Daily brief, Friday, January 30, 2026

Jan 29, 7:00 PM to Jan 30, 7:00 PM ET

Generated Nov 7, 2026, 8:07 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-2025-51958** Aelsantex runcommand

aelsantex runcommand 2014-04-01, a plugin for DokuWiki, allows unauthenticated attackers to execute arbitrary system commands via lib/plugins/runcommand/postaction.php.

9.8 **CVE-2020-37027**

Sickbeard alpha contains a remote command injection vulnerability that allows unauthenticated attackers to execute arbitrary commands through the extra scripts configuration. Attackers can set malicious commands in the extra scripts field and trigger processin

9.5 **CVE-2025-26385**

Johnson Controls Metasys component listed below have Improper Neutralization of Special Elements used in a Command (Command Injection) Vulnerability . Successful exploitation of this vulnerability could allow remote SQL execution This issue affects * Metasys:

9.8 **CVE-2020-37052**

AirControl 1.4.2 contains a pre-authentication remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary system commands through malicious Java expression injection. Attackers can exploit the /.seam endpoint by crafting a s

9.2 **CVE-2026-1723**

Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in TOTOLINK X6000R allows OS Command Injection.This issue affects X6000R: through V9.4.0cu.1498_B20250826.

9.6 **CVE-2026-25130**

Cybersecurity AI (CAI) is a framework for AI Security. In versions up to and including 0.5.10, the CAI (Cybersecurity AI) framework contains multiple argument injection vulnerabilities in its function tools. User-controlled input is passed directly to shell co

9.8 **CVE-2020-37050**

Quick Player 1.3 contains a buffer overflow vulnerability that allows attackers to execute arbitrary code by crafting a malicious .m3l file with carefully constructed payload. Attackers can trigger the vulnerability by loading a specially crafted file through

9.8 **CVE-2020-37043**

10-Strike Bandwidth Monitor 3.9 contains a buffer overflow vulnerability that allows attackers to bypass SafeSEH, ASLR, and DEP protections through carefully crafted input. Attackers can exploit the vulnerability by sending a malicious payload to the applicati

9.9 **CVE-2026-0963** Craftycontrol crafty controller

An input neutralization vulnerability in the File Operations API Endpoint component of Crafty Controller allows a remote, authenticated attacker to perform file tampering and remote code execution via path traversal.

9.8 **CVE-2026-25141** Orval orval

Orval generates type-safe JS clients (TypeScript) from any valid OpenAPI v3 or Swagger v2 specification. Versions starting with 7.19.0 and prior to 7.21.0 and 8.2.0 have an incomplete fix for CVE-2026-23947. While the jsStringEscape function properly handles s

9.8 **CVE-2020-37056**

Crystal Shard http-protection 0.2.0 contains an IP spoofing vulnerability that allows attackers to bypass protection middleware by manipulating request headers. Attackers can hardcode consistent IP values across X-Forwarded-For, X-Client-IP, and X-Real-IP head

10.0 **CVE-2026-1699** Eclipse theia website

In the Eclipse Theia Website repository, the GitHub Actions workflow .github/workflows/preview.yml used pull_request_target trigger while checking out and executing untrusted pull request code. This allowed any GitHub user to execute arbitrary code in the repo

9.3 **CVE-2026-24728**

A missing authentication for critical function vulnerability in the /servlet/baServer3 endpoint of Interinfo DreamMaker versions before 2025/10/22 allows remote attackers to access exposed administrative functionality without prior authentication.

9.8 **CVE-2019-25232**

NetPCLinker 1.0.0.0 contains a buffer overflow vulnerability in the Clients Control Panel DNS/IP field that allows attackers to execute arbitrary shellcode. Attackers can craft a malicious payload in the DNS/IP input to overwrite SEH handlers and execute shell

10.0 **CVE-2026-24729**

An unrestricted upload of file with dangerous type vulnerability in the file upload function of Interinfo DreamMaker versions before 2025/10/22 allows remote attackers to execute arbitrary system commands via a malicious class file.

9.2 **CVE-2025-7964**

After receiving a malformed 802.15.4 MAC Data Request the Zigbee Coordinator sends a ‘network leave’ request to Zigbee router resulting in the Zigbee Router getting stuck in a non-rejoinable state. If a suitable parent is not available, the end devices will be

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.