Daily brief, Friday, August 7, 2026

Aug 6, 8:00 PM to Aug 7, 8:00 PM ET

Generated Nov 2, 2026, 7:54 PM ET

0	1	0	37	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 37 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

9.6 **CVE-2026-8037** Progress LoadMaster CISA KEV DETECTION

An attacker gains remote code execution on Progress LoadMaster without authentication.

New public exploit code

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

New critical CVEs

37

9.6 **CVE-2026-8037** Progress LoadMaster KEV EXPLOIT CODE DETECTION

An attacker gains remote code execution on Progress LoadMaster without authentication.

9.8 **CVE-2026-19264** Gitroomhq postiz-app EXPLOIT CODE

Postiz is an open-source social media scheduling tool. The route that serves locally stored media joins URL-supplied path segments onto the upload directory and streams the file without normalising the path or confining it to that directory, and the route requ

10.0 **CVE-2026-56162** Microsoft azure sql database

Improper authentication in Azure SQL Database allows an unauthorized attacker to elevate privileges over a network.

10.0 **CVE-2026-65667** Microsoft teams

Missing authorization in Microsoft Teams allows an unauthorized attacker to elevate privileges over a network.

9.9 **CVE-2026-50481** Microsoft azure active directory
Modification of assumed-immutable data (maid) in Azure Active Directory allows an authorized attacker to elevate privileges over a network.

9.9 **CVE-2026-50515** Microsoft azure service bus
Deserialization of untrusted data in Azure Service Bus allows an authorized attacker to execute code over a network.

9.9 **CVE-2026-59115** Microsoft entra provisioning service
'.../...//' in Microsoft Entra Provisioning Service (SyncFabric) allows an authorized attacker to elevate privileges over a network.

9.9 **CVE-2026-62830** Microsoft azure sre agent
Missing authorization in Azure SRE Agent allows an authorized attacker to elevate privileges over a network.

9.8 **CVE-2026-62873** Microsoft windows admin center
Improper verification of cryptographic signature in Microsoft 365 Admin Center allows an unauthorized attacker to elevate privileges over a network.

9.6 **CVE-2026-56161** Microsoft azure logic apps
Improper access control in Azure Logic Apps allows an authorized attacker to disclose information over a network.

9.6 **CVE-2026-62896** Microsoft teams
Improper authentication in Microsoft Teams allows an authorized attacker to elevate privileges over a network.

9.6 **CVE-2026-70332** Microsoft sharepoint online
Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an unauthorized attacker to perform spoofing over a network.

9.1 **CVE-2026-68823** Microsoft azure confidential ledger
Exposed dangerous method or function in Azure Confidential Ledger allows an authorized attacker to execute code over a network.

9.0 **CVE-2026-71851** Brix crypto-js
crypto-js is a JavaScript library of crypto standards. Versions of crypto-js prior to 4.0.0 generate randomness in CryptoJS.lib.WordArray.random() using a custom variation of the Multiply-With-Carry pseudorandom number generator, seeded from Math.random(), ins

9.9 **CVE-2026-64637** WebPros Plesk
Improper privilege management in the XML-RPC API of Plesk before 18.0.80, allows an authenticated reseller to obtain an administrative session for the root user account.

10.0 **CVE-2026-63508** Microsoft planetary computer
Missing authentication for critical function in Microsoft Planetary Computer Pro allows an unauthorized attacker to elevate privileges over a network.

9.8 **CVE-2026-14364**
The TrueBooker – Appointment Booking and Scheduler System plugin for WordPress is vulnerable to account takeover via improper password reset validation in all versions up to, and including, 1.2.3. This is due to the plugin not properly validating a user's iden

9.8 **CVE-2026-14365**

The TrueBooker – Appointment Booking and Scheduler System plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.2.3. This is due to the plugin not properly verifying that a user is authorized to perform an action. T

9.8 **CVE-2026-14205**

The WP Events Manager WordPress plugin before 2.2.5 does not validate the requested quantity when registering for a paid event and computes the price from the attacker-controlled quantity, allowing any authenticated user to create a completed booking for a pai

9.8 **CVE-2026-16258**

The Ajax Search Lite WordPress plugin before 4.14.5 does not prevent the deserialization of untrusted input, allowing unauthenticated attackers to perform PHP Object Injection. When a suitable POP chain is present via another installed Ajax Search Lite WordPre

17 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

Exact Sciences exactsciences.com 10,869,543 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.