Daily brief, Tuesday, January 20, 2026

Jan 19, 7:00 PM to Jan 20, 7:00 PM ET

Generated Nov 7, 2026, 9:35 PM ET

0	0	0	16	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

16 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

16

9.8 **CVE-2026-0907** Google chrome

Incorrect security UI in Split View in Google Chrome prior to 144.0.7559.59 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)

9.1 **CVE-2025-55130** Nodejs node.js

A flaw in Node.js's Permissions model allows attackers to bypass `--allow-fs-read` and `--allow-fs-write` restrictions using crafted relative symlink paths. By chaining directories and symlinks, a script granted access only to the current directory can escape

9.9 **CVE-2026-0933** Cloudflare wrangler

SummaryA command injection vulnerability (CWE-78) has been found to exist in the `wrangler pages deploy` command. The issue occurs because the `--commit-hash` parameter is passed directly to a shell command without proper validation or sanitization, allowing a

10.0 **CVE-2026-21636** Nodejs node.js

A flaw in Node.js's permission model allows Unix Domain Socket (UDS) connections to bypass network restrictions when `--permission` is enabled. Even without `--allow-net`, attacker-controlled inputs (such as URLs or socketPath options) can connect to arbitrary

9.8 **CVE-2026-21969** Oracle agile product lifecycle management for process

Vulnerability in the Oracle Agile Product Lifecycle Management for Process product of Oracle Supply Chain (component: Supplier Portal). The supported version that is affected is 6.2.4. Easily exploitable vulnerability allows unauthenticated attacker with netwo

9.8 **CVE-2026-0906** Google chrome

Incorrect security UI in Google Chrome on Android prior to 144.0.7559.59 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Low)

9.8 **CVE-2026-0905** Google chrome

Insufficient policy enforcement in Network in Google Chrome prior to 144.0.7559.59 allowed an attack who obtained a network log file to potentially obtain potentially sensitive information via a network log file. (Chromium security severity: Medium)

9.8 **CVE-2025-56005** Dabeaz ply

An undocumented and unsafe feature in the PLY (Python Lex-Yacc) library 3.11 allows Remote Code Execution (RCE) via the `picklefile` parameter in the `yacc()` function. This parameter accepts a `.pkl` file that is deserialized with `pickle.load()` without vali

9.9 **CVE-2026-22844**

A Command Injection vulnerability in Zoom Node Multimedia Routers (MMRs) before version 5.2.1716.0 may allow a meeting participant to conduct remote code execution of the MMR via network access.

9.8 **CVE-2025-55423** Iptime n104s-r1 firmware

A command injection vulnerability exists in the upnp_relay() function in multiple ipTIME router models because the controlURL value used to pass port-forwarding information to an upper router is passed to system() without proper validation or sanitization, all

9.8 **CVE-2025-14533**

The Advanced Custom Fields: Extended plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 0.9.2.1. This is due to the 'insert_user' function not restricting the roles with which a user can register. This makes it pos

9.8 **CVE-2026-23947** Orval orval

Orval generates type-safe JS clients (TypeScript) from any valid OpenAPI v3 or Swagger v2 specification. Versions prior to 7.19.0 until 8.0.2 are vulnerable to arbitrary code execution in environments consuming generated clients. This issue is similar in natur

9.6 **CVE-2025-53912** Meddream pacs server

An arbitrary file read vulnerability exists in the encapsulatedDoc functionality of MedDream PACS Premium 7.3.6.870. A specially crafted HTTP request can lead to an arbitrary file read. An attacker can send http request to trigger this vulnerability.

9.8 **CVE-2025-64087** Opensagres xdocreport

A Server-Side Template Injection (SSTI) vulnerability in the FreeMarker component of opensagres XDocReport v1.0.0 to v2.1.0 allows attackers to execute arbitrary code via injecting crafted template expressions.

9.8 **CVE-2025-65482** Opensagres xdocreport

An XML External Entity (XXE) vulnerability in opensagres XDocReport v0.9.2 to v2.0.3 allows attackers to execute arbitrary code via uploading a crafted .docx file.

9.8 **CVE-2026-1221**

PrismX MX100 AP controller developed by BROWAN COMMUNICATIONS has a Use of Hard-coded Credentials vulnerability, allowing unauthenticated remote attackers to log in to the database using hardcoded database credentials stored in the firmware.

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.