Daily brief, Wednesday, January 21, 2026

Jan 20, 7:00 PM to Jan 21, 7:00 PM ET

Generated Nov 7, 2026, 9:23 PM ET

0	1	0	12	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 12 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

8.2 **CVE-2026-20045** Cisco Unified Communications Manager CISA KEV

Code injection flaw in Cisco Unified Communications Manager and Unity Connection lets an attacker inject code into these products.

New public exploit code

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

New critical CVEs

12

9.8 **CVE-2021-47851** Yodinfo mini mouse

Mini Mouse 9.2.0 contains a remote code execution vulnerability that allows attackers to execute arbitrary commands through an unauthenticated HTTP endpoint. Attackers can leverage the /op=command endpoint to download and execute payloads by sending crafted JS

9.8 **CVE-2021-47748** Hasura graphql engine

Hasura GraphQL 1.3.3 contains a remote code execution vulnerability that allows attackers to execute arbitrary shell commands through SQL query manipulation. Attackers can inject commands into the run_sql endpoint by crafting malicious GraphQL queries that exe

9.8 **CVE-2021-47854**

DD-WRT version 45723 contains a buffer overflow vulnerability in the UPNP network discovery service that allows remote attackers to potentially execute arbitrary code. Attackers can send crafted M-SEARCH packets with oversized UUID payloads to trigger buffer o

9.8 **CVE-2026-23524** Laravel reverb

Laravel Reverb provides a real-time WebSocket communication backend for Laravel applications. In versions 1.6.3 and below, Reverb passes data from the Redis channel directly into PHP's unserialize() function without restricting which classes can be instantiate

9.8 **CVE-2025-69762** Tenda ax3 firmware

Tenda AX3 firmware v16.03.12.11 contains a stack overflow in formSetIptv via the list parameter, which can cause memory corruption and enable remote code execution.

9.8 **CVE-2025-69763** Tenda ax3 firmware

Tenda AX3 firmware v16.03.12.11 contains a stack overflow in formSetIptv via the vlanId parameter, which can cause memory corruption and enable remote code execution.

9.6 **CVE-2026-22792** 5ire 5ire

+1 more CVEs in the same release

5ire is a cross-platform desktop artificial intelligence assistant and model context protocol client. Prior to version 0.15.3, an unsafe HTML rendering permits untrusted HTML (including on* event attributes) to execute in the renderer context. An attacker can

9.8 **CVE-2025-69766** 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 citytag stack buffer, which may result in memory corruption and remote code execution.

9.8 **CVE-2021-47875**

GeoGebra CAS Calculator 6.0.631.0 contains a denial of service vulnerability that allows attackers to crash the application by generating a large buffer overflow. Attackers can create a payload with 8000 repeated characters and paste it into the calculator's i

9.8 **CVE-2025-15521**

The Academy LMS – WordPress LMS Plugin for Complete eLearning Solution plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 3.5.0. This is due to the plugin not properly validating a user's ident

9.8 **CVE-2026-23518** Fleetdm fleet

Fleet is open source device management software. In versions prior to 4.78.3, 4.77.1, 4.76.2, 4.75.2, and 4.53.3, a vulnerability in Fleet's Windows MDM enrollment flow could allow an attacker to submit forged authentication tokens that are not properly valida

Ransomware

No leak-site posts collected.

New data breaches 1

Under Armour underarmour.com 72,742,892 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.