Daily brief, Friday, February 27, 2026

Feb 26, 7:00 PM to Feb 27, 7:00 PM ET

Generated Nov 7, 2026, 3:36 PM ET

0	0	0	36	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

36 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

36

9.8 **CVE-2026-28517** Opendcim opendcim

openDCIM version 23.04, through commit 4467e9c4, contains an OS command injection vulnerability in report_network_map.php. The application retrieves the 'dot' configuration parameter from the database and passes it directly to exec() without validation or sani

9.8 **CVE-2026-3301** Totolink n300rh firmware

A security flaw has been discovered in Totolink N300RH 6.1c.1353_B20190305. Affected by this vulnerability is the function setWebWlanIdx of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. Performing a manipulation of the argument webWl

9.0 **CVE-2026-24663** Copeland xweb 500b pro firmware

An OS command injection vulnerability exists in XWEB Pro version 1.12.1 and prior, enabling an unauthenticated attacker to achieve remote code execution on the system by sending a crafted request to the libraries installation route and injecting malicious inpu

10.0 **CVE-2026-28409** Wegia wegia DETECTION

WeGIA is a web manager for charitable institutions. Prior to version 3.6.5, a critical Remote Code Execution (RCE) vulnerability exists in the WeGIA application's database restoration functionality. An attacker with administrative access (which can be obtained

9.8 **CVE-2026-28411** Wegia wegia DETECTION

WeGIA is a web manager for charitable institutions. Prior to version 3.6.5, an unsafe use of the `extract()` function on the `$_REQUEST` superglobal allows an unauthenticated attacker to overwrite local variables in multiple PHP scripts. This vulnerability can

9.8 **CVE-2026-21654** Johnsoncontrols frick controls quantum hd firmware

Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Johnson Controls Frick Controls Quantum HD allows OS Command Injection. Insufficient validation of input in certain parameters may permit unexpected act

9.8 **CVE-2026-21659** Johnsoncontrols frick controls quantum hd firmware

Unauthenticated Remote Code Execution and Information Disclosure due to Local File Inclusion (LFI) vulnerability in Johnson Controls Frick Controls Quantum HD allow an unauthenticated attacker to execute arbitrary code on the affected device, leading to full s

9.1 **CVE-2026-28370** Openstack vitrage

In the query parser in OpenStack Vitrage before 12.0.1, 13.0.0, 14.0.0, and 15.0.0, a user allowed to access the Vitrage API may trigger code execution on the Vitrage service host as the user the Vitrage service runs under. This may result in unauthorized acce

9.8 **CVE-2026-2293** Nestjs nest

A NestJS application using @nestjs/platform-fastify can allow bypass of authentication/authorization middleware when Fastify path-normalization options are enabled. This issue affects nest.Js: 11.1.13.

9.4 **CVE-2026-25851** Chargemap chargemap.com

WebSocket endpoints lack proper authentication mechanisms, enabling attackers to perform unauthorized station impersonation and manipulate data sent to the backend. An unauthenticated attacker can connect to the OCPP WebSocket endpoint using a known or discove

9.8 **CVE-2026-28268** Vikunja vikunja

Vikunja is an open-source self-hosted task management platform. Versions prior to 2.1.0 have a business logic vulnerability exists in the password reset mechanism of vikunja/api that allows password reset tokens to be reused indefinitely. Due to a failure to i

9.8 **CVE-2026-21658** Johnsoncontrols frick controls quantum hd firmware

Unauthenticated Remote Code Execution i.e Improper Control of Generation of Code ('Code Injection') vulnerability in Johnson Controls Frick Controls Quantum HD allows Code Injection. Insufficient validation of input in certain parameters may permit unexpected

9.1 **CVE-2026-28231** Bigcat88 pillow-heif

pillow_heif is a Python library for working with HEIF images and plugin for Pillow. Prior to version 1.3.0, an integer overflow in the encode path buffer validation of `_pillow_heif.c` allows an attacker to bypass bounds checks by providing large image dimensi

10.0 **CVE-2026-21718** Copeland xweb 300d pro firmware

An authentication bypass vulnerability exists in Copeland XWEB Pro version 1.12.1 and prior, enabling any attackers to bypass the authentication requirement and achieve pre-authenticated code execution on the system.

9.4 **CVE-2026-24731** Ev2go ev2go.io

WebSocket endpoints lack proper authentication mechanisms, enabling attackers to perform unauthorized station impersonation and manipulate data sent to the backend. An unauthenticated attacker can connect to the OCPP WebSocket endpoint using a known or discove

9.8 **CVE-2025-12981**

The Listee theme for WordPress is vulnerable to privilege escalation in all versions up to, and including, 1.1.6. This is due to a broken validation check in the bundled listee-core plugin's user registration function that fails to properly sanitize the user_r

9.9 **CVE-2026-2749** Centreon open tickets

Vulnerability in Centreon Centreon Open Tickets on Central Server on Linux (Centroen Open Ticket modules).This issue affects Centreon Open Tickets on Central Server: from all before 25.10.3, 24.10.8, 24.04.7.

9.4 **CVE-2026-27772** Ev.Energy ev.energy

WebSocket endpoints lack proper authentication mechanisms, enabling attackers to perform unauthorized station impersonation and manipulate data sent to the backend. An unauthenticated attacker can connect to the OCPP WebSocket endpoint using a known or discove

9.4 **CVE-2026-20781** Cloudcharge cloudcharge.se

WebSocket endpoints lack proper authentication mechanisms, enabling attackers to perform unauthorized station impersonation and manipulate data sent to the backend. An unauthenticated attacker can connect to the OCPP WebSocket endpoint using a known or discove

9.4 **CVE-2026-27767** Swtchenergy swtchenergy.com

WebSocket endpoints lack proper authentication mechanisms, enabling attackers to perform unauthorized station impersonation and manipulate data sent to the backend. An unauthenticated attacker can connect to the OCPP WebSocket endpoint using a known or discove

16 more critical CVEs in this window: see the dashboard

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.