Daily brief, Monday, July 27, 2026

Jul 26, 8:00 PM to Jul 27, 8:00 PM ET

Generated Nov 3, 2026, 6:39 AM ET

0	2	0	89	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 newly exploited, 89 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild 2

10.0 **CVE-2026-16812** Arista VeloCloud Orchestrator CISA KEV

A remote attacker gains access to privileged internal functionality on Arista VeloCloud Orchestrator On-Prem.

5.3 **CVE-2025-68686** Fortinet FortiOS CISA KEV

An attacker gains unauthorized access to sensitive information, including configuration and authentication data, on Fortinet FortiOS.

New public exploit code

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

New critical CVEs 89

10.0 **CVE-2026-16812** Arista VeloCloud Orchestrator KEV

A remote attacker gains access to privileged internal functionality on Arista VeloCloud Orchestrator On-Prem.

9.8 **CVE-2026-43803** Apple iOS and iPadOS

+3 more CVEs in the same release

Product not on watchlist.

9.8 **CVE-2026-64767** Apple macOS

A buffer overflow was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.7.8, macOS Sequoia 15.8.2, macOS Sonoma 14.8.8, macOS Tahoe 26.6. A remote attacker may be able to cause unexpected system termination or corrupt kernel memo

9.8 **CVE-2026-43807** Apple iOS and iPadOS
+1 more CVEs in the same release
Product not on watchlist.

9.8 **CVE-2026-64695** Apple iOS and iPadOS
Product not on watchlist.

9.8 **CVE-2026-43778** Apple iOS and iPadOS
+4 more CVEs in the same release
Product not on watchlist.

9.8 **CVE-2026-64762** Apple iOS and iPadOS
+2 more CVEs in the same release
Product not on watchlist.

9.8 **CVE-2026-64733** Apple iOS and iPadOS
Product not on watchlist.

9.8 **CVE-2026-43730** Apple iOS and iPadOS
Product not on watchlist.

9.8 **CVE-2026-28928** Apple iOS and iPadOS
+3 more CVEs in the same release
Product not on watchlist.

9.8 **CVE-2026-43748** Apple iOS and iPadOS
Product not on watchlist.

9.8 **CVE-2026-64698** Apple macOS
+6 more CVEs in the same release
Product not on watchlist.

9.8 **CVE-2026-64746** Apple iOS and iPadOS
Product not on watchlist.

9.8 **CVE-2026-64702** Apple macOS
Product not on watchlist.

9.3 **CVE-2026-64740** Apple iOS and iPadOS
Product not on watchlist.

9.8 **CVE-2026-28911** Apple macos
The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.8.8, macOS Tahoe 26.6. A malicious app may be able to corrupt memory of a system process.

9.8 **CVE-2026-28982** Apple macos
A race condition was addressed with improved locking. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. A remote user may be able to cause unexpected system termination or corrupt kernel memory.

9.8 **CVE-2026-43750** Apple macos

A buffer overflow was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to execute arbitrary code out of its sandbox or with certain elevated privileges.

9.8 **CVE-2026-43764** Apple macos

+1 more CVEs in the same release

An integer overflow was addressed with improved input validation. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to cause unexpected system termination.

9.8 **CVE-2026-43769** Apple ipados

+1 more CVEs in the same release

An integer overflow was addressed with improved input validation. This issue is fixed in iOS 18.7.10 and iPadOS 18.7.10, iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. An app may b

48 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.