# Daily brief, Friday, August 28, 2026

Aug 27, 8:00 PM to Aug 28, 8:00 PM ET

Generated Nov 2, 2026, 12:14 AM ET

| 0 | 0 | 0 | 74 | 0 | 0 |
|---|---|---|---|---|---|
| Breaking | Newly exploited | Exploit code | Critical CVEs | Ransomware posts | New breaches |

74 new critical CVEs.

## Breaking

*Nothing spreading fast in technology large companies run.*

## Newly exploited in the wild

*No CVEs added to CISA's known-exploited list.*

## New public exploit code

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

## New critical CVEs

74

**9.0** **CVE-2026-40541** Synology Synology Chat Server

Product not on watchlist.

**10.0** **CVE-2026-82222** DETECTION

Deserialization of Untrusted Data vulnerability in Liquid Web / StellarWP GiveWP allows Object Injection. This issue affects GiveWP: from n/a through 4.16.7.1.

**10.0** **CVE-2026-54745**

Kubeflow Pipelines enables users to build and deploy portable, scalable machine learning workflows. Prior to 2.17.0, the Kubeflow Pipelines frontend exposes an unauthenticated server-side request forgery vulnerability through the /_proxy/ route in frontend/ser

**9.9** **CVE-2026-55565**

Yamcs is a mission control framework. Prior to 5.12.8 and 5.13.2, Yamcs LikeExpression.fillCode_getValueReturn in yamcs-core/src/main/java/org/yamcs/yarch/streamsql/LikeExpression.java inserts an unescaped LIKE pattern into Java source compiled by Expression.g

9.9 **CVE-2026-55634**

Pimcore is an Open Source Data & Experience Management Platform. Prior to 11.5.19, 12.3.10, and 2026.1.6, the class-definition import endpoint /pimcore-studio/api/class/definition/configuration-view/detail/{id}/import accepts a DataObject field name that is em

9.9 **CVE-2026-18527**

IBM Administration Runtime Expert for i 1R1M0 IBM Application Runtime Expert (ARE) for i could allow a remote attacker to gain elevated privileges, caused by ARE GUI component processing. An unauthenticated attacker can exploit this vulnerability to execute ac

9.9 **CVE-2026-19295** Langflow langflow

IBM Langflow OSS 1.0.0 through 1.11.1 allows an authenticated attacker to execute arbitrary operating system commands in the server process by saving a flow with a crafted type field value and triggering a build of a wrapper flow that references it. This allow

9.8 **CVE-2026-69658**

MQTT credentials and control traffic are transmitted in cleartext, exposing sensitive information to network-level attackers. This may enable unauthorized device impersonation and disruption of messaging functions.

9.8 **CVE-2026-71187**

The Ebyte device relies on client side authentication logic that can be reproduced by unauthenticated users. An attacker may generate valid authentication requests and bypass authentication to obtain administrative access to the device.

9.8 **CVE-2026-73125**

Ebyte device web management interface does not consistently enforce authentication before granting access to administrative functionality. An unauthenticated remote attacker could access sensitive configuration information, modify device settings, or disrupt a

9.8 **CVE-2026-75337**

The static resource interface /api/static/{deployKey}/ of Yu AI Code Mother v4.3 is vulnerable to path traversal. The user-controlled path is concatenated to the preview root directory without any normalization, allowing anonymous attackers to read files outsi

9.8 **CVE-2026-76179**

An improper protection of authentication tokens vulnerability exists in certain Ebyte gateway products. Authentication tokens used by the web management interface are insufficiently protected during client-side session handling, which may allow an attacker wit

9.8 **CVE-2026-76943**

Xiiaozet LK100Wt contains an authentication weakness within an administrative service that may allow an attacker to bypass intended access controls and obtain command execution capabilities. Successful exploitation could allow unauthorized interaction with pri

9.8 **CVE-2026-78239**

Xiiaozet LK100W exposes a critical management function that can be invoked without authentication, allowing a remote attacker to enable administrative services that should be restricted. Successful exploitation may permit unauthorized access to the device.

**9.8** **CVE-2026-82082**

NUMail developed by Green-Computing has an OS Command Injection vulnerability. Unauthenticated remote attackers can inject arbitrary OS commands and execute them on the server.

**9.8** **CVE-2026-76581**

The WPMU DEV Dashboard plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 5.0.1. This is due to inconsistent and ambiguous HMAC message construction between the unauthenticated `wdpsso_step1` and `wdpsso_step2` AJ

**9.8** **CVE-2026-78032**

SOY CMS contains an issue with deserialization of untrusted data. An arbitrary code may be executed by an attacker with the web server privilege.

**9.8** **CVE-2026-80600**

In the Linux kernel, the following vulnerability has been resolved: batman-adv: dat: acquire ARP hw source only after skb realloc The pskb_may_pull() called by batadv_get_vid() could reallocate the buffer behind the skb. Variables which were pointing to the ol

**9.8** **CVE-2026-80609**

In the Linux kernel, the following vulnerability has been resolved: qede: fix out-of-bounds check for cqe->len_list[] Move index check before element access.

**9.8** **CVE-2026-80612**

In the Linux kernel, the following vulnerability has been resolved: net: lwtunnel: Drop skb metadata before LWT encapsulation skb metadata is meant for passing information between XDP and TC. It lives in the skb headroom, immediately before skb->data. LWT prog

*54 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.