Daily brief, Wednesday, January 28, 2026

Jan 27, 7:00 PM to Jan 28, 7:00 PM ET

Generated Nov 7, 2026, 8:25 PM ET

0	0	0	20	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

20 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

20

9.8 **CVE-2025-40553** Solarwinds web help desk

SolarWinds Web Help Desk was found to be susceptible to an untrusted data deserialization vulnerability that could lead to remote code execution, which would allow an attacker to run commands on the host machine. This could be exploited without authentication.

9.8 **CVE-2025-40554** Solarwinds web help desk DETECTION

SolarWinds Web Help Desk was found to be susceptible to an authentication bypass vulnerability that, if exploited, could allow an attacker to invoke specific actions within Web Help Desk.

9.8 **CVE-2025-40552** Solarwinds web help desk DETECTION

SolarWinds Web Help Desk was found to be susceptible to an authentication bypass vulnerability that if exploited, would allow a malicious actor to execute actions and methods that should be protected by authentication.

9.8 **CVE-2026-1056**

The Snow Monkey Forms plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the 'generate_user_dirpath' function in all versions up to, and including, 12.0.3. This makes it possible for unauthenticated attack

9.8 **CVE-2020-36962** Tendenci tendenci

Tendenci 12.3.1 contains a CSV formula injection vulnerability in the contact form message field that allows attackers to inject malicious formulas during export. Attackers can submit crafted payloads like '=10+20+cmd|' /C calc'!A0' in the message field to tri

10.0 **CVE-2026-24897** Erugo erugo

Erugo is a self-hosted file-sharing platform. In versions up to and including 0.2.14, an authenticated low-privileged user can upload arbitrary files to any specified location due to insufficient validation of user?supplied paths when creating shares. By speci

9.9 **CVE-2026-24841** Dokploy dokploy

Dokploy is a free, self-hostable Platform as a Service (PaaS). In versions prior to 0.26.6, a critical command injection vulnerability exists in Dokploy's WebSocket endpoint `/docker-container-terminal`. The `containerId` and `activeWay` parameters are directl

10.0 **CVE-2026-23830** Nyariv sandboxjs

SandboxJS is a JavaScript sandboxing library. Versions prior to 0.8.26 have a sandbox escape vulnerability due to `AsyncFunction` not being isolated in `SandboxFunction`. The library attempts to sandbox code execution by replacing the global `Function` constru

9.1 **CVE-2025-57794** Explorance blue

Explorance Blue versions prior to 8.14.9 contain an authenticated unrestricted file upload vulnerability in the administrative interface. The application does not adequately restrict uploaded file types, allowing malicious files to be uploaded and executed by

9.9 **CVE-2025-57795** Explorance blue

Explorance Blue versions prior to 8.14.13 contain an authenticated remote file download vulnerability in a web service component. In default configurations, this flaw can be leveraged to achieve remote code execution.

9.8 **CVE-2020-36967**

Zortam Mp3 Media Studio 27.60 contains a buffer overflow vulnerability in the library creation file selection process that allows remote code execution. Attackers can craft a malicious text file with shellcode to trigger a structured exception handler (SEH) ov

9.8 **CVE-2020-36961**

10-Strike Network Inventory Explorer 8.65 contains a buffer overflow vulnerability in exception handling that allows remote attackers to execute arbitrary code. Attackers can craft a malicious file with 209 bytes of padding and a specially constructed Structur

9.8 **CVE-2025-61140** Dchester jsonpath

The value function in jsonpath 1.1.1 lib/index.js is vulnerable to Prototype Pollution.

9.8 **CVE-2020-36964**

YATinyWinFTP contains a denial of service vulnerability that allows attackers to crash the FTP service by sending a 272-byte buffer with a trailing space. Attackers can exploit the service by connecting and sending a malformed command that triggers a buffer ov

10.0 **CVE-2025-57792** Explorance blue

Explorance Blue versions prior to 8.14.9 contain a SQL injection vulnerability caused by insufficient validation of user input in a web application endpoint. An attacker can supply crafted input that is executed as part of backend database queries. The issue i

9.8 **CVE-2026-24857** Simsong bulk extractor

`bulk_extractor` is a digital forensics exploitation tool. Starting in version 1.4, `bulk_extractor`'s embedded unrar code has a heap?buffer?overflow in the RAR PPM LZ decoding path. A crafted RAR inside a disk image causes an out?of?bounds write in `Unpack::C

9.0 **CVE-2026-24769** Nocodb nocodb

NocoDB is software for building databases as spreadsheets. Prior to version 0.301.0, a stored cross-site scripting (XSS) vulnerability exists in NocoDB's attachment handling mechanism. Authenticated users can upload malicious SVG files containing embedded Java

9.1 **CVE-2025-69602** Altumcode 66biolinks

A session fixation vulnerability exists in 66biolinks v62.0.0 by AltumCode, where the application does not regenerate the session identifier after successful authentication. As a result, the same session cookie value is reused for users logging in from the sam

9.1 **CVE-2026-24838** Dnnsoftware dotnetnuke

DNN (formerly DotNetNuke) is an open-source web content management platform (CMS) in the Microsoft ecosystem. Prior to versions 9.13.10 and 10.2.0, module title supports richtext which could include scripts that would execute in certain scenarios. Versions 9.1

9.1 **CVE-2026-24785** Jmlepisto clatter

Clatter is a no_std compatible, pure Rust implementation of the Noise protocol framework with post-quantum support. Versiosn prior to2.2.0 have a protocol compliance vulnerability. The library allowed post-quantum handshake patterns that violated the PSK valid

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.