Daily brief, Thursday, July 30, 2026

Jul 29, 8:00 PM to Jul 30, 8:00 PM ET

Generated Nov 3, 2026, 3:44 AM ET

0	0	0	117	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

117 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

117

9.8 **CVE-2026-59309** VMware Cloud Foundation

Product not on watchlist.

9.3 **CVE-2026-47876** VMware Cloud Foundation

Product not on watchlist.

10.0 **CVE-2026-66803** Microsoft azure cosmos db

Improper access control in Azure Cosmos DB allows an unauthorized attacker to execute code over a network.

9.8 **CVE-2026-17543** Php php

Improper escaping of backslashes in attacker-provided parameters would allow for trivial SQL injection in PHP versions from 8.2.* before 8.2.33, from 8.3.* before 8.3.33, from 8.4.* before 8.4.24, and from 8.5.* before 8.5.9.

9.8 **CVE-2026-17544** Php php

Attacker-provided inputs to bccomp() could lead to an out-of-bounds write with stack and heap corruption in PHP versions from 8.4.* before 8.4.24 and from 8.5.* before 8.5.9.

9.6 **CVE-2026-17651** Google chrome

Insufficient validation of untrusted input in Dawn in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)

9.6 **CVE-2026-17652** Google chrome

+1 more CVEs in the same release

Use after free in Views in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)

9.6 **CVE-2026-17655** Google chrome

+1 more CVEs in the same release

Insufficient validation of untrusted input in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)

9.6 **CVE-2026-17656** Google chrome

Use after free in Ozone in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)

9.6 **CVE-2026-17669** Google chrome

Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.6 **CVE-2026-17671** Google chrome

Insufficient validation of untrusted input in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.6 **CVE-2026-17672** Google chrome

Insufficient validation of untrusted input in Chromecast in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Hi

9.6 **CVE-2026-17673** Google chrome

Integer overflow in QUIC in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.6 **CVE-2026-17675** Google chrome

Out of bounds write in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.6 **CVE-2026-17676** Google chrome

Inappropriate implementation in ANGLE in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.6 **CVE-2026-17680** Google chrome

Heap buffer overflow in Color in Google Chrome on ChromeOS prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.6 **CVE-2026-17681** Google chrome

Insufficient validation of untrusted input in Web Authentication in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium se

9.6 **CVE-2026-17682** Google chrome

Integer overflow in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.6 **CVE-2026-17684** Google chrome

Insufficient validation of untrusted input in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security s

9.6 **CVE-2026-17687** Google chrome

Type Confusion in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

95 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.