CVEs más relevantes de la semana

Del 02/12/2025 al 09/12/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-13542

Descripción: The DesignThemes LMS plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.0.4. This is due to the 'dtlms_register_user_front_end' function not restricting what user roles a user can register with. This makes it possible for unauthenticated attackers to supply the 'administrator' role during registration and gain administrator access to the site.

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: 2025-12-02

CVE-2025-13486

Descripción: The Advanced Custom Fields: Extended plugin for WordPress is vulnerable to Remote Code Execution in versions 0.9.0.5 through 0.9.1.1 via the prepare_form() function. This is due to the function accepting user input and then passing that through call_user_func_array(). This makes it possible for unauthenticated attackers to execute arbitrary code on the server, which can be leveraged to inject b...

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-94

Tecnología: No especificado

Publicado el: 2025-12-03

CVE-2025-13342

Descripción: The Frontend Admin by DynamiApps plugin for WordPress is vulnerable to unauthorized modification of arbitrary WordPress options in all versions up to, and including, 3.28.20. This is due to insufficient capability checks and input validation in the ActionOptions::run() save handler. This makes it possible for unauthenticated attackers to modify critical WordPress options such as users_can_regis...

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: 2025-12-03

CVE-2025-66032

Descripción: Claude Code is an agentic coding tool. Prior to 1.0.93, Due to errors in parsing shell commands related to $IFS and short CLI flags, it was possible to bypass the Claude Code read-only validation and trigger arbitrary code execution. Reliably exploiting this requires the ability to add untrusted content into a Claude Code context window. This vulnerability is fixed in 1.0.93.

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-77

Tecnología: No especificado

Publicado el: 2025-12-03

CVE-2025-66208

Descripción: Collabora Online - Built-in CODE Server (richdocumentscode) provides a built-in server with all of the document editing features of Collabora Online. In versions prior to 25.04.702, Collabora Online has a Configuration-Dependent RCE (OS Command Injection) in richdocumentscode proxy. Users of Nextcloud with Collabora Online - Built-in CODE Server app can be vulnerable to attack via proxy.php and...

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-78

Tecnología: No especificado

Publicado el: 2025-12-03

CVE-2025-66222

Descripción: DeepChat is a smart assistant uses artificial intelligence. In 0.5.0 and earlier, there is a Stored Cross-Site Scripting (XSS) vulnerability in the Mermaid diagram renderer allows an attacker to execute arbitrary JavaScript within the application context. By leveraging the exposed Electron IPC bridge, this XSS can be escalated to Remote Code Execution (RCE) by registering and starting a malicio...

CVSS: 9.6 (CRITICAL)

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

Tipo: CWE-94

Tecnología: No especificado

Publicado el: 2025-12-03

CVE-2025-14004

Descripción: A security flaw has been discovered in dayrui XunRuiCMS up to 4.7.1. Affected is an unknown function of the file /admind45f74adbd95.php?c=email&m=add of the component Email Setting Handler. Performing manipulation results in server-side request forgery. Remote exploitation of the attack is possible. The exploit has been released to the public and may be exploited. The vendor was contacted early...

CVSS: 4.7 (MEDIUM)

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

Tipo: CWE-918

Tecnología: No especificado

Publicado el: 2025-12-04

CVE-2024-45538

Descripción: Cross-Site Request Forgery (CSRF) vulnerability in WebAPI Framework in Synology DiskStation Manager (DSM) before 7.2.1-69057-2 and 7.2.2-72806 and Synology Unified Controller (DSMUC) before 3.1.4-23079 allows remote attackers to execute arbitrary code via unspecified vectors.

CVSS: 9.6 (CRITICAL)

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

Tipo: CWE-352

Tecnología: No especificado

Publicado el: 2025-12-04

CVE-2025-13313

Descripción: The CRM Memberships plugin for WordPress is vulnerable to privilege escalation via password reset in all versions up to, and including, 2.5. This is due to missing authorization and authentication checks on the `ntzcrm_changepassword` AJAX action. This makes it possible for unauthenticated attackers to reset arbitrary user passwords and gain unauthorized access to user accounts via the `ntzcrm_...

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: 2025-12-05

CVE-2025-12374

Descripción: The Email Verification, Email OTP, Block Spam Email, Passwordless login, Hide Login, Magic Login – User Verification plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 2.0.39. This is due to the plugin not properly validating that an OTP was generated before comparing it to user input in the "user_verification_form_wrap_process_otpLogin" function. ...

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: 2025-12-05

CVE-2025-12673

Descripción: The Flex QR Code Generator plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the update_qr_code() function in all versions up to, and including, 1.2.6. This makes it possible for unauthenticated attackers to upload arbitrary 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: 2025-12-06

CVE-2025-13377

Descripción: The 10Web Booster – Website speed optimization, Cache & Page Speed optimizer plugin for WordPress is vulnerable to arbitrary folder deletion due to insufficient file path validation in the get_cache_dir_for_page_from_url() function in all versions up to, and including, 2.32.7. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary folders...

CVSS: 9.6 (CRITICAL)

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

Tipo: CWE-22

Tecnología: No especificado

Publicado el: 2025-12-06

CVE-2025-61318

Descripción: Emlog Pro 2.5.20 has an arbitrary file deletion vulnerability. This vulnerability stems from the admin/template.php component and the admin/plugin.php component. They fail to perform path verification and dangerous code filtering for deletion parameters, allowing attackers to exploit this feature for directory traversal.

CVSS: 9.1 (CRITICAL)

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

Tipo: NVD-CWE-Other

Tecnología: No especificado

Publicado el: 2025-12-08

CVE-2025-14256

Descripción: A vulnerability was detected in itsourcecode Student Management System 1.0. This impacts an unknown function of the file /newcurriculm.php. Performing manipulation of the argument ID results in sql injection. The attack can be initiated remotely.
The exploit is now public and may be used.

CVSS: 7.3 (HIGH)

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

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-12-08

CVE-2025-14257

Descripción: A flaw has been found in itsourcecode Student Management System 1.0. Affected is an unknown function of the file /newrecord.php. Executing manipulation of the argument ID can lead to sql injection. The attack can be launched remotely. The exploit has been published and may be used.

CVSS: 7.3 (HIGH)

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

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-12-08

CVE-2025-48626

Descripción: In multiple locations, there is a possible way to launch an application from the background due to a precondition check failure. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.

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: NVD-CWE-noinfo

Tecnología: No especificado

Publicado el: 2025-12-08

CVE-2025-14258

Descripción: A vulnerability has been found in itsourcecode Student Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /newsubject.php. The manipulation of the argument sub leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.

CVSS: 7.3 (HIGH)

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

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-12-08

CVE-2025-64081

Descripción: SQL injection vulnerability in /php/api_patient_schedule.php in SourceCodester Patients Waiting Area Queue Management System v1 allows attackers to execute arbitrary SQL commands via the appointmentID parameter.

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: 2025-12-08

CVE-2025-11022

Descripción: Cross-Site Request Forgery (CSRF) vulnerability in Personal Project Panilux allows Cross Site Request Forgery.

This

CSRF vulnerability resulting in Command Injection has been identified.

This issue affects Panilux: before v.0.10.0. NOTE: The vendor was contacted and responded that they deny ownership of the mentioned product.

CVSS: 9.6 (CRITICAL)

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

Tipo: CWE-352

Tecnología: No especificado

Publicado el: 2025-12-09

CVE-2025-12504

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in TalentSoft Software UNIS allows SQL Injection.This issue affects UNIS: before 42321.

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: 2025-12-09

CVE-2025-42880

Descripción: Due to missing input sanitation, SAP Solution Manager allows an authenticated attacker to insert malicious code when calling a remote-enabled function module. This could provide the attacker with full control of the system hence leading to high impact on confidentiality, integrity and availability of the system.

CVSS: 9.9 (CRITICAL)

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

Tipo: CWE-94

Tecnología: No especificado

Publicado el: 2025-12-09

CVE-2025-42928

Descripción: Under certain conditions, a high privileged user could exploit a deserialization vulnerability in SAP jConnect to launch remote code execution. The system may be vulnerable when specially crafted input is used to exploit the vulnerability resulting in high impact on confidentiality, integrity and availability of the system.

CVSS: 9.1 (CRITICAL)

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

Tipo: CWE-502

Tecnología: No especificado

Publicado el: 2025-12-09

Resumen del Reporte

CVEs analizados: 22

Promedio CVSS: 9.13

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat