Daily brief, Wednesday, August 26, 2026

Aug 25, 8:00 PM to Aug 26, 8:00 PM ET

Generated Nov 2, 2026, 2:15 AM ET

0	6	0	81	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

6 newly exploited, 81 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

6

8.8 **CVE-2019-1068** Microsoft SQL Server CISA KEV

An attacker gets remote code execution in the SQL Server Database Engine service account.

8.8 **CVE-2026-8452** Citrix NetScaler ADC and NetScaler Gateway CISA KEV DETECTION

An attacker can execute arbitrary code on a Citrix NetScaler ADC or Gateway system.

8.1 **CVE-2021-23758** Ajax.NET Professional Ajax.NET Professional CISA KEV DETECTION

An attacker can execute arbitrary code on an Ajax.NET Professional server via deserialization of untrusted data.

7.8 **CVE-2022-0995** Linux Kernel CISA KEV

A local user gains privileged access or causes a denial of service on the system due to an out-of-bounds memory write in the Linux Kernel.

7.8 **CVE-2015-5287** Red Hat Automatic Bug Reporting Tool CISA KEV

An attacker gains local privileges via a symlink attack on a file with a predictable name in Red Hat's Automatic Bug Reporting Tool.

7.4 **CVE-2015-3246** Red Hat Libuser CISA KEV

An authenticated local user can corrupt the /etc/passwd file to cause a denial of service or privilege escalation on Red Hat Libuser.

New public exploit code

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

New critical CVEs 81

9.3 **CVE-2026-65641** Veeam One
Product not on watchlist.

10.0 **CVE-2026-77537**
A malicious actor with access to the network could exploit an Improper Input Validation vulnerability found in UniFi Protect Application to execute a Command Injection on the host device.

10.0 **CVE-2026-77550**
A malicious actor with access to the network could exploit an Improper Neutralization of CRLF Sequences vulnerability found in certain devices running UniFi OS to bypass authentication to such UniFi OS devices or instances.

10.0 **CVE-2026-77554**
A malicious actor with access to the network could exploit an Improper Input Validation vulnerability found in UniFi Talk Application to execute a Command Injection on the host device.

10.0 **CVE-2026-65956**
KubePi is a Kubernetes multi-cluster management panel. In versions up to and including 1.6.15, the SSO configuration API endpoints are exposed on the same public routing boundary as the SSO login and callback endpoints, so SSO, OIDC, and SAML management operat

9.9 **CVE-2026-77533**
+4 more CVEs in the same release
A malicious actor with access to the network and low privileges could exploit an Improper Input Validation vulnerability found in UniFi Protect Application to execute a Command Injection on the host device.

9.9 **CVE-2026-77534**
+2 more CVEs in the same release
A malicious actor with access to the network and low privileges could exploit an Improper Access Control vulnerability found in certain devices running UniFi OS to escalate privileges within such UniFi OS devices or instances.

9.9 **CVE-2026-65646**
Improper neutralization of special elements in in Plesk's DNS zone management functionality allows remote authenticated users to disclose arbitrary local files and escalate privileges.

9.8 **CVE-2026-19632** DETECTION
The TranslatePress – Translate Multilingual sites with AI Translation plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.3.1 via the 'trp_get_translations_regular' AJAX action. This makes it possible fo

9.8 **CVE-2026-18431**
The Avada theme for WordPress is vulnerable to Arbitrary File Write in all versions up to, and including, 7.16 when the Fusion Builder plugin is installed and active in versions up to, and including, 3.16. This is due to a chain of authorization and input vali

9.8 **CVE-2026-80235**

EFence developed by Thinking Software Technology has an Arbitrary File Upload vulnerability. Unauthenticated remote attackers can upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.

9.8 **CVE-2026-59683**

The OpenRGB network protocol allows to write attacker controlled strings into arbitrary file system paths (extension of CVE-2026-59682). This allows either a full system compromise from local or remote (if the daemon is running as root) or a full account takeo

9.8 **CVE-2026-80349**

TarsWeb decides whether a request comes from a trusted local caller using a client-controlled header. app.js sets Koa's proxy option to true without naming which upstream proxies may be trusted and without limiting the number of forwarded hops, so the request

9.8 **CVE-2026-18080**

The ERP: Complete HR, Accounting & CRM Suite Built for WooCommerce plugin for WordPress is vulnerable to Unrestricted File Type Upload in all versions up to, and including, 1.17.8 via the save_attachments() function. This is due to missing file extension valid

9.8 **CVE-2026-77552**

A malicious actor with access to the network could exploit an Improper Input Validation vulnerability found in UniFi Enterprise Audio/Video Bridge to execute a Command Injection on the device.

9.8 **CVE-2026-77557**

A malicious actor with access to the network could exploit an Improper Access Control vulnerability found in UniFi Protect AI Key to escalate privileges on the device.

9.8 **CVE-2026-80203**

The getgrav/grav-plugin-api plugin before 1.0.18 does not enforce API-key scope in the requireNotSuperTarget() function in UsersController.php across seven sensitive user-management endpoints. The check uses isSuperAdmin() on the acting account rather than ver

9.8 **CVE-2026-74737**

In the Linux kernel, the following vulnerability has been resolved: net: ethernet: ti: am65-cpsw-nuss: Fix port_id extraction from SRC TAG On the packet reception path, the ID of the MAC Port on which the packet was received, is embedded in the RX DMA Descript

9.8 **CVE-2026-74743**

In the Linux kernel, the following vulnerability has been resolved: macvlan: inherit needed_headroom and needed_tailroom from lowerdev macvlan devices inherit hard_header_len from lowerdev during macvlan_init(), but leave needed_headroom and needed_tailroom se

9.8 **CVE-2026-74744**

In the Linux kernel, the following vulnerability has been resolved: ipvlan: inherit needed_headroom and needed_tailroom from phy_dev ipvlan devices inherit hard_header_len from phy_dev during ipvlan_init(), but leave needed_headroom and needed_tailroom set to

55 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.