Daily brief, Tuesday, August 11, 2026

Aug 10, 8:00 PM to Aug 11, 8:00 PM ET

Generated Nov 2, 2026, 3:43 PM ET

0	3	0	58	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

3 newly exploited, 58 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

3

10.0 **CVE-2026-72898** Metabase Metabase CISA KEV DETECTION

An unauthenticated attacker gains administrator access to Metabase.

8.6 **CVE-2026-20349** Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Fir… CISA KEV

An unauthenticated attacker causes a denial of service on Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD).

7.0 **CVE-2026-68820** Microsoft Windows Ancillary Function Driver for WinSock CISA KEV

Microsoft Windows Ancillary Function Driver for WinSock contains a use-after-free vulnerability that allows an authorized attacker to elevate privileges locally.

New public exploit code

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

New critical CVEs

58

10.0 **CVE-2026-72898** Metabase Metabase KEV EXPLOIT CODE DETECTION

An unauthenticated attacker gains administrator access to Metabase.

9.4 **CVE-2026-66147** SonicWall GMS

Product not on watchlist.

9.1 **CVE-2026-44758** SAP SE SAP Manufacturing Integration and Intelligence

SAP Manufacturing Integration and Intelligence (MII) allows an attacker with high privileges to submit specially crafted input to certain affected functionality, which is processed without sufficient validation. Successful exploitation could allow the attacker

9.1 **CVE-2026-66145** SonicWall GMS

Product not on watchlist.

9.8 **CVE-2026-34265** SAP SE SAP NetWeaver and ABAP Platform

SAP NetWeaver Application Server ABAP allows an unauthenticated attacker to exploit logical errors in DIAG protocol parsing, resulting in memory corruption. This vulnerability could potentially disclose sensitive system information or crash the system, leading

9.8 **CVE-2026-59124** Microsoft windows app

Deserialization of untrusted data in Microsoft High Performance Computing (HPC) Pack allows an unauthorized attacker to execute code over a network.

9.8 **CVE-2026-62815** Microsoft windows 11 23h2

Use after free in Microsoft QUIC allows an unauthorized attacker to execute code over a network.

9.8 **CVE-2026-62878** Microsoft windows 10 1607

Stack-based buffer overflow in Windows DNS allows an unauthorized attacker to execute code over a network.

9.8 **CVE-2026-62893** Microsoft windows 10 1607

Use after free in Windows Deployment Services allows an unauthorized attacker to execute code over a network.

9.8 **CVE-2026-65791** Microsoft windows 10 1607

Heap-based buffer overflow in Windows iSCSI Target Service allows an unauthorized attacker to execute code over a network.

9.4 **CVE-2026-50516** Microsoft azure kubernetes service

Incorrect authorization in Microsoft Azure Kubernetes Service allows an authorized attacker to elevate privileges over a network.

9.3 **CVE-2026-70306** Microsoft sharepoint server

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-2026-71290** Apache httpclient

Improper TLS hostname verification vulnerability in Apache HttpComponents Client 5.4 or newer. HostnameVerificationPolicy#BUILTIN setting has no effect when used with the async version of HttpClient. An attacker that can intercept and modify traffic between th

9.9 **CVE-2026-72765** N8n n8n

n8n before 2.31.5 and before 2.32.1 contain a sandbox escape vulnerability in expression evaluation. An authenticated user with permission to create or modify workflows can craft expressions using arrow-function bodies to bypass the expression sandbox, trigger

9.8 **CVE-2026-10579** Red Hat Red Hat JBoss Enterprise Application Platform 7.4.25

A flaw was found in Picketlink Federation SAML; the unsolcited response handler would accept forged assertions with no verification or validation, permitting an unauthed attacker to authenticate as any principal in any role. This could lead to information disc

10.0 **CVE-2026-58231**

SAP Commerce Cloud allows an unauthenticated attacker to abuse a default authentication client and submit specially crafted input to certain functions lacking sufficient validation. Successful exploitation could enable arbitrary code execution and compromise i

10.0 **CVE-2026-58115**

A vulnerability has been identified in SIMATIC IoT2050 Advanced (6ES7647-0BA00-1YA2) (All versions < V4.3.4.1 running Industrial OS with Node-RED installed). Affected devices do not enforce authentication on the Node-RED HTTP interface, allowing unauthenticate

10.0 **CVE-2026-48056**

Streambert is a cross-platform Electron Desktop App to stream and download video content. Versions prior to 2.5.0 improperly validate executable paths supplied to the run-download IPC handler, allowing a compromised renderer process to execute arbitrary local

10.0 **CVE-2026-17061**

A Deserialization of Untrusted Data vulnerability affecting SIMULIA Execution Engine from Release 2023 through Release 2026 could lead to an unauthenticated remote code execution.

10.0 **CVE-2026-20702** Intel data center attestation primitives

Protection mechanism failure for some Intel(R) Data Center Attestation Primitives (Intel(R) DCAP) may allow information disclosure. Unprivileged software adversary with an unauthenticated user combined with a low complexity attack may enable data exposure. Thi

38 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.