Daily brief, Friday, July 10, 2026

Jul 9, 8:00 PM to Jul 10, 8:00 PM ET

Generated Nov 3, 2026, 9:56 PM ET

0	2	0	39	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 newly exploited, 39 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild 2

10.0 **CVE-2026-48939** iCagenda iCagenda CISA KEV DETECTION

An attacker can upload and execute arbitrary PHP code on an iCagenda server.

10.0 **CVE-2026-56291** Balbooa Forms CISA KEV DETECTION

An unauthenticated attacker gains full RCE on Balbooa Forms.

New public exploit code

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

New critical CVEs 39

10.0 **CVE-2026-48939** iCagenda iCagenda KEV EXPLOIT CODE DETECTION

An attacker can upload and execute arbitrary PHP code on an iCagenda server.

10.0 **CVE-2026-56291** Balbooa Forms KEV EXPLOIT CODE DETECTION

An unauthenticated attacker gains full RCE on Balbooa Forms.

9.8 **CVE-2026-53363** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: xfrm: iptfs: preserve shared-frag marker in iptfs_consume_frags() iptfs_consume_frags() transfers paged fragments from one socket buffer to another but fails to propagate the SKBFL_SHARED_FRAG

9.8 **CVE-2026-61459** Suyogs mcp-server-kubernetes

MCP Server Kubernetes before 3.9.0 contains an argument injection vulnerability in structured tools (kubectl_get, kubectl_describe, kubectl_delete) that allows attackers to bypass the assertNoDangerousFlags security check by supplying resourceType and name par

9.1 **CVE-2026-56688** Dell powerflex manager

Dell PowerFlex Manager, Version prior to 5.1.0.1, contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability

9.0 **CVE-2026-41880** R-SOFT SERWIS DMS

R-SOFT DMS is vulnerable to OS Command Injection in the Optical Character Recognition (OCR) module. Multiple command execution functions accept user-controllable file paths without proper sanitization before passing them to the system shell via SSH. In current

9.6 **CVE-2026-59792** Jetbrains intellij idea

In JetBrains IntelliJ IDEA before 2026.1.4, 2026.2 code execution via path traversal in project workspace ID handling was possible

10.0 **CVE-2026-54769**

Langroid is a framework for building large-language-model-powered applications. Versions prior to 0.65.2 are vulnerable to a critical Sandbox Escape leading to Remote Code Execution (RCE) in its `TableChatAgent` and `VectorStore` capabilities. When these agent

9.9 **CVE-2026-55500**

9Router is an AI router & token saver. Prior to 0.4.80, the /api/settings/database endpoint allows full database export (containing all credentials, API keys, OAuth tokens, and settings) and full database import (complete overwrite) without any authentication

9.9 **CVE-2026-14480**

OpenPLC Runtime v3 contains an authenticated arbitrary file write vulnerability in the legacy web UI program?upload workflow. The application stores an attacker?supplied filename (prog_file) directly into the Programs.File database field and later uses this va

9.8 **CVE-2026-14894** DETECTION

The Super Forms – Drag & Drop Form Builder plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 6.3.313 via the submit_form function. This is due to missing file type validation and the absence of any capability che

9.8 **CVE-2026-15282**

The Instant Appointment plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'insapp_upload_image_as_attachment' function in all versions up to, and including, 1.2. This makes it possible for unauthenticated a

9.8 **CVE-2026-28564**

Insufficient Session Expiration, Authentication Bypass by Capture-replay vulnerability in Apache IoTDB. REST Basic Authentication Accepts Stale Cached Credentials This issue affects Apache IoTDB: from 1.0.0 before 2.0.10. Users are recommended to upgrade to ve

9.8 **CVE-2026-40008**
Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') vulnerability in Apache IoTDB. The pipe processor reads a fully qualified Java class name and instantiates it using Class.forName().newInstance() without any validation or allow

9.8 **CVE-2026-56765**
Vikunja before 2.2.1 contains an authorization flaw where the LinkSharing.ReadAll endpoint exposes share hashes to users with read access, enabling permission escalation to admin-level shares. The GetTaskAttachment endpoint performs permission checks against u

9.8 **CVE-2026-2397**
Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in Adam Retail Automation Ltd. MobilMen 20T allows SQL Injection. This issue affects MobilMen 20T: from v3 through 10072026. NOTE: The vendor was contacted early

9.8 **CVE-2026-5801**
Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in Semtek Informatics Software Consulting Trade Ltd. Co. SEM-PMP allows Command Line Execution through SQL Injection. This issue affects SEM-PMP: through 2304202

9.8 **CVE-2026-57156** Freerdp freerdp
FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.28.0 on 32-bit builds, FreeRDP clients contain an integer overflow in update_read_delta_points in libfreerdp/core/orders.c when multiplying an attacker-controlled point count by sizeof

9.8 **CVE-2026-12761**
The miniOrange Social Login and Register (Discord, Google, Twitter, LinkedIn) plugin for WordPress is vulnerable to authentication bypass leading to account takeover in versions up to and including 7.7.0. This is due to the Profile Completion flow accepting an

9.8 **CVE-2026-57807**
Authentication Bypass Using an Alternate Path or Channel vulnerability in miniOrange Security Software Pvt Ltd. OAuth Single Sign On - SSO (OAuth Client) allows Password Recovery Exploitation. This issue affects OAuth Single Sign On - SSO (OAuth Client): from

19 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.