CVEs más relevantes de la semana

Del 28/10/2025 al 04/11/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-64095

Descripción: DNN (formerly DotNetNuke) is an open-source web content management platform (CMS) in the Microsoft ecosystem. Prior to 10.1.1, the default HTML editor provider allows unauthenticated file uploads and images can overwrite existing files. An unauthenticated user can upload and replace existing files allowing defacing a website and combined with other issue, injection XSS payloads. This vulnerabil...

CVSS: 10.0 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Tipo: CWE-434

Tecnología: No especificado

Publicado el: 2025-10-28

CVE-2025-64102

Descripción: Zitadel is open-source identity infrastructure software. Prior to 4.6.0, 3.4.3, and 2.71.18, an attacker can perform an online brute-force attack on OTP, TOTP, and passwords. While Zitadel allows preventing online brute force attacks in scenarios like TOTP, Email OTP, or passwords using a lockout mechanism. The mechanism is not enabled by default and can cause a denial of service for the corres...

CVSS: 9.8 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-307

Tecnología: No especificado

Publicado el: 2025-10-29

CVE-2025-64103

Descripción: Starting from 2.53.6, 2.54.3, and 2.55.0, Zitadel only required multi factor authentication in case the login policy has either enabled requireMFA or requireMFAForLocalUsers. If a user has set up MFA without this requirement, Zitadel would consider single factor auhtenticated sessions as valid as well and not require multiple factors. Bypassing second authentication factors weakens multifactor ...

CVSS: 9.8 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-287

Tecnología: No especificado

Publicado el: 2025-10-29

CVE-2025-5397

Descripción: The Noo JobMonster theme for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 4.8.1. This is due to the check_login() function not properly verifying a user's identity prior to successfully authenticating them This makes it possible for unauthenticated attackers to bypass standard authentication and access administrative user accounts. Please note social l...

CVSS: 9.8 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-288

Tecnología: No especificado

Publicado el: 2025-10-31

CVE-2025-8489

Descripción: The King Addons for Elementor – Free Elements, Widgets, Templates, and Features for Elementor plugin for WordPress is vulnerable to privilege escalation in versions 24.12.92 to 51.1.14 . This is due to the plugin not properly restricting the roles that users can register with. This makes it possible for unauthenticated attackers to register with administrator-level user accounts.

CVSS: 9.8 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-269

Tecnología: No especificado

Publicado el: 2025-10-31

CVE-2025-6520

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Abis Technology BAPSIS allows Blind SQL Injection.This issue affects BAPSIS: before 202510271606.

CVSS: 9.8 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-89

Tecnología: No especificado

Publicado el: 2025-10-31

CVE-2025-11833

Descripción: The Post SMTP – Complete SMTP Solution with Logs, Alerts, Backup SMTP & Mobile App plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the __construct function in all versions up to, and including, 3.6.0. This makes it possible for unauthenticated attackers to read arbitrary logged emails sent through the Post SMTP plugin, including password re...

CVSS: 9.8 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-862

Tecnología: No especificado

Publicado el: 2025-11-01

CVE-2025-11499

Descripción: The Tablesome Table – Contact Form DB – WPForms, CF7, Gravity, Forminator, Fluent plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the set_featured_image_from_external_url() function in all versions up to, and including, 1.1.32. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which ma...

CVSS: 9.8 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-434

Tecnología: No especificado

Publicado el: 2025-11-01

CVE-2025-0987

Descripción: Authorization Bypass Through User-Controlled Key vulnerability in CB Project Ltd. Co. CVLand allows Parameter Injection.This issue affects CVLand: from 2.1.0 through 20251103.

CVSS: 9.9 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:L

Tipo: CWE-639

Tecnología: No especificado

Publicado el: 2025-11-03

CVE-2025-8900

Descripción: The Doccure Core plugin for WordPress is vulnerable to privilege escalation in versions up to, and excluding, 1.5.4. This is due to the plugin allowing users who are registering new accounts to set their own role or by supplying 'user_type' field. This makes it possible for unauthenticated attackers to gain elevated privileges by creating an account with the administrator role.

CVSS: 9.8 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-269

Tecnología: No especificado

Publicado el: 2025-11-03

CVE-2025-11007

Descripción: The CE21 Suite plugin for WordPress is vulnerable to unauthorized plugin settings update due to a missing capability check on the wp_ajax_nopriv_ce21_single_sign_on_save_api_settings AJAX action in versions 2.2.1 to 2.3.1. This makes it possible for unauthenticated attackers to update the plugin's API settings including a secret key used for authentication. This allows unauthenticated attackers...

CVSS: 9.8 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-306

Tecnología: No especificado

Publicado el: 2025-11-04

CVE-2025-11008

Descripción: The CE21 Suite plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.3.1 via the log file. This makes it possible for unauthenticated attackers to extract sensitive data including authentication credentials, which can be used to log in as other users as long as they have used the plugin's custom authentication feature before. This may inclu...

CVSS: 9.8 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-532

Tecnología: No especificado

Publicado el: 2025-11-04

CVE-2025-12158

Descripción: The Simple User Capabilities plugin for WordPress is vulnerable to Privilege Escalation due to a missing capability check on the suc_submit_capabilities() function in all versions up to, and including, 1.0. This makes it possible for unauthenticated attackers to elevate the role of any user account to administrator.

CVSS: 9.8 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-862

Tecnología: No especificado

Publicado el: 2025-11-04

CVE-2025-12493

Descripción: The ShopLentor – WooCommerce Builder for Elementor & Gutenberg +21 Modules – All in One Solution (formerly WooLentor) plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 3.2.5 via the 'load_template' function. This makes it possible for unauthenticated attackers to include and execute arbitrary .php files on the server, allowing the execution of any ...

CVSS: 9.8 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-22

Tecnología: No especificado

Publicado el: 2025-11-04

CVE-2025-12682

Descripción: The Easy Upload Files During Checkout plugin for WordPress is vulnerable to arbitrary JavaScript file uploads due to missing file type validation in the 'file_during_checkout' function in all versions up to, and including, 2.9.8. This makes it possible for unauthenticated attackers to upload arbitrary JavaScript files on the affected site's server which may make remote code execution possible.

CVSS: 9.8 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-434

Tecnología: No especificado

Publicado el: 2025-11-04

Resumen del Reporte

CVEs analizados: 15

Promedio CVSS: 9.82

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat