CVEs más relevantes de la semana

Del 09/12/2025 al 16/12/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-64672

Descripción: Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.

CVSS: 8.8 (HIGH)

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

Tipo: CWE-79

Tecnología: No especificado

Publicado el: 2025-12-09

CVE-2025-14335

Descripción: A vulnerability has been found in itsourcecode Student Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /new_school_year.php. The manipulation of the argument sy leads to sql injection. It is possible to initiate the attack 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: 2025-12-09

CVE-2025-14336

Descripción: A vulnerability was found in itsourcecode Student Management System 1.0. Affected by this issue is some unknown functionality of the file /promote.php. The manipulation of the argument sy results in sql injection. It is possible to launch the attack remotely. The exploit has been made public and could 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: 2025-12-09

CVE-2025-61808

Descripción: ColdFusion versions 2025.4, 2023.16, 2021.22 and earlier are affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could lead to arbitrary code execution by a high priviledged attacker. Exploitation of this issue does not require user interaction and scope is changed.

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-434

Tecnología: No especificado

Publicado el: 2025-12-10

CVE-2025-61809

Descripción: ColdFusion versions 2025.4, 2023.16, 2021.22 and earlier are affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized read and write access. Exploitation of this issue does not require user interaction and scope is unchanged.

CVSS: 9.1 (CRITICAL)

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

Tipo: CWE-20

Tecnología: No especificado

Publicado el: 2025-12-10

CVE-2025-61811

Descripción: ColdFusion versions 2025.4, 2023.16, 2021.22 and earlier are affected by an Improper Access Control vulnerability that could result in arbitrary code execution in the context of the current user. A high privileged attacker could leverage this vulnerability to bypass security measures and execute malicious code. Exploitation of this issue does not require user interaction and scope is changed.

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-22

Tecnología: No especificado

Publicado el: 2025-12-10

CVE-2025-13613

Descripción: The Elated Membership plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 1.2. This is due to the plugin not properly logging in a user with the data that was previously verified through the 'eltdf_membership_check_facebook_user' and the 'eltdf_membership_login_user_from_social_network' function. This makes it possible for 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-289

Tecnología: No especificado

Publicado el: 2025-12-10

CVE-2025-41730

Descripción: An unauthenticated remote attacker can abuse unsafe sscanf calls within the check_account() function to write arbitrary data into fixed-size stack buffers which leads to full device compromise.

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-121

Tecnología: No especificado

Publicado el: 2025-12-10

CVE-2025-41732

Descripción: An unauthenticated remote attacker can abuse unsafe sscanf calls within the check_cookie() function to write arbitrary data into fixed-size stack buffers which leads to full device compromise.

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-121

Tecnología: No especificado

Publicado el: 2025-12-10

CVE-2025-64537

Descripción: Adobe Experience Manager versions 6.5.23 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could lead to arbitrary code execution. An attacker could exploit this vulnerability by injecting malicious scripts into a web page that are executed in the context of the victim's browser. A successful attacker can abuse this to achieve session takeover, increasing the...

CVSS: 9.3 (CRITICAL)

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

Tipo: CWE-79

Tecnología: No especificado

Publicado el: 2025-12-10

CVE-2025-64538

Descripción: Adobe Experience Manager versions 6.5.23 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could lead to arbitrary code execution. An attacker could exploit this vulnerability by injecting malicious scripts into a web page that are executed in the context of the victim's browser. A successful attacker can abuse this to achieve session takeover, increasing the...

CVSS: 9.3 (CRITICAL)

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

Tipo: CWE-79

Tecnología: No especificado

Publicado el: 2025-12-10

CVE-2025-64539

Descripción: Adobe Experience Manager versions 6.5.23 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could lead to arbitrary code execution. An attacker could exploit this vulnerability by injecting malicious scripts into a web page that are executed in the context of the victim's browser. A successful attacker can abuse this to achieve session takeover, increasing the...

CVSS: 9.3 (CRITICAL)

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

Tipo: CWE-79

Tecnología: No especificado

Publicado el: 2025-12-10

CVE-2025-13764

Descripción: The WP CarDealer plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.2.16. This is due to the 'WP_CarDealer_User::process_register' 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: 2025-12-11

CVE-2025-14527

Descripción: A weakness has been identified in projectworlds Advanced Library Management System 1.0. This vulnerability affects unknown code of the file /view_book.php. Executing manipulation of the argument book_id can lead to sql injection. The attack can be executed remotely. The exploit has been made available to the public and could be exploited.

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: 2025-12-11

CVE-2025-14534

Descripción: A vulnerability was determined in UTT □□ 512W up to 3.1.7.7-171114. This impacts the function strcpy of the file /goform/formNatStaticMap of the component Endpoint. Executing manipulation of the argument NatBind can lead to buffer overflow. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but d...

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-119

Tecnología: No especificado

Publicado el: 2025-12-11

CVE-2025-14535

Descripción: A vulnerability was identified in UTT □□ 512W up to 3.1.7.7-171114. Affected is the function strcpy of the file /goform/formConfigFastDirectionW. The manipulation of the argument ssid leads to buffer overflow. The attack may be initiated remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.

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-119

Tecnología: No especificado

Publicado el: 2025-12-11

CVE-2025-36937

Descripción: In AudioDecoder::HandleProduceRequest of audio_decoder.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution 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: CWE-787

Tecnología: No especificado

Publicado el: 2025-12-11

CVE-2025-66419

Descripción: MaxKB is an open-source AI assistant for enterprise. In versions 2.3.1 and below, the tool module allows an attacker to escape the sandbox environment and escalate privileges under certain concurrent conditions. This issue is fixed in version 2.4.0.

CVSS: 8.8 (HIGH)

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

Tipo: CWE-362

Tecnología: No especificado

Publicado el: 2025-12-11

CVE-2025-12963

Descripción: The LazyTasks – Project & Task Management with Collaboration, Kanban and Gantt Chart plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 1.2.29. This is due to the plugin not properly validating a user's identity via the 'wp-json/lazytasks/api/v1/user/role/edit/' REST API endpoint prior to updating their details like email addres...

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: 2025-12-12

CVE-2025-14344

Descripción: The Multi Uploader for Gravity Forms plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the 'plupload_ajax_delete_file' function in all versions up to, and including, 1.1.7. This makes it possible for unauthenticated attackers to delete arbitrary files on the server.

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: 2025-12-12

CVE-2025-54947

Descripción: In Apache StreamPark versions 2.0.0 through 2.1.7, a security vulnerability involving a hard-coded encryption key exists. This vulnerability occurs because the system uses a fixed, immutable key for encryption instead of dynamically generating or securely configuring the key. Attackers may obtain this key through reverse engineering or code analysis, potentially decrypting sensitive data or for...

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-321

Tecnología: No especificado

Publicado el: 2025-12-12

CVE-2025-14611

Descripción: Gladinet CentreStack and Triofox prior to version 16.12.10420.56791 used hardcoded values for their implementation of the AES cryptoscheme. This degrades security for public exposed endpoints that may make use of it and may offer arbitrary local file inclusion when provided a specially crafted request without authentication. This opens the door for future exploitation and can be leveraged with ...

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-798

Tecnología: No especificado

Publicado el: 2025-12-12

CVE-2025-10738

Descripción: The URL Shortener Plugin For WordPress plugin for WordPress is vulnerable to SQL Injection via the 'analytic_id' parameter in all versions up to, and including, 3.0.7 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing...

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: 2025-12-13

CVE-2025-11693

Descripción: The Export WP Page to Static HTML & PDF plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.3.4 through publicly exposed cookies.txt files containing authentication cookies. This makes it possible for unauthenticated attackers to cookies that may have been injected into the log file if the site administrator triggered a back-up using a sp...

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-200

Tecnología: No especificado

Publicado el: 2025-12-13

CVE-2025-14440

Descripción: The JAY Login & Register plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 2.4.01. This is due to incorrect authentication checking in the 'jay_login_register_process_switch_back' function with the 'jay_login_register_process_switch_back' cookie value. This makes it possible for unauthenticated attackers to log in as any existing user on the site, suc...

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-565

Tecnología: No especificado

Publicado el: 2025-12-13

CVE-2025-14620

Descripción: A vulnerability was determined in code-projects Student File Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/login_query.php. Executing manipulation of the argument Username can lead to sql injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.

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: 2025-12-13

CVE-2025-14621

Descripción: A vulnerability was identified in code-projects Student File Management System 1.0. This affects an unknown part of the file /admin/update_user.php. The manipulation of the argument user_id leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might 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: 2025-12-13

CVE-2025-14622

Descripción: A security flaw has been discovered in code-projects Student File Management System 1.0. This vulnerability affects unknown code of the file /admin/save_user.php. The manipulation of the argument firstname results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be exploited.

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: 2025-12-13

CVE-2025-14665

Descripción: A security flaw has been discovered in Tenda WH450 1.0.0.18. Impacted is an unknown function of the file /goform/DhcpListClient of the component HTTP Request Handler. The manipulation of the argument page results in stack-based buffer overflow. The attack can be executed remotely. The exploit has been released to the public and may be exploited.

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-119

Tecnología: No especificado

Publicado el: 2025-12-14

CVE-2025-14705

Descripción: A vulnerability was determined in Shiguangwu sgwbox N3 2.0.25. This affects an unknown function of the component SHARESERVER Feature. This manipulation of the argument params causes command injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.

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-74

Tecnología: No especificado

Publicado el: 2025-12-15

CVE-2025-14706

Descripción: A vulnerability was identified in Shiguangwu sgwbox N3 2.0.25. This impacts an unknown function of the file /usr/sbin/http_eshell_server of the component NETREBOOT Interface. Such manipulation leads to command injection. The attack can be launched remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.

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-74

Tecnología: No especificado

Publicado el: 2025-12-15

CVE-2025-14707

Descripción: A security flaw has been discovered in Shiguangwu sgwbox N3 2.0.25. Affected is an unknown function of the file /usr/sbin/http_eshell_server of the component DOCKER Feature. Performing manipulation of the argument params results in command injection. The attack may be initiated remotely. The exploit has been released to the public and may be exploited. The vendor was contacted early about this ...

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-74

Tecnología: No especificado

Publicado el: 2025-12-15

CVE-2025-14708

Descripción: A weakness has been identified in Shiguangwu sgwbox N3 2.0.25. Affected by this vulnerability is an unknown functionality of the file /usr/sbin/http_eshell_server of the component WIREDCFGGET Interface. Executing manipulation of the argument params can lead to buffer overflow. The attack may be launched remotely. The exploit has been made available to the public and could be exploited. The vend...

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-119

Tecnología: No especificado

Publicado el: 2025-12-15

CVE-2025-14709

Descripción: A security vulnerability has been detected in Shiguangwu sgwbox N3 2.0.25. Affected by this issue is some unknown functionality of the file /usr/sbin/http_eshell_server of the component WIRELESSCFGGET Interface. The manipulation of the argument params leads to buffer overflow. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. The vendor was ...

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-119

Tecnología: No especificado

Publicado el: 2025-12-15

CVE-2025-14156

Descripción: The Fox LMS – WordPress LMS Plugin plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 1.0.5.1. This is due to the plugin not properly validating the 'role' parameter when creating new users via the `/fox-lms/v1/payments/create-order` REST API endpoint. This makes it possible for unauthenticated attackers to create new user accounts with arbitrary ro...

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-20

Tecnología: No especificado

Publicado el: 2025-12-15

Resumen del Reporte

CVEs analizados: 35

Promedio CVSS: 9.21

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat ▯