoft entra id

Azure Entra ID Elevation of Privilege Vulnerability

9.8 **CVE-2026-0920**

The LA-Studio Element Kit for Elementor plugin for WordPress is vulnerable to Administrative User Creation in all versions up to, and including, 1.5.6.3. This is due to the 'ajax_register_handle' function not restricting what user roles a user can register wit

9.8 **CVE-2025-69764** Tenda ax3 firmware

Tenda AX3 firmware v16.03.12.11 contains a stack-based buffer overflow in the formGetIptv function due to improper handling of the stbpvid stack buffer, which may result in memory corruption and remote code execution.

9.8 **CVE-2025-67617**

Deserialization of Untrusted Data vulnerability in themeton Consult Aid consultaid allows Object Injection.This issue affects Consult Aid: from n/a through <= 1.4.3.

9.8 **CVE-2026-1331** Hamastar meetinghub paperless meetings

MeetingHub developed by HAMASTAR Technology has an Arbitrary File Upload vulnerability, allowing unauthenticated remote attackers to upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.

10.0 **CVE-2025-68001**

Unrestricted Upload of File with Dangerous Type vulnerability in garidium g-FFL Checkout g-ffl-checkout allows Upload a Web Shell to a Web Server.This issue affects g-FFL Checkout: from n/a through <= 2.1.0.

9.4 **CVE-2026-24042** Appsmith appsmith

Appsmith is a platform to build admin panels, internal tools, and dashboards. In versions 1.94 and below, publicly accessible apps allow unauthenticated users to execute unpublished (edit-mode) actions by sending viewMode=false (or omitting it) to POST /api/v1

10.0 **CVE-2025-50002**

Unrestricted Upload of File with Dangerous Type vulnerability in Farost Energia energia allows Upload a Web Shell to a Web Server.This issue affects Energia: from n/a through <= 1.1.2.

9.8 **CVE-2025-69101**
Authentication Bypass Using an Alternate Path or Channel vulnerability in AmentoTech Workreap Core workreap_core allows Authentication Abuse.This issue affects Workreap Core: from n/a through <= 3.4.1.

9.1 **CVE-2025-67944**
Improper Control of Generation of Code ('Code Injection') vulnerability in Nelio Software Nelio AB Testing nelio-ab-testing allows Code Injection.This issue affects Nelio AB Testing: from n/a through <= 8.1.8.

9.8 **CVE-2026-24058** Charm soft serve
Soft Serve is a self-hostable Git server for the command line. Versions 0.11.2 and below have a critical authentication bypass vulnerability that allows an attacker to impersonate any user (including admin) by "offering" the victim's public key during the SSH

9.9 **CVE-2025-68909**
Unrestricted Upload of File with Dangerous Type vulnerability in blazethemes Blogistic blogistic allows Using Malicious Files.This issue affects Blogistic: from n/a through <= 1.0.5.

9.9 **CVE-2025-68910**
Unrestricted Upload of File with Dangerous Type vulnerability in blazethemes Blogzee blogzee allows Using Malicious Files.This issue affects Blogzee: from n/a through <= 1.0.5.

9.0 **CVE-2026-23873** Hustoj hustoj
hustoj is an open source online judge based on PHP/C++/MySQL/Linux for ACM/ICPC and NOIP training. All versions are vulnerable to CSV Injection (Formula Injection) through the contest rank export functionality (contestrank.xls.php and admin/ranklist_export.php

9.9 **CVE-2025-67968**
Unrestricted Upload of File with Dangerous Type vulnerability in InspiryThemes Real Homes CRM realhomes-crm allows Using Malicious Files.This issue affects Real Homes CRM: from n/a through <= 1.0.0.

10.0 **CVE-2025-69828**
File Upload vulnerability in TMS Global Software TMS Management Console v.6.3.7.27386.20250818 allows a remote attacker to execute arbitrary code via the Logo upload in /Customer/AddEdit

24 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.