Daily brief, Friday, February 6, 2026

Feb 5, 7:00 PM to Feb 6, 7:00 PM ET

Generated Nov 7, 2026, 6:53 PM ET

0	0	0	20	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

20 new critical CVEs, 1 new breaches.

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

9.4 **CVE-2026-1709** Redhat enterprise linux

A flaw was found in Keylime. The Keylime registrar, since version 7.12.0, does not enforce client-side Transport Layer Security (TLS) authentication. This authentication bypass vulnerability allows unauthenticated clients with network access to perform adminis

9.1 **CVE-2026-25804** Linuxfoundation antrea

Antrea is a Kubernetes networking solution intended to be Kubernetes native. Prior to versions 2.3.2 and 2.4.3, Antrea's network policy priority assignment system has a uint16 arithmetic overflow bug that causes incorrect OpenFlow priority calculations when ha

9.8 **CVE-2026-2017** Ip-Com w30ap firmware

A vulnerability was detected in IP-COM W30AP up to 1.0.0.11(1340). Affected by this issue is the function R7WebsSecurityHandler of the file /goform/wx3auth of the component POST Request Handler. The manipulation of the argument data results in stack-based buff

9.1 **CVE-2026-25643** Frigate frigate

Frigate is a network video recorder (NVR) with realtime local object detection for IP cameras. Prior to 0.16.4, a critical Remote Command Execution (RCE) vulnerability has been identified in the Frigate integration with go2rtc. The application does not sanitiz

9.9 **CVE-2026-25592**

Semantic Kernel is an SDK used to build, orchestrate, and deploy AI agents and multi-agent systems. Prior to 1.71.0, an Arbitrary File Write vulnerability has been identified in Microsoft's Semantic Kernel .NET SDK, specifically within the SessionsPythonPlugin

9.8 **CVE-2025-64111** Gogs gogs

Gogs is an open source self-hosted Git service. In version 0.13.3 and prior, due to the insufficient patch for CVE-2024-56731, it's still possible to update files in the .git directory and achieve remote command execution. This issue has been patched in versio

10.0 **CVE-2026-25520** Nyariv sandboxjs

SandboxJS is a JavaScript sandboxing library. Prior to 0.8.29, The return values of functions aren't wrapped. Object.values/Object.entries can be used to get an Array containing the host's Function constructor, by using Array.prototype.at you can obtain the ho

9.8 **CVE-2026-25544** Payloadcms payload

Payload is a free and open source headless content management system. Prior to 3.73.0, when querying JSON or richText fields, user input was directly embedded into SQL without escaping, enabling blind SQL injection attacks. An unauthenticated attacker could ex

10.0 **CVE-2026-25632** Waterfutures epyt-flow

EPyT-Flow is a Python package designed for the easy generation of hydraulic and water quality scenario data of water distribution networks. Prior to 0.16.1, EPyT-Flow’s REST API parses attacker-controlled JSON request bodies using a custom deserializer (my_loa

10.0 **CVE-2026-25587** Nyariv sandboxjs

SandboxJS is a JavaScript sandboxing library. Prior to 0.8.29, as Map is in SAFE_PROTOYPES, it's prototype can be obtained via Map.prototype. By overwriting Map.prototype.has the sandbox can be escaped. This vulnerability is fixed in 0.8.29.

10.0 **CVE-2026-25586** Nyariv sandboxjs

SandboxJS is a JavaScript sandboxing library. Prior to 0.8.29, a sandbox escape is possible by shadowing hasOwnProperty on a sandbox object, which disables prototype whitelist enforcement in the property-access path. This permits direct access to __proto__ and

9.1 **CVE-2026-25752** Frangoteam fuxa

FUXA is a web-based Process Visualization (SCADA/HMI/Dashboard) software. An authorization bypass vulnerability in FUXA allows an unauthenticated, remote attacker to modify device tags via WebSockets. Exploitation allows an unauthenticated, remote attacker to

10.0 **CVE-2026-25725** Anthropic claude code

Claude Code is an agentic coding tool. Prior to version 2.1.2, Claude Code's bubblewrap sandboxing mechanism failed to properly protect the .claude/settings.json configuration file when it did not exist at startup. While the parent directory was mounted as wri

10.0 **CVE-2026-25641** Nyariv sandboxjs

SandboxJS is a JavaScript sandboxing library. Prior to 0.8.29, there is a sandbox escape vulnerability due to a mismatch between the key on which the validation is performed and the key used for accessing properties. Even though the key used in property access

9.9 **CVE-2026-25763** Openproject openproject

OpenProject is an open-source, web-based project management software. Prior to versions 16.6.7 and 17.0.3, an arbitrary file write vulnerability exists in OpenProject's repository changes endpoint (/projects/:project_id/repository/changes) when rendering the "

9.1 **CVE-2026-25722** Anthropic claude code

Claude Code is an agentic coding tool. Prior to version 2.0.57, Claude Code failed to properly validate directory changes when combined with write operations to protected folders. By using the cd command to navigate into sensitive directories like .claude, it

9.1 **CVE-2019-25298** Lolypop55 html5 snmp

html5_snmp 1.11 contains multiple SQL injection vulnerabilities that allow attackers to manipulate database queries through Router_ID and Router_IP parameters. Attackers can exploit error-based, time-based, and union-based injection techniques to potentially e

9.8 **CVE-2026-25803** Denpiligrim 3dp-manager

3DP-MANAGER is an inbound generator for 3x-ui. In version 2.0.1 and prior, the application automatically creates an administrative account with known default credentials (admin/admin) upon the first initialization. Attackers with network access to the applicat

9.8 **CVE-2026-25753** Prasklatechnology placipy

PlaciPy is a placement management system designed for educational institutions. In version 1.0.0, the application uses a hard-coded, static default password for all newly created student accounts. This results in mass account takeover, allowing any attacker to

9.1 **CVE-2026-1727**

The Agentspace service was affected by a vulnerability that exposed sensitive information due to the use of predictable Google Cloud Storage bucket names. These names were utilized for error logs and temporary staging during data imports from GCS and Cloud SQL

Ransomware

No leak-site posts collected.

New data breaches 1

Substack substack.com 663,121 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.