Daily brief, Sunday, August 9, 2026

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

Generated Nov 2, 2026, 5:49 PM ET

0	0	0	13	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

13 new critical CVEs, 1 new breaches.

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

13

9.8 **CVE-2026-71984**

MSI Radix AXE6600 router firmware version v781521 contains a command injection vulnerability in the urlfilter function that allows remote attackers to execute arbitrary commands on the affected device. Attackers can exploit the urlfilter function to inject mal

9.8 **CVE-2026-71985**

MSI Radix AXE6600 router firmware version v781521 contains a command injection vulnerability in the accesscontrol function that allows remote attackers to execute arbitrary commands on the affected device. Attackers can exploit this vulnerability through the a

9.8 **CVE-2026-71986**

MSI Radix AXE6600 router firmware version v781521 contains a command injection vulnerability in the dmz function that allows remote attackers to execute arbitrary commands on the affected device. Attackers can exploit this vulnerability through the dmz functio

9.8 **CVE-2026-71987**

MSI Radix AXE6600 router firmware version v781521 contains a command injection vulnerability in the alg function that allows remote attackers to execute arbitrary commands on the affected device. Attackers can exploit this vulnerability through the alg functio

9.8 **CVE-2026-71988**

MSI Radix AXE6600 router firmware version v781521 contains a command injection vulnerability in the portFw function that allows remote attackers to execute arbitrary commands on the affected device. Attackers can exploit this vulnerability through the alg func

9.8 **CVE-2026-71989**

MSI Radix AXE6600 router firmware version v781521 contains a command injection vulnerability in the porTrigger function that allows remote attackers to execute arbitrary commands on the affected device. Attackers can exploit this vulnerability through the alg

9.8 **CVE-2026-71990**

+1 more CVEs in the same release

MSI Radix AXE6600 router firmware version v781521 contains a command injection vulnerability in the TelnetSSH function used for SSH configuration that allows remote attackers to execute arbitrary commands on the affected device. Attackers can exploit this vuln

9.8 **CVE-2026-71992**

MSI Radix AXE6600 router firmware version v781521 contains a command injection vulnerability in the macfilter function that allows remote attackers to execute arbitrary commands on the affected device. Attackers can exploit the macfilter function to inject mal

9.8 **CVE-2026-71993**

MSI Radix AXE6600 router firmware version v781521 contains a command injection vulnerability in the openvpn function that allows remote attackers to execute arbitrary commands on the affected device. Attackers can exploit the macfilter function to inject malic

9.8 **CVE-2026-15038**

The InfiniteWP Client WordPress plugin before 1.13.6 does not properly verify the site-connection state and the authenticity of requests to its remote-management endpoint on WordPress Multisite installations, allowing unauthenticated attackers to bind their ow

9.8 **CVE-2026-19348**

A security flaw has been discovered in Shenzhen Aitemi M300 Wi-Fi Repeater r0-ea7890a. Impacted is the function sprintf of the file /protocol.csp?fname=net&opt=smacfilter_conf&function=set&act=add&name=test&enable=1. Performing a manipulation of the argument e

9.1 **CVE-2026-18473**

The WP Directory Kit WordPress plugin before 1.5.5 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by unauthenticated users.

Ransomware

No leak-site posts collected.

New data breaches 1

Alcon alcon.com 218,395 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.