Daily brief, Tuesday, June 9, 2026

Jun 8, 8:00 PM to Jun 9, 8:00 PM ET

Generated Nov 5, 2026, 3:25 AM ET

0	3	0	43	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

3 newly exploited, 43 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

3

8.8 **CVE-2026-11645** Google Chromium V8 CISA KEV

An attacker gets remote code execution on Google Chromium V8 with user interaction.

7.8 **CVE-2026-20245** Cisco Catalyst SD-WAN Manager CISA KEV

An authenticated, local attacker executes arbitrary commands as root by supplying a crafted file to Cisco's Catalyst SD-WAN Manager.

5.8 **CVE-2026-7473** Arista Extensible Operating System CISA KEV

An attacker gets unauthorized access to an Arista Extensible Operating System switch without authentication or user interaction.

New public exploit code

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

New critical CVEs

43

9.9 **CVE-2026-10523** Ivanti Sentry EXPLOIT CODE

(1) Ivanti Sentry before R10.5.2, R10.6.2, and R10.7.1 versions. (2) An attacker gains full administrative access to the system. (3) Update to Ivanti Sentry version R10.5.2, R10.6.2, or R10.7.1 or later.

9.4 **CVE-2026-44963** Veeam Backup and Replication EXPLOIT CODE

Product not on watchlist.

9.8 **CVE-2026-46325** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: RDMA/rxe: Fix iova-to-va conversion for MR page sizes != PAGE_SIZE The current implementation incorrectly handles memory regions (MRs) with page sizes different from the system PAGE_SIZE. The

9.8 **CVE-2026-44815** Microsoft windows 10 1607

Stack-based buffer overflow in Windows DHCP Client allows an unauthorized attacker to execute code over a network.

9.8 **CVE-2026-45657** Microsoft windows 11 23h2

Use after free in Windows Kernel allows an unauthorized attacker to execute code over a network.

9.8 **CVE-2026-47291** Microsoft windows 10 1607

Integer overflow or wraparound in Windows HTTP.sys allows an unauthorized attacker to execute code over a network.

9.8 **CVE-2026-47643** Microsoft azure stack edge

External control of file name or path in Azure Stack Edge allows an unauthorized attacker to execute code over a network.

9.6 **CVE-2026-11634** Google chrome

Use after free in Gamepad in Google Chrome on Windows prior to 149.0.7827.103 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)

9.6 **CVE-2026-11638** Google chrome

Use after free in Printing in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)

9.6 **CVE-2026-11651** Google chrome

Use after free in Network in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)

9.6 **CVE-2026-11654** Google chrome

Use after free in CameraCapture in Google Chrome on Mac prior to 149.0.7827.103 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.6 **CVE-2026-11659** Google chrome

Integer overflow in UI in Google Chrome on Linux prior to 149.0.7827.103 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.6 **CVE-2026-11671** Google chrome

Use after free in Navigation in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.6 **CVE-2026-11697** Google chrome

Insufficient validation of untrusted input in UI in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.6 **CVE-2026-42904** Microsoft windows 10 21h2

Heap-based buffer overflow in Windows TCP/IP allows an unauthorized attacker to elevate privileges over an adjacent network.

9.3 **CVE-2026-46316** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: vgic-its: Drop the translation cache reference only for the erased entry vgic_its_invalidate_cache() walks the per-ITS translation cache with xa_for_each() and drops the cache's re

9.1 **CVE-2026-34182** Openssl openssl

Issue Summary: Cryptographic Message Services (CMS) processing fails to perform sufficient input validation on the cipher and tag length fields of AuthEnvelopedData containers, leading to various potential compromises. Impact Summary: Attackers making use of t

9.1 **CVE-2026-45602** Microsoft windows 10 1607

No cwe for this issue in Windows DHCP Server allows an unauthorized attacker to perform tampering over a network.

10.0 **CVE-2026-47938** Adobe campaign

Adobe Campaign Classic (ACC) versions 7.4.3 build 9394 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could result in privilege escalation. Exploitation of this issue does not require user interaction. Scope is changed.

10.0 **CVE-2026-48303** Adobe campaign

Adobe Campaign Classic (ACC) versions 7.4.3 build 9394 and earlier are affected by an Incorrect Authorization vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user inter

23 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.