Daily brief, Friday, August 14, 2026

Aug 13, 8:00 PM to Aug 14, 8:00 PM ET

Generated Nov 2, 2026, 1:04 PM ET

0	0	0	17	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

17 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

17

10.0 **CVE-2026-72811**

SiYuan versions <= v3.7.2 contain a SQL injection vulnerability in the backlink/mention search query (kernel/model/backlink.go), which concatenates stored block metadata (title, name, alias, anchor text) and the client-supplied keyword into a SQL MATCH/search

10.0 **CVE-2026-19188**

A critical OS command injection vulnerability has been identified in the Haiwell IoT Cloud HMI Gateway product. The vulnerability exists in the Net Check feature accessible via the /setting endpoint. The cmdPing Socket.io event fails to properly sanitize user-

10.0 **CVE-2026-73678**

MindsDB Minds Platform version 26.1.0 and earlier contains an unauthenticated remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary OS commands by submitting crafted prompts to the unprotected POST /api/v1/responses/ en

9.9 **CVE-2026-19626** Tenable security center

A remote code execution vulnerability exists in Tenable Security Center's report generation functionality. An authenticated, non-administrative user could exploit this issue by supplying specially crafted input that is later processed unsafely during server-si

9.9 **CVE-2026-19681** Tenable security center

An authenticated command injection vulnerability exists in Security Center related to file upload processing. An attacker could exploit this issue by uploading a specially crafted file, potentially resulting in arbitrary command execution on the underlying ope

9.9 **CVE-2026-19682** Tenable security center

A command injection vulnerability exists in Security Center where a remote, unauthenticated attacker could exploit this issue to execute arbitrary commands on the underlying operating system with the privileges of the service account.

9.9 **CVE-2026-17186** Ibm db2 mirror for i

IBM Db2 Mirror for i 7.4, 7.5, and 7.6 could allow a remote attacker to execute arbitrary CL commands due to improper neutralization of special elements in a command.

9.8 **CVE-2026-12949**

The Wishlist Member plugin for WordPress is vulnerable to Account Takeover via Insufficient Verification of Data Authenticity in versions up to and including 3.34.1. This is due to the wpm_register() function validating the registration cookie only against the

9.8 **CVE-2026-48528**

Metacat is data repository software that helps researchers preserve, share, and discover data. Metacat versions 2.0.0 through 3.4.0 contain an unauthenticated SQL injection vulnerability in the `/cn/v1/object` and `/cn/v2/object` REST API endpoints due to unsa

9.8 **CVE-2026-73849**

Emlog is an open source website building system. In 2.6.26 and earlier, install.php accepts action=reinstall without authentication and deliberately skips the already-installed check because the guard runs only when $act != 'reinstall'. A remote attacker can s

9.8 **CVE-2026-50027**

mcp-memory-service is a semantic memory layer for AI applications. Prior to 10.67.1, all HTTP routes under /api/documents/* in mcp-memory-service are served without any authentication dependency, even when the server is configured with an API key (MCP_API_KEY)

9.8 **CVE-2026-17182** Ibm db2 mirror for i

IBM Db2 Mirror for i 7.4, 7.5, and 7.6 could allow a remote attacker to bypass authentication and obtain or alter sensitive information due to improper validation of request URI path segments.

9.8 **CVE-2026-17184** Ibm db2 mirror for i

IBM Db2 Mirror for i 7.4, 7.5, and 7.6 could allow a remote attacker to execute arbitrary code due to external control of file name or path.

9.3 **CVE-2026-19871**

Use of Hard-coded Credentials in the human resources component in Roskus Prospero Flow CRM before 5.15.9 allows unauthenticated remote attackers to authenticate as any employee onboarded through the standard flow, knowing only their email address, because the

9.3 **CVE-2026-17181** Ibm db2 mirror for i

IBM Db2 Mirror for i 7.4, 7.5, and 7.6 could allow a remote attacker to write files to arbitrary locations due to path traversal.

9.2 **CVE-2026-67365**

Joomla Extension - icagenda.com - Unauthenticated SQL injection in iCagenda < 4.0.0-4.0.11 - Unauthenticated SQL injection in mod_icagenda_calendar (iCagenda), reachable via com_ajax with no session, token or account.

9.1 **CVE-2026-49457**

erlang_quic is a pure Erlang QUIC implementation. Prior to version 1.4.4, the QUIC client did not authenticate the server during the TLS 1.3 handshake. The CertificateVerify signature was not checked, the certificate chain was not validated, and the hostname w

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.