Daily brief, Tuesday, August 25, 2026

Aug 24, 8:00 PM to Aug 25, 8:00 PM ET

Generated Nov 2, 2026, 3:01 AM ET

0	1	0	90	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 90 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

9.8 **CVE-2026-60004** Gitea Gitea CISA KEV DETECTION

An attacker with repository write access can run shell commands as the Gitea service account.

New public exploit code

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

New critical CVEs

90

9.8 **CVE-2026-60004** Gitea Gitea KEV EXPLOIT CODE DETECTION

An attacker with repository write access can run shell commands as the Gitea service account.

9.8 **CVE-2026-63073** OpenSSL OpenSSL

Product not on watchlist.

9.6 **CVE-2026-78904** Google Chrome

Product not on watchlist.

9.6 **CVE-2026-78948** Google Chrome

Product not on watchlist.

9.6 **CVE-2026-78900** Google Chrome

Product not on watchlist.

9.6 **CVE-2026-78909** Google Chrome
+2 more CVEs in the same release
Product not on watchlist.

9.6 **CVE-2026-78939** Google Chrome
Product not on watchlist.

9.6 **CVE-2026-78951** Google Chrome
Product not on watchlist.

9.6 **CVE-2026-78964** Google Chrome
Product not on watchlist.

9.8 **CVE-2026-79090** Google chrome
Improper privilege management in Actor in Google Chrome prior to 152.0.7977.65 allowed a remote attacker leveraging social engineering to bypass system access restrictions via a crafted HTML page. (Chromium security severity: Low)

9.8 **CVE-2026-79152** Google chrome
Incorrect authorization in CustomTabs in Google Chrome on on Android prior to 152.0.7977.65 allowed a local attacker to bypass web origin policy via a co-installed app. (Chromium security severity: Low)

9.8 **CVE-2026-65637** Apache tomcat
Improper Input Validation vulnerability in Apache Tomcat due to incomplete fix for CVE-2026-32990. This issue affects Apache Tomcat: from 11.0.20 through 11.0.24, from 10.1.53 through 10.1.57, from 9.0.115 through 9.0.120. Users are recommended to upgrade to v

9.8 **CVE-2026-65905** Apache tomcat
Authentication Bypass by Capture-replay vulnerability in Apache Tomcat's DIGEST authenticator. If, before windowSize requests have been made, a client makes a DIGEST authenticated request with a nonceCount on the upper boundary of the replay window then that r

9.6 **CVE-2026-78935** Google chrome
Use of uninitialized variable in Mobile in Google Chrome on on iOS prior to 152.0.7977.65 allowed a remote attacker to potentially execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: Critical)

9.6 **CVE-2026-78937** Google chrome
Use after free in Search in Google Chrome on on Android prior to 152.0.7977.65 allowed a remote attacker leveraging social engineering to potentially execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: Medium)

9.6 **CVE-2026-78985** Google chrome
Incorrect reference resolution in FileSystem in Google Chrome prior to 152.0.7977.65 allowed a remote attacker leveraging social engineering to potentially execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: Medium)

9.6 **CVE-2026-78989** Google chrome

Out of bounds read in ANGLE in Google Chrome on on Windows prior to 152.0.7977.65 allowed a remote attacker to potentially execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)

9.6 **CVE-2026-79012** Google chrome

Use after free in Safebrowsing in Google Chrome on on Mac prior to 152.0.7977.65 allowed a remote attacker leveraging social engineering to execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: Critical)

9.6 **CVE-2026-79019** Google chrome

+1 more CVEs in the same release

Out of bounds write in ANGLE in Google Chrome on on Windows prior to 152.0.7977.65 allowed a remote attacker to potentially execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)

9.6 **CVE-2026-79026** Google chrome

Use after free in Extensions in Google Chrome prior to 152.0.7977.65 allowed a remote attacker leveraging social engineering to potentially execute arbitrary code outside the sandbox via a crafted Chrome extension. (Chromium security severity: High)

67 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

Carhartt carhartt.com 12,933,413 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.