CVEs más relevantes de la semana

Del 06/12/2025 al 13/12/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-14141

Descripción: A flaw has been found in UTT □□ 520W 1.7.7-180627. The impacted element is the function strcpy of the file /goform/formArpBindConfig. Executing manipulation of the argument pools can lead to buffer overflow. The attack may be performed from remote. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.

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-119

Tecnología: No especificado

Publicado el: 2025-12-06

CVE-2025-14182

Descripción: A vulnerability has been found in Sobey Media Convergence System 2.0/2.1. This vulnerability affects unknown code of the file /sobey-mchEditor/watermark/upload. The manipulation of the argument File leads to path traversal. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.

CVSS: 6.3 (MEDIUM)

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

Tipo: CWE-22

Tecnología: No especificado

Publicado el: 2025-12-07

CVE-2025-14199

Descripción: A flaw has been found in Verysync □□□□ up to 2.21.3. This impacts an unknown function of the file /rest/f/api/resources/f96956469e7be39d/tmp/text.txt?override=false of the component Web Administration Module. Executing manipulation can lead to unrestricted upload. The attack may be performed from remote. The exploit has been published and may be used. The vendor was contacted early about this d...

CVSS: 6.3 (MEDIUM)

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

Tipo: CWE-284

Tecnología: No especificado

Publicado el: 2025-12-07

CVE-2025-14209

Descripción: A weakness has been identified in Campcodes School File Management System 1.0. This impacts an unknown function of the file /update_query.php. This manipulation of the argument stud_id causes sql injection. The attack can be initiated 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: 2025-12-08

CVE-2025-14210

Descripción: A security vulnerability has been detected in projectworlds Advanced Library Management System 1.0. Affected is an unknown function of the file /delete_member.php. Such manipulation of the argument user_id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed publicly 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-2025-14211

Descripción: A vulnerability was detected in projectworlds Advanced Library Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /delete_book.php. Performing manipulation of the argument book_id results in sql injection. The attack may 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-2025-14212

Descripción: A flaw has been found in projectworlds Advanced Library Management System 1.0. Affected by this issue is some unknown functionality of the file /member_search.php. Executing manipulation of the argument roll_number can lead to sql injection. The attack may 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-2025-14215

Descripción: A vulnerability was found in code-projects Currency Exchange System 1.0. This vulnerability affects unknown code of the file /edit.php. The manipulation of the argument ID results in sql injection. The attack can be executed 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: 2025-12-08

CVE-2025-14216

Descripción: A vulnerability was determined in code-projects Currency Exchange System 1.0. This issue affects some unknown processing of the file /viewserial.php. This manipulation of the argument ID causes sql injection. The attack is possible to be carried out 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: 2025-12-08

CVE-2025-14217

Descripción: A vulnerability was identified in code-projects Currency Exchange System 1.0. Impacted is an unknown function of the file /edittrns.php. Such manipulation of the argument ID leads to sql injection. The attack may be performed from remote. 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: 2025-12-08

CVE-2025-14218

Descripción: A security flaw has been discovered in code-projects Currency Exchange System 1.0. The affected element is an unknown function of the file /editotheraccount.php. Performing manipulation of the argument ID results in sql injection. It is possible to initiate the attack 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: 2025-12-08

CVE-2025-14223

Descripción: A vulnerability has been found in code-projects Simple Leave Manager 1.0. Affected by this vulnerability is an unknown functionality of the file /request.php. Such manipulation of the argument staff_id leads to sql injection. The attack may be launched 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-2025-14224

Descripción: A vulnerability was found in Yottamaster DM2, DM3 and DM200 up to 1.2.23/1.9.12. Affected by this issue is some unknown functionality of the component File Upload. Performing manipulation results in path traversal. Remote exploitation of the attack is possible. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.

CVSS: 4.3 (MEDIUM)

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

Tipo: CWE-22

Tecnología: No especificado

Publicado el: 2025-12-08

CVE-2025-14226

Descripción: A vulnerability was identified in itsourcecode Student Management System 1.0. This vulnerability affects unknown code of the file /edit_user.php. The manipulation of the argument fname leads to sql injection. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. Other parameters might be affected as well.

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-2025-14245

Descripción: A vulnerability has been found in IdeaCMS up to 1.8. This affects the function whereRaw of the file app/common/logic/index/Coupon.php. Such manipulation of the argument params leads to sql injection. The attack may be launched 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-2025-14246

Descripción: A vulnerability was found in code-projects Simple Shopping Cart 1.0. This vulnerability affects unknown code of the file /Customers/settings.php. Performing manipulation of the argument user_id results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used.

CVSS: 6.3 (MEDIUM)

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

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-12-08

CVE-2025-14247

Descripción: A vulnerability was determined in code-projects Simple Shopping Cart 1.0. This issue affects some unknown processing of the file /Admin/additems.php. Executing manipulation of the argument item_name can lead to sql injection. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.

CVSS: 6.3 (MEDIUM)

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

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-12-08

CVE-2025-14248

Descripción: A vulnerability was identified in code-projects Simple Shopping Cart 1.0. Impacted is an unknown function of the file /adminlogin.php. The manipulation of the argument admin_username leads to sql injection. The attack is possible to be carried out remotely. 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: 2025-12-08

CVE-2025-14249

Descripción: A security flaw has been discovered in code-projects Online Ordering System 1.0. The affected element is an unknown function of the file /user_school.php. The manipulation of the argument product_id results in sql injection. The attack may be performed from remote. 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: 2025-12-08

CVE-2025-14250

Descripción: A weakness has been identified in code-projects Online Ordering System 1.0. The impacted element is an unknown function of the file /user_contact.php. This manipulation of the argument Name causes sql injection. It is possible to initiate the attack 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: 2025-12-08

CVE-2025-14251

Descripción: A security vulnerability has been detected in code-projects Online Ordering System 1.0. This affects an unknown function of the file /admin/ of the component Admin Login. Such manipulation of the argument Username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed publicly 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-2025-61318

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-2025-14285

Descripción: A vulnerability was found in code-projects Employee Profile Management System 1.0. Affected is an unknown function of the file edit_personnel.php. The manipulation of the argument per_id results in sql injection. The attack can be launched 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-2025-11022

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-2025-14321

Descripción: Use-after-free in the WebRTC: Signaling component. This vulnerability affects Firefox < 146, Firefox ESR < 140.6, Thunderbird < 146, and Thunderbird < 140.6.

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-416

Tecnología: No especificado

Publicado el: 2025-12-09

CVE-2025-14324

Descripción: JIT miscompilation in the JavaScript Engine: JIT component. This vulnerability affects Firefox < 146, Firefox ESR < 115.31, Firefox ESR < 140.6, Thunderbird < 146, and Thunderbird < 140.6.

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: 2025-12-09

CVE-2025-14326

Descripción: Use-after-free in the Audio/Video: GMP component. This vulnerability affects Firefox < 146 and Thunderbird < 146.

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-416

Tecnología: No especificado

Publicado el: 2025-12-09

CVE-2025-14330

Descripción: JIT miscompilation in the JavaScript Engine: JIT component. This vulnerability affects Firefox < 146, Firefox ESR < 140.6, Thunderbird < 146, and Thunderbird < 140.6.

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: 2025-12-09

CVE-2025-40938

Descripción: A vulnerability has been identified in SIMATIC CN 4100 (All versions < V4.0.1). The affected device stores sensitive information in the firmware. This could allow an attacker to access and misuse this information, potentially impacting the device's confidentiality, integrity, and availability.

CVSS: 8.1 (HIGH)

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

Tipo: CWE-798

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

CVE-2025-66565

Descripción: Fiber Utils is a collection of common functions created for Fiber. In versions 2.0.0-rc.3 and below, when the system's cryptographic random number generator (crypto/rand) fails, both functions silently fall back to returning predictable UUID values, including the zero UUID "00000000-0000-0000-0000-000000000000". The vulnerability occurs through two related but distinct failure paths, both ultim...

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-252

Tecnología: No especificado

Publicado el: 2025-12-09

CVE-2025-66567

Descripción: The ruby-saml library is for implementing the client side of a SAML authorization. ruby-saml versions up to and including 1.12.4 contain an authentication bypass vulnerability due to an incomplete fix for CVE-2025-25292. ReXML and Nokogiri parse XML differently, generating entirely different document structures from the same input. This allows an attacker to execute a Signature Wrapping attack....

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-347

Tecnología: No especificado

Publicado el: 2025-12-09

CVE-2025-66568

Descripción: The ruby-saml library implements the client side of an SAML authorization. Versions up to and including 1.12.4, are vulnerable to authentication bypass through the libxml2 canonicalization process used by Nokogiri for document transformation, which allows an attacker to execute a Signature Wrapping attack. When libxml2's canonicalization is invoked on an invalid XML input, it may return an empt...

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-347

Tecnología: No especificado

Publicado el: 2025-12-09

CVE-2025-67504

Descripción: WBCE CMS is a content management system. Versions 1.6.4 and below use function GenerateRandomPassword() to create passwords using PHP's rand(). rand() is not cryptographically secure, which allows password sequences to be predicted or brute-forced. This can lead to user account compromise or privilege escalation if these passwords are used for new accounts or password resets. The vulnerability ...

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-331

Tecnología: No especificado

Publicado el: 2025-12-09

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-2025-61808

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: 8.4 (HIGH)

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

Tipo: CWE-284

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-2025-14534

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-2025-12963

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

Resumen del Reporte

CVEs analizados: 56

Promedio CVSS: 8.40

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat ▯