Daily brief, Friday, July 31, 2026

Jul 30, 8:00 PM to Jul 31, 8:00 PM ET

Generated Nov 3, 2026, 2:41 AM 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

10.0 **CVE-2026-18452**

DMS+ (Non-Mobile) developed by Rich Source has a Use of Hard-coded Credentials vulnerability. Unauthenticated remote attackers can exploit a fixed API key to gain control over all installed DMS+ devices.

9.9 **CVE-2026-17566** Pgadmin pgadmin 4

pgAdmin 4's Import/Export Data tool builds a psql \copy (...) command line by interpolating a user-supplied SQL query into a Jinja template and passing the rendered line to psql via --command. To stop an attacker from breaking out of the (...) wrapper, create_

9.9 **CVE-2026-52855**

Wings is the server control plane for Pterodactyl, a free, open-source game server management panel. Prior to 1.12.3, {{config.}} placeholders in egg configuration-file templates allow a low-privileged user to read {{config.token}}, {{config.token_id}}, and {{

9.8 **CVE-2026-14537** Google mcp toolbox for databases

Incorrect Authorization in the direct HTTP API tool invocation endpoint in Google mcp-toolbox versions v1.3.0 and v1.4.0 allows an unauthenticated attacker to invoke tools protected by the scopeRequired feature via sending tool invocation requests through lega

9.8 **CVE-2026-43830**

A command injection vulnerability in the firmware upgrade file verification process could allow an attacker to execute arbitrary commands.

9.8 **CVE-2026-63223**

CodeIgniter is a PHP full-stack web framework. Prior to 4.7.4, the is_image and mime_in upload validation rules do not independently enforce a safe client filename extension, allowing a remote attacker to upload executable content when an application preserves

9.8 **CVE-2026-14483** DETECTION

The Realtyna Organic IDX plugin + WPL Real Estate plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 5.2.0 via the upload function. This is due to missing file type validation in the upload function, combined with

9.8 **CVE-2026-14919**

The ShopMonitor.io WordPress plugin before 1.2.0 does not properly restrict its email-rerouting test mode, gating it behind a trusted-source check that is satisfiable with client-supplied request headers, allowing unauthenticated attackers to redirect outgoing

9.8 **CVE-2026-17561**

Improper Control of Generation of Code ('Code Injection') vulnerability in Innotim Software, Telecommunications and Consulting Trade Ltd. Co. Logsign SIEM allows Code Injection. This issue affects Logsign SIEM: before 6.4.115.

9.8 **CVE-2026-16504**

Deployment of the VPS.org one-click Zulip template deploys a hardcoded application signing key, a default database password ("zulip"), and DISABLE_HTTPS=True.

9.8 **CVE-2026-67822**

Tenda W6-S 1.0.0.4(510) contains a stack-based buffer overflow vulnerability in the /goform/wifiSSIDset endpoint. The function formwrlSSIDset uses sprintf to copy user-controlled 'GO' and 'index' parameters into a 64-byte stack buffer without length restrictio

9.8 **CVE-2026-21662** Johnsoncontrols fms employee

Unrestricted upload of file with dangerous type vulnerability in Johnson Controls FM Systems Employee allows Using Malicious Files. This issue affects FM Systems Employee: before 2025.3.1.

9.8 **CVE-2026-38711**

+2 more CVEs in the same release

TR1200 v2.4.15, TR3000 v2.4.21, WR300 v2.4.25, WR1200 v2.4.23, WR1300 v2.4.22, WR1500 v2.3.10, WR3000 v2.4.19, WR3600 v2.3.16, and WR6500 v2.3.15 were discovered to contain a command injection vulnerability in the system.upgrade_check interface. This vulnerabi

9.8 **CVE-2025-69946**

SourceCodester Modern Loan Management System 1.0 is vulnerable to SQL Injection in ajaxData.php via the parameters district_id , division_id, region_id, and ward_id.

9.8 **CVE-2025-69948**

SourceCodester Modern Loan Management System 1.0 is vulnerable to SQL Injection in /admin/delete_group.php?id=1.

9.8 **CVE-2026-51785**
An issue in Hugo Leisink Hiawatha v.12.1 and before allows a remote attacker to execute arbitrary code via a crafted request

9.8 **CVE-2026-68770**
sentence-transformers contains a security control bypass vulnerability that allows attackers to achieve arbitrary code execution by exploiting a logic flaw in the import_module_class helper within sentence_transformers/util/misc.py, where the guard condition i

9.8 **CVE-2026-52134**
An issue in the parseGoosePayload() function (/goose/goose_receiver.c) of libiec61850 v1.6 allows attackers to bypass authentication via a captured GOOSE frame.

9.8 **CVE-2026-68771**
ComfyUI v0.23.0 contains an unsafe deserialization vulnerability in the LoadTrainingDataset node that allows unauthenticated remote attackers to execute arbitrary Python code by uploading a crafted pickle file and triggering its deserialization. Attackers can

9.6 **CVE-2026-17349** Pgadmin pgadmin 4
/misc/workspace/adhoc_connect_server, part of the Workspaces feature introduced in pgAdmin 4 9.0, when passed the id of an existing server, clones that server via Server.clone(), which copies every column from the source row, including user_id, shared, shared_

6 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. CVE IDs link to the full record on Watch Floor.