Daily brief, Thursday, August 20, 2026

Aug 19, 8:00 PM to Aug 20, 8:00 PM ET

Generated Nov 2, 2026, 7:30 AM ET

0	2	0	79	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 newly exploited, 79 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild 2

9.8 **CVE-2026-72529** TrueConf Server CISA KEV

A remote unauthorized attacker can execute an arbitrary script on TrueConf Server.

9.0 **CVE-2026-72530** TrueConf Server CISA KEV

An unauthorized remote attacker with network access via port 4307/TCP executes arbitrary code on the host system using TrueConf Server.

New public exploit code

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

New critical CVEs 79

9.0 **CVE-2026-72530** TrueConf Server KEV EXPLOIT CODE

An unauthorized remote attacker with network access via port 4307/TCP executes arbitrary code on the host system using TrueConf Server.

9.8 **CVE-2026-72529** TrueConf Server KEV

A remote unauthorized attacker can execute an arbitrary script on TrueConf Server.

10.0 **CVE-2026-69836** Microsoft Microsoft Entra

Product not on watchlist.

9.3 **CVE-2026-66592** rtCamp rtMedia for WordPress, BuddyPress and bbPress

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in rtCamp Inc. rtMedia for WordPress, BuddyPress and bbPress buddypress-media allows Blind SQL Injection.This issue affects rtMedia for WordPress, BuddyPress and

10.0 **CVE-2026-65770** Microsoft azure managed instance for apache cassandra

Improper neutralization of argument delimiters in a command ('argument injection') in Azure Managed Instance for Apache Cassandra allows an unauthorized attacker to execute code over a network.

10.0 **CVE-2026-65801** Microsoft exchange online

Server-side request forgery (ssrf) in Microsoft Exchange Online allows an unauthorized attacker to elevate privileges over a network.

10.0 **CVE-2026-65816** Microsoft azure web apps

Use of incorrectly-resolved name or reference in Azure Arc allows an unauthorized attacker to elevate privileges over a network.

10.0 **CVE-2026-69555** Microsoft azure arc

Incorrect authorization in Azure Arc allows an unauthorized attacker to elevate privileges over a network.

9.9 **CVE-2026-68782** Microsoft azure sql database

+1 more CVEs in the same release

Improper neutralization of special elements used in an sql command ('sql injection') in Azure SQL Database allows an authorized attacker to elevate privileges over a network.

9.9 **CVE-2026-69851** Microsoft entra id

Server-side request forgery (ssrf) in Azure Active Directory allows an authorized attacker to elevate privileges over a network.

9.6 **CVE-2026-69400** Microsoft azure logic apps

Improper limitation of a pathname to a restricted directory ('path traversal') in Azure Logic Apps allows an unauthorized attacker to elevate privileges over a network.

9.3 **CVE-2026-62834** Microsoft azure data factory

Improper verification of cryptographic signature in Azure Data Factory allows an unauthorized attacker to elevate privileges over a network.

9.1 **CVE-2026-66309** Microsoft azure sql database

Improper access control in Azure SQL Database allows an authorized attacker to elevate privileges over a network.

9.8 **CVE-2026-17142** Ibm vios

IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary commands due to improper authentication.

9.8 **CVE-2026-17040** Ibm vios

+2 more CVEs in the same release

IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to a buffer overflow.

9.8 **CVE-2026-17122** Ibm vios

IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to a stack-based buffer overflow.

9.8 **CVE-2026-17118** Ibm vios

IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to a use-after-free vulnerability.

9.8 **CVE-2026-17136** Ibm vios

IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to a format string vulnerability.

9.8 **CVE-2026-17145** Ibm vios

IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to improper privilege management.

9.8 **CVE-2026-15706** Baylan Measuring Instruments Industry and Trade Baylan Smart Meter Manageme…

Missing authentication for critical function vulnerability in Baylan Measuring Instruments Industry and Trade Inc. Baylan Smart Meter Management Application (BMS) allows Authentication Bypass. This issue affects Baylan Smart Meter Management Application (BMS):

56 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.