Daily brief, Wednesday, August 19, 2026

Aug 18, 8:00 PM to Aug 19, 8:00 PM ET

Generated Nov 2, 2026, 8:21 AM ET

0	1	0	109	0	2
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 109 new critical CVEs, 2 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

9.3 **CVE-2026-64849** MLflow MLflow CISA KEV DETECTION

An attacker can reach internal or cloud metadata services on MLflow.

New public exploit code

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

New critical CVEs

109

9.3 **CVE-2026-64849** MLflow MLflow KEV EXPLOIT CODE DETECTION

An attacker can reach internal or cloud metadata services on MLflow.

10.0 **CVE-2026-18051** Unknown W3 Total Cache EXPLOIT CODE DETECTION

The W3 Total Cache WordPress plugin before 2.10.5 does not properly validate the request path it uses to build cache file names, allowing unauthenticated attackers to write a file into any existing directory on the server, inside or outside the web root, overw

9.4 **CVE-2026-76310** Splunk splunk

+1 more CVEs in the same release

In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, an unauthenticated user who has an embedded report token could download the associated search job dispatch archive, recover session material, and use it to access all relevant data availab

9.4 **CVE-2026-76312** Splunk splunk

In Splunk Enterprise versions below 10.4.1, 10.2.6, 10.0.9, and 9.4.14, an unauthenticated user who can read the Hypertext Markup Language (HTML) source of a page that embeds a Splunk report could use exposed session material to access all relevant data and af

9.1 **CVE-2026-76404** Splunk model context protocol server

In Splunk MCP Server app versions below 1.2.1, a user who holds the "admin" Splunk role could execute arbitrary commands on the underlying operating system. The vulnerability is possible because of missing input validation in the app's credential management co

9.8 **CVE-2026-63722** ICEcoder ICEcoder

ICEcoder 8.1 contains an unauthenticated remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary OS commands by chaining an authentication bypass, CSRF validation bypass, and unsanitized command execution. Attackers can s

9.8 **CVE-2026-16845** Ibm aix

IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to a heap buffer overflow.

9.8 **CVE-2026-16862** Ibm aix

+4 more CVEs in the same release

IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to a stack buffer overflow.

9.8 **CVE-2026-16872** Ibm vios

IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to a stack-based buffer overflow.

9.8 **CVE-2026-16840** Ibm aix

IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to an out-of-bounds write.

9.8 **CVE-2026-16917** Ibm vios

IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to an integer overflow.

9.8 **CVE-2026-16919** Ibm aix

IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to improper validation of network-supplied pointers.

9.8 **CVE-2026-16834** Ibm aix

IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service due to an integer underflow.

9.1 **CVE-2026-71960** Shenzhen Cudy Technology WR3000 2.0

Cudy WR3000 2.0 running firmware before 2.5.24 contains a hard-coded JWT HMAC signing secret vulnerability in the Mosquitto MQTT broker's authentication plugin that allows unauthenticated attackers to forge valid JWT tokens by extracting the secret from the fi

9.4 **CVE-2026-16839** Ibm aix

IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to obtain sensitive information due to an integer underflow in the IPv4 IP-options parser.

9.8 **CVE-2026-58081** Freebsd freebsd

Several encoding modules, including HZ, UTF-7, VIQR, and ZW, did not properly check the size of the caller-supplied output buffer before writing converted characters. An application that uses iconv(3) to convert untrusted input to or from one of the affected e

9.8 **CVE-2026-58082** Freebsd freebsd

The ISO-2022 encoding module used a stack buffer sized to MB_LEN_MAX (6 bytes) for intermediate character output. Some ISO-2022 variants can require up to 10 bytes per character, in which case conversions can trigger a stack buffer overflow of up to four bytes

9.8 **CVE-2026-72889**

Net::OAuth versions before 0.33 for Perl allow the sender to choose the signature algorithm in verify. verify resolves the signature method class from the signature_method parameter of the incoming message. signature_method is required on every request, so the

9.1 **CVE-2026-75595** Netty netty

Product not on watchlist.

10.0 **CVE-2026-76008**

A flaw has been found in Comfast CF-N1-S 2.6.0.1. This affects the function get_para_from_uri of the file /cgi-bin/mbox-config of the component URI Parameter Parsing. This manipulation of the argument width/height causes stack-based buffer overflow. The attack

84 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 2

Oz Hair and Beauty ozhairandbeauty.com 1,988,331 accounts

Fanlore fanlore.org 144,520 accounts

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.