Daily brief, Wednesday, July 1, 2026

Jun 30, 8:00 PM to Jul 1, 8:00 PM ET

Generated Nov 4, 2026, 6:07 AM ET

0	1	0	55	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 55 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

8.8 **CVE-2026-45659** Microsoft SharePoint Server CISA KEV DETECTION

An attacker gains arbitrary code execution in SharePoint Server.

New public exploit code

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

New critical CVEs

55

9.8 **CVE-2026-58457** Shenzhen Aitemi E Commerce M300 Wi-Fi Repeater EXPLOIT CODE

Shenzhen Aitemi M300 Wi-Fi Repeater (hardware model MT02) contains an unauthenticated OS command injection vulnerability that allows network-adjacent attackers to execute arbitrary shell commands by injecting unsanitized input through the smacfilter_conf handl

9.8 **CVE-2026-51947** EXPLOIT CODE

An issue in Pivotal CRM 6.6.4.08 and systems using patch-ghi-15381-cwe-502-20251225.zip (fixed in Pivotal CRM 6.6.5.10 and Patch_CWE502_20260316.zip) allows a remote attacker to execute arbitrary code via the Pivotal.Engine.Client.Services.Conversion.dll compo

9.6 **CVE-2026-14392** Google chrome

Out of bounds write in Tint in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.6 **CVE-2026-14387** Google chrome

Integer overflow in Skia in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)

9.6 **CVE-2026-14382** Google chrome

+1 more CVEs in the same release

Insufficient validation of untrusted input in ANGLE in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.6 **CVE-2026-14390** Google chrome

+2 more CVEs in the same release

Use after free in ANGLE in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.6 **CVE-2026-14397** Google chrome

Out of bounds write in ANGLE in Google Chrome on Mac prior to 150.0.7871.46 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)

9.4 **CVE-2026-53488** Containerd containerd

Product not on watchlist.

9.8 **CVE-2026-53355** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: net: rds: clear i_sends on setup unwind The RDS IB connection teardown path is written so it can run during partial startup and on repeated shutdown attempts. It uses NULL pointers to distingu

9.6 **CVE-2026-14405** Google chrome

Uninitialized Use in V8 in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Low)

9.6 **CVE-2026-14416** Google chrome

Out of bounds read in Dawn in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Low)

9.6 **CVE-2026-14417** Google chrome

Use after free in Dawn in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)

9.6 **CVE-2026-14419** Google chrome

Use after free in Skia in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)

9.6 **CVE-2026-14420** Google chrome

Out of bounds read and write in Dawn in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)

9.6 **CVE-2026-14423** Google chrome

Type Confusion in Tint in Google Chrome prior to 150.0.7871.46 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.6 **CVE-2026-14424** Google chrome

Use after free in Dawn in Google Chrome on Mac prior to 150.0.7871.46 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.8 **CVE-2026-52186**

SQL Injection vulnerability in UTT nv518G nv518GV3v3.2.7-210919-161313 allows a remote attacker to execute arbitrary code via the gohead/sub_463bbc component

9.8 **CVE-2026-58521** Mediawiki cargo

+1 more CVEs in the same release

Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in The Wikimedia Foundation Mediawiki - Cargo Extension allows SQL Injection. This issue affects Mediawiki - Cargo Extension: from * before 1.43.9,1.44.6,1.45.4.

10.0 **CVE-2026-50160** Hoppscotch hoppscotch DETECTION

Hoppscotch is an API development ecosystem. In self-hosted deployments of hoppscotch-backend from version 2026.4.1 and earlier, the unauthenticated POST /v1/onboarding/config endpoint is vulnerable to mass assignment. The global NestJS ValidationPipe is config

9.8 **CVE-2026-7840** Uvnc ultravnc

UltraVNC repeater through 1.8.2.2 contains a global buffer overflow in its embedded HTTP administration server. The functions wi_senderr() and wi_replyhdr() in repeater/webgui/webutils.c write the caller-supplied HTTP request URI into a fixed 1000-byte global

31 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.