Daily brief, Thursday, September 10, 2026

Sep 9, 8:00 PM to Sep 10, 8:00 PM ET

Generated Nov 1, 2026, 11:16 AM ET

0	2	0	4	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 newly exploited, 4 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild 2

9.2 **CVE-2026-86060** MikroTik RouterOS CISA KEV

An attacker can change the trusted RouterOS policy mask and escalate privileges on a MikroTik RouterOS.

8.8 **CVE-2026-67277** MikroTik RouterOS CISA KEV

An attacker can bypass authentication checks on a MikroTik RouterOS system and access kernel memory.

New public exploit code

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

New critical CVEs 4

9.2 **CVE-2026-86060** MikroTik RouterOS KEV EXPLOIT CODE

An attacker can change the trusted RouterOS policy mask and escalate privileges on a MikroTik RouterOS.

9.9 **CVE-2026-89049** AWS Amazon SSM Agent

An attacker can bypass authentication controls on an Amazon SSM Agent server with user interaction.

9.1 **CVE-2026-85228** Amazon Deep Java Library

An integer overflow in the tensor buffer validation component in Amazon Deep Java Library (DJL) from 0.13.0 through 0.36.0 on all platforms might allow a remote unauthenticated actor to obtain information from adjacent process memory or cause a denial of servi

9.6 **CVE-2026-82107** IBM DataStage on Cloud Pak for Data

An attacker can obtain sensitive information and bypass security restrictions without authentication.

Ransomware

No leak-site posts collected.

New data breaches 1

McKesson mckesson.com 6,404,340 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.