Daily brief, Monday, February 9, 2026

Feb 8, 7:00 PM to Feb 9, 7:00 PM ET

Generated Nov 7, 2026, 6:20 PM ET

0	0	0	28	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

28 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

28

9.9 **CVE-2026-1868** GitLab GitLab AI Gateway

Product not on watchlist.

9.8 **CVE-2026-25895** Frangoteam fuxa DETECTION

FUXA is a web-based Process Visualization (SCADA/HMI/Dashboard) software. A path traversal vulnerability in FUXA allows an unauthenticated, remote attacker to write arbitrary files to arbitrary locations on the server filesystem. This affects FUXA through vers

9.1 **CVE-2026-25939** Frangoteam fuxa

FUXA is a web-based Process Visualization (SCADA/HMI/Dashboard) software. From 1.2.8 through version 1.2.10, an authorization bypass vulnerability in the FUXA allows an unauthenticated, remote attacker to create and modify arbitrary schedulers, exposing connec

9.8 **CVE-2026-1615**

Versions of the package jsonpath before 1.3.0 are vulnerable to Arbitrary Code Injection via unsafe evaluation of user-supplied JSON Path expressions. The library relies on the static-eval module to process JSON Path input, which is not designed to handle untr

9.8 **CVE-2026-25938** Frangoteam fuxa

FUXA is a web-based Process Visualization (SCADA/HMI/Dashboard) software. From 1.2.8 through 1.2.10, an authentication bypass vulnerability in FUXA allows an unauthenticated, remote attacker to execute arbitrary code on the server when the Node-RED plugin is e

9.8 **CVE-2026-25894** Frangoteam fuxa

FUXA is a web-based Process Visualization (SCADA/HMI/Dashboard) software. An insecure default configuration in FUXA allows an unauthenticated, remote attacker to gain administrative access and execute arbitrary code on the server. This affects FUXA through ver

9.8 **CVE-2026-25893** Frangoteam fuxa

FUXA is a web-based Process Visualization (SCADA/HMI/Dashboard) software. Prior to 1.2.10, an authentication bypass vulnerability in FUXA allows an unauthenticated, remote attacker to gain administrative access via the heartbeat refresh API and execute arbitra

9.8 **CVE-2026-22903**

An unauthenticated remote attacker can send a crafted HTTP request containing an overly long SESSIONID cookie. This can trigger a stack buffer overflow in the modified lighttpd server, causing it to crash and potentially enabling remote code execution due to m

9.8 **CVE-2026-22904**

Improper length handling when parsing multiple cookie fields (including TRACKID) allows an unauthenticated remote attacker to send oversized cookie values and trigger a stack buffer overflow, resulting in a denial?of?service condition and possible remote code

9.0 **CVE-2026-25881** Nyariv sandboxjs

SandboxJS is a JavaScript sandboxing library. Prior to 0.8.31, a sandbox escape vulnerability allows sandboxed code to mutate host built-in prototypes by laundering the isGlobal protection flag through array literal intermediaries. When a global prototype refe

9.1 **CVE-2026-24677** Freerdp freerdp

FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.22.0, ecam_encoder_compress_h264 trusts server-controlled dimensions and does not validate the source buffer size, leading to an out-of-bounds read in sws_scale. This vulnerability is

9.1 **CVE-2026-24679** Freerdp freerdp

FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.22.0, The URBDRC client uses server-supplied interface numbers as array indices without bounds checks, causing an out-of-bounds read in libusb_udev_select_interface. This vulnerability

9.4 **CVE-2025-66630** Gofiber fiber

Fiber is an Express inspired web framework written in Go. Before 2.52.11, on Go versions prior to 1.24, the underlying crypto/rand implementation can return an error if secure randomness cannot be obtained. Because no error is returned by the Fiber v2 UUID fun

9.1 **CVE-2026-25057** Markusproject markus

MarkUs is a web application for the submission and grading of student assignments. Prior to 2.9.1, instructors are able to upload a zip file to create an assignment from an exported configuration (courses/<:course_id>/assignments/upload_config_files). The uplo

9.1 **CVE-2026-2234**
C&Cm@il developed by HGiga has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to read and modify any user's mail content.

9.1 **CVE-2026-25923** Mylittleforum my little forum
my little forum is a PHP and MySQL based internet forum that displays the messages in classical threaded view. Prior to 20260208.1, the application fails to filter the phar:// protocol in URL validation, allowing attackers to upload a malicious Phar Polyglot f

9.1 **CVE-2026-25848** Jetbrains hub
In JetBrains Hub before 2025.3.119807 authentication bypass allowing administrative actions was possible

9.8 **CVE-2025-6830**
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Xpoda Türkiye Information Technology Inc. Password Module allows SQL Injection. This issue affects Password Module: through 11022026.

9.8 **CVE-2026-25814** Prasklatechnology placipy
PlaciPy is a placement management system designed for educational institutions. In version 1.0.0, User-controlled query parameters are passed directly into DynamoDB query/filter construction without validation or sanitization.

9.8 **CVE-2026-25809** Prasklatechnology placipy
PlaciPy is a placement management system designed for educational institutions. In version 1.0.0, the code evaluation endpoint does not validate the assessment lifecycle state before allowing execution. There is no check to ensure that the assessment has start

8 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.