# Daily brief, Thursday, July 9, 2026

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

Generated Nov 3, 2026, 10:52 PM ET

| 0 | 0 | 0 | 29 | 0 | 0 |
|---|---|---|---|---|---|
| Breaking | Newly exploited | Exploit code | Critical CVEs | Ransomware posts | New breaches |

29 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

29

**9.9** **CVE-2026-0284** Palo Alto Networks pan-os

An XML injection vulnerability in the Large Scale VPN (LSVPN) functionality of Palo Alto Networks PAN-OS® software enables an unauthenticated attacker with network access to inject malicious XML content, potentially leading to information disclosure or corrupt

**10.0** **CVE-2026-59726** DETECTION

Ruflo is an agent meta-harness for Claude Code and Codex. Prior to 3.16.3, ruflo's default docker-compose deployment exposed the MCP bridge POST /mcp and POST /mcp/:group endpoints without authentication, allowing an unauthenticated network attacker to invoke

**9.9** **CVE-2026-59827** Metabase metabase

Metabase is an open-source business intelligence and embedded analytics tool. Prior to 1.58.15, 1.59.12, 1.60.6.3, and 1.61.1.4, Metabase instances with an H2 database connection, including the default sample database, deserialize arbitrary Java objects return

9.8 **CVE-2026-14245**

The miniOrange OTP Login, Verification and SMS Notifications plugin for WordPress is vulnerable to Authentication Bypass leading to Administrator Account Takeover in all versions up to, and including, 5.5.1. This is due to the `um_reset_password_process_hook()

9.8 **CVE-2026-15158**

The Blocksy Companion plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 2.1.46 via the save_attachments function. This is due to the Custom Fonts extension registering a wp_check_filetype_and_ext filter that appr

9.8 **CVE-2026-5955**

Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in Inrove Software and Internet Services BiEticaret allows SQL Injection. This issue affects BiEticaret: before v3.3.57.

9.8 **CVE-2026-12116**

A vulnerability in the Xerte Online Tools allows for RCE through the antivirus binary path in the tools server settings, which can be changed to a PHP interpreter, allowing an attacker to upload PHP data that will then be executed.

9.8 **CVE-2026-51599**

An insufficient input validation vulnerability in the RTSP service of MERCURY MIPC252W v1.0.5 Build 230306 Rel.79931n allows an unauthenticated remote attacker to render an individual TCP connection temporarily unusable via sending an RTSP request with a Conte

9.8 **CVE-2026-58123** DETECTION

Hermes WebUI before 0.51.788 contains an unauthenticated remote code execution vulnerability that allows remote attackers to execute arbitrary shell commands by accessing the embedded terminal API endpoints without credentials. Attackers can create a session,

9.6 **CVE-2026-13461**

When coupled with the SSL bypass vulnerability, JavaScript can be injected into a WebView in the PayRange version 7.0.7 app. The injection of specific JavaScript function calls allows the attacker to escape the WebView sandbox and perform a number of dangerous

9.4 **CVE-2025-27462**

**+7 more CVEs in the same release**

[This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] The Windows PV drivers expose various facilities to userspace. Several of these have no security descriptor, and are therefore full

9.4 **CVE-2025-58146**

There are multiple issues. 1. Updates to the XAPI database sanitise input strings, but try generating the notification using the unsanitised input. This causes the database's event thread to terminate and cease further processing. 2. XAPI's UTF-8 encoder imple

9.4 **CVE-2025-58151**

varstored is a component of the Xapi toolstack handling UEFI Variables for a VM. It has a communication path with OVMF inside the VM involving mapping a buffer prepared by OVMF. Within varstored, there were insufficient compiler barriers, creating TOCTOU issue

**9.4** **CVE-2026-23556**
When oxenstored is tearing a domain down, the node data is cleaned up but the usage counts are leaked. When the domain ID is eventually reused, the new domain can create fewer nodes before beeing deemed to be over quota.

**9.3** **CVE-2026-47646** Microsoft dynamics 365 customer voice
Improper neutralization of input during web page generation ('cross-site scripting') in Dynamics 365 Customer Voice allows an unauthorized attacker to perform spoofing over a network.

**9.3** **CVE-2026-2342**
Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in OceanicSoft Informatics Systems Ltd. ValeApp allows Stored XSS. This issue affects ValeApp: through 09072026. NOTE: The vendor was contacted early about this

**9.1** **CVE-2026-47826** Cloudfoundry bosh cli
The blobs.yml path key traversal vulnerability in the BOSH CLI tool allows an attacker to write arbitrary files and exfiltrate sensitive information. Affected versions: BOSH CLI tool versions prior to v7.10.4.

**9.1** **CVE-2026-14261**
A vulnerability in the Xerte Online Tools allows for authentication bypass and remote code execution via reinstallation through the /setup/ folder, enabling attackers to reinstall the service to a remote database they control.

**9.1** **CVE-2026-51597**
MERCURY MIPC252W IP camera v1.0.5 Build 230306 Rel.79931n does not implement nonce expiration in RTSP Digest authentication. An adjacent network attacker can capture a legitimate authentication exchange and replay the nonce and response values in a new connect

**9.1** **CVE-2026-59826** Metabase metabase
Metabase is an open-source business intelligence and embedded analytics tool. From 1.55.0 until 1.58.15.1, 1.59.12, 1.60.6.3, and 1.61.2, Metabase did not validate unsafe H2 connection properties on one database-creation code path, allowing an authenticated ad

*2 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.