Daily brief, Tuesday, June 30, 2026

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

Generated Nov 4, 2026, 6:55 AM ET

0	0	0	89	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

89 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

89

10.0 **CVE-2026-10134** IBM Langflow OSS EXPLOIT CODE

Product not on watchlist.

9.9 **CVE-2026-7873** IBM Langflow OSS EXPLOIT CODE DETECTION

Product not on watchlist.

10.0 **CVE-2026-13782** Google chrome

Use after free in Browser in Google Chrome prior to 150.0.7871.47 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)

9.8 **CVE-2026-8655** Citrix netscaler application delivery controller

Multiple Memory overflow vulnerabilities in NetScaler ADC and NetScaler Gateway leading to unpredictable or erroneous behavior and Denial of Service if NetScaler ADC is configured as an LB of type Oracle OR NetScaler ADC is configured as a DNS Proxy OR NetScal

9.8 **CVE-2026-14241** Mozilla firefox

Memory safety bugs present in Firefox 152.0.3. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability was fixed in Firefox 152.0.4.

9.8 **CVE-2026-13775** Google chrome

+1 more CVEs in the same release

Use after free in GPU in Google Chrome prior to 150.0.7871.47 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)

9.8 **CVE-2026-13776** Google chrome

Type Confusion in Dawn in Google Chrome prior to 150.0.7871.47 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)

9.8 **CVE-2026-14104** Google chrome

Insufficient validation of untrusted input in WebAppInstalls in Google Chrome prior to 150.0.7871.47 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Low)

9.8 **CVE-2026-14121** Google chrome

Use after free in Chromoting in Google Chrome on Linux prior to 150.0.7871.47 allowed a remote attacker to execute arbitrary code via malicious network traffic. (Chromium security severity: Low)

9.6 **CVE-2026-13780** Google chrome

Insufficient validation of untrusted input in ANGLE in Google Chrome prior to 150.0.7871.47 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critica

9.6 **CVE-2026-13781** Google chrome

Insufficient validation of untrusted input in Skia in Google Chrome prior to 150.0.7871.47 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-2026-13785** Google chrome

Use after free in Bluetooth in Google Chrome on Mac prior to 150.0.7871.47 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)

9.6 **CVE-2026-13792** Google chrome

Use after free in Touchbar in Google Chrome on Mac prior to 150.0.7871.47 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.6 **CVE-2026-13796** Google chrome

Integer overflow in Chromecast in Google Chrome prior to 150.0.7871.47 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-2026-13797** Google chrome

Insufficient validation of untrusted input in Chromecast in Google Chrome prior to 150.0.7871.47 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-2026-13798** Google chrome

Heap buffer overflow in Chromecast in Google Chrome prior to 150.0.7871.47 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-2026-13843** Google chrome

Insufficient validation of untrusted input in Chrome for iOS in Google Chrome on iOS prior to 150.0.7871.47 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-2026-13846** Google chrome

+1 more CVEs in the same release

Use after free in USB in Google Chrome on Mac prior to 150.0.7871.47 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-2026-13853** Google chrome

Use after free in Journeys in Google Chrome prior to 150.0.7871.47 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-2026-13854** Google chrome

Use after free in Ozone in Google Chrome on Linux prior to 150.0.7871.47 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)

67 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.