Daily brief, Wednesday, February 25, 2026

Feb 24, 7:00 PM to Feb 25, 7:00 PM ET

Generated Nov 7, 2026, 3:52 PM ET

0	2	0	40	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 newly exploited, 40 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

2

10.0 **CVE-2026-20127** Cisco Catalyst SD-WAN Controller and Manager CISA KEV

Authentication bypass in Cisco Catalyst SD-WAN Controller and Manager lets an attacker gain unauthorized access to the SD-WAN network.

7.8 **CVE-2022-20775** Cisco SD-WAN CISA KEV

An authenticated local attacker gains root command execution through a path traversal flaw in the Cisco SD-WAN CLI.

New public exploit code

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

New critical CVEs

40

10.0 **CVE-2026-20127** Cisco Catalyst SD-WAN Controller and Manager KEV EXPLOIT CODE

Authentication bypass in Cisco Catalyst SD-WAN Controller and Manager lets an attacker gain unauthorized access to the SD-WAN network.

9.8 **CVE-2026-21902** Juniper junos os evolved DETECTION

An Incorrect Permission Assignment for Critical Resource vulnerability in the On-Box Anomaly detection framework of Juniper Networks Junos OS Evolved on PTX Series allows an unauthenticated, network-based attacker to execute code as root. The On-Box Anomaly de

9.8 **CVE-2026-20129** Cisco catalyst sd-wan manager

A vulnerability in the API user authentication of Cisco Catalyst SD-WAN Manager could allow an unauthenticated, remote attacker to gain access to an affected system as a user who has the netadmin role. The vulnerability is due to improper authentication f

9.9 **CVE-2026-27577** N8n n8n

n8n is an open source workflow automation platform. Prior to versions 2.10.1, 2.9.3, and 1.123.22, additional exploits in the expression evaluation of n8n have been identified and patched following CVE-2025-68613. An authenticated user with permission to creat

9.0 **CVE-2026-27822** Rustfs rustfs

RustFS is a distributed object storage system built in Rust. Prior to version 1.0.0-alpha.83, a Stored Cross-Site Scripting (XSS) vulnerability in the RustFS Console allows an attacker to execute arbitrary JavaScript in the context of the management console. B

9.8 **CVE-2026-2624** Epati antikor next generation firewall

Missing Authentication for Critical Function vulnerability in ePati Cyber ??Security Technologies Inc. Antikor Next Generation Firewall (NGFW) allows Authentication Bypass. This issue affects Antikor Next Generation Firewall (NGFW): from v.2.0.1298 before v.2.

9.9 **CVE-2026-24849** Open-Emr openemr

+1 more CVEs in the same release

OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 7.0.4, the `disposeDocument()` method in `EtherFaxActions.php` allows authenticated users to read arbitrary files from the server filesyst

9.9 **CVE-2026-27728** Hackerbay oneuptime

OneUptime is a solution for monitoring and managing online services. Prior to version 10.0.7, an OS command injection vulnerability in `NetworkPathMonitor.performTraceroute()` allows any authenticated project user to execute arbitrary operating system commands

9.8 **CVE-2026-27606** Rollupjs rollup

Rollup is a module bundler for JavaScript. Versions prior to 2.80.0, 3.30.0, and 4.59.0 of the Rollup module bundler (specifically v4.x and present in current source) is vulnerable to an Arbitrary File Write via Path Traversal. Insecure file name sanitization

9.0 **CVE-2026-27493** N8n n8n

n8n is an open source workflow automation platform. Prior to versions 2.10.1, 2.9.3, and 1.123.22, a second-order expression injection vulnerability existed in n8n's Form nodes that could allow an unauthenticated attacker to inject and evaluate arbitrary n8n e

9.8 **CVE-2026-27641** Jugmac00 flask-reuploaded

Flask-Reuploaded provides file uploads for Flask. A critical path traversal and extension bypass vulnerability in versions prior to 1.5.0 allows remote attackers to achieve arbitrary file write and remote code execution through Server-Side Template Injection (

9.8 **CVE-2026-27744** Spip tickets

The SPIP tickets plugin versions prior to 4.3.3 contain an unauthenticated remote code execution vulnerability in the forum preview handling for public ticket pages. The plugin appends untrusted request parameters into HTML that is later rendered by a template

10.0 **CVE-2026-27597** Agentfront enclave

Enclave is a secure JavaScript sandbox designed for safe AI agent code execution. Prior to version 2.11.1, it is possible to escape the security boundraries set by `@enclave-vm/core`, which can be used to achieve remote code execution (RCE). The issue has been

9.1 **CVE-2026-27699** Patrickjuchli basic-ftp

The `basic-ftp` FTP client library for Node.js contains a path traversal vulnerability (CWE-22) in versions prior to 5.2.0 in the `downloadToDir()` method. A malicious FTP server can send directory listings with filenames containing path traversal sequences (`

9.8 **CVE-2026-27613** Ritlabs tinyweb

TinyWeb is a web server (HTTP, HTTPS) written in Delphi for Win32. A vulnerability in versions prior to 2.01 allows unauthenticated remote attackers to bypass the web server's CGI parameter security controls. Depending on the server configuration and the speci

9.9 **CVE-2026-27495** N8n n8n

+1 more CVEs in the same release

n8n is an open source workflow automation platform. Prior to versions 2.10.1, 2.9.3, and 1.123.22, an authenticated user with permission to create or modify workflows could exploit a vulnerability in the JavaScript Task Runner sandbox to execute arbitrary code

9.8 **CVE-2026-27637** Freescout freescout

FreeScout is a free help desk and shared inbox built with PHP's Laravel framework. Prior to version 1.8.206, FreeScout's `TokenAuth` middleware uses a predictable authentication token computed as `MD5(user_id + created_at + APP_KEY)`. This token is static (nev

9.8 **CVE-2026-25952** Freerdp freerdp

FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.23.0, `xf_SetWindowMinMaxInfo` dereferences a freed `xfAppWindow` pointer because `xf_rail_get_window` in `xf_rail_server_min_max_info` returns an unprotected pointer from the

9.8 **CVE-2026-25953** Freerdp freerdp

+1 more CVEs in the same release

FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.23.0, `xf_AppUpdateWindowFromSurface` reads from a freed `xfAppWindow` because the RDPGFX DVC thread obtains a bare pointer via `xf_rail_get_window` without any lifetime protec

9.8 **CVE-2026-27743** Spip referer spam

The SPIP referer_spam plugin versions prior to 1.3.0 contain an unauthenticated SQL injection vulnerability in the referer_spam_ajouter and referer_spam_supprimer action handlers. The handlers read the url parameter from a GET request and interpolate it direct

17 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

Canadian Tire canadiantire.ca 38,306,562 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.