Daily brief, Sunday, August 16, 2026

Aug 15, 8:00 PM to Aug 16, 8:00 PM ET

Generated Nov 2, 2026, 11:04 AM ET

0	0	0	16	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

16 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

16

9.9 **CVE-2026-19959**

A weakness has been identified in Edimax EW-7478APC 1.04. This affects the function formWanTcpipSetup of the file /goform/formWanTcpipSetup. This manipulation of the argument pppUserName causes stack-based buffer overflow. Remote exploitation of the attack is

9.9 **CVE-2026-19961**

A vulnerability was detected in Edimax EW-7478APC 1.04. Affected is the function formWlSiteSurvey of the file /goform/formWlSiteSurvey. Performing a manipulation of the argument selSSID results in buffer overflow. The attack is possible to be carried out remot

9.8 **CVE-2026-19924**

A security vulnerability has been detected in Tenda AC10 16.03.10.09_multi_TDE01. This vulnerability affects the function R7WebsSecurityHandler of the component httpd. The manipulation leads to improper authentication. The attack may be initiated remotely. The

9.8 **CVE-2026-16098**

The ProSolution WP Client plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 2.0.10 via the proSol_handleFileUpload function. This is due to missing validation of the attacker-controlled Content-Disposition header

9.8 **CVE-2026-18432**

The Frontend Admin by DynamiApps plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 3.29.9. The vulnerability exists because `ActionUser::conditions_logic()` gates the `current_user_can('edit_user', $user_id)` auth

9.8 **CVE-2024-13784**

The Contact Form, Survey, Quiz & Popup Form Builder – ARForms plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.8.5 via deserialization of untrusted input from form submissions. This makes it possible for unauth

9.8 **CVE-2026-19349**

Lemonldap::NG::Portal versions from 2.0.0 before 2.16.9, from 2.17.0 before 2.21.5, from 2.22.0 before 2.23.3 for Perl allow authentication bypass via an OAuth2 state parameter stored as an SSO session in the GitHub and LinkedIn backends. Before redirecting to

9.8 **CVE-2026-72887**

Net::OAuth::Client versions before 0.32 for Perl allow the service provider to silently downgrade OAuth 1.0a to OAuth 1.0 in get_request_token. Passing a callback to the constructor selects OAuth 1.0a. get_request_token then revokes that choice when the reques

9.8 **CVE-2026-73056**

SiYuan kernel versions before 3.7.4 contain an improper restriction of excessive authentication attempts vulnerability in the CheckAuth() middleware. The middleware accepts the API token (Conf.Api.Token) via an Authorization header (Token/Bearer) or a ?token=

9.8 **CVE-2026-73061**

Scriban before 7.2.2 contains an access-modifier bypass vulnerability in TypedObjectAccessor that allows template code to write CLR object properties without setter-visibility checks. Attackers can modify properties with private, internal, or init-only setters

9.3 **CVE-2026-74251**

Joomla Extension - phoca.cz - Unauthenticated SQL injection via attribute filter in Phoca Cart 5.0.0-6.1.6 - The a[] (attribute) and s[] (specification) GET array parameters on Phoca Cart's public shop items page are concatenated raw into SQL WHERE clauses wit

9.1 **CVE-2026-14524**

The ProSolution WP Client plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the proSol_fileDeleteProcess function in all versions up to, and including, 2.0.8. This makes it possible for unauthenticated at

9.1 **CVE-2026-18316**

The Solace Extra plugin for WordPress is vulnerable to unauthorized modification and loss of data due to a missing capability check on the import_zip() function in versions up to, and including, 1.6.0. The handler is registered on both wp_ajax_action-import-zi

9.1 **CVE-2026-19714**

The Simple JWT Login WordPress plugin before 3.6.8 does not validate the audience of the Google identity tokens it accepts, allowing unauthenticated users to authenticate as any user whose email address such a token carries, up to and including an administrato

9.1 **CVE-2026-19725**

The WPvivid — Backup, Migration & Staging WordPress plugin before 0.9.131 does not sanitise a value taken from an unauthenticated request before using it to build a log file path, allowing an attacker holding a site to site transfer key to create a log file in

9.1 **CVE-2026-74790**

Scriban before 7.0.0 caches TypedObjectAccessor by Type only without considering MemberFilter changes, allowing reused TemplateContext instances to expose members that should be hidden. Attackers can access filtered properties and fields by reusing a TemplateC

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.