CVEs más relevantes de la semana

Del 13/12/2025 al 20/12/2025

Porque el primer paso para defender es conocer las amenazas.

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-2025-14586

Descripción: A vulnerability was determined in TOTOLINK X5000R 9.1.0cu.2089_B20211224. Affected by this issue is the function snprintf of the file /cgi-bin/cstecgi.cgi?action=exportOvpn&type=user. This manipulation of the argument User causes os command injection. Remote exploitation of the attack is possible. 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-77

Tecnología: No especificado

Publicado el: 2025-12-13

CVE-2025-14587

Descripción: A vulnerability was identified in itsourcecode Online Pet Shop Management System 1.0. This affects an unknown part of the file /pet1/available.php. Such manipulation of the argument Name leads to sql injection. The attack can be executed 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: 2025-12-13

CVE-2025-14588

Descripción: A security flaw has been discovered in itsourcecode Student Management System 1.0. This vulnerability affects unknown code of the file /update_program.php. Performing manipulation of the argument ID results in sql injection. The attack is possible to be carried out 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-2025-14590

Descripción: A security vulnerability has been detected in code-projects Prison Management System 2.0. Impacted is an unknown function of the file /admin/search1.php. The manipulation of the argument keyname leads to sql injection. It is possible to initiate 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: 2025-12-13

CVE-2025-14619

Descripción: A vulnerability was found in code-projects Student File Management System 1.0. Affected by this vulnerability is an unknown functionality of the file login_query.php. Performing manipulation of the argument stud_no results in sql injection. The attack may be initiated 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: 2025-12-13

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-2025-14623

Descripción: A weakness has been identified in code-projects Student File Management System 1.0. This issue affects some unknown processing of the file /admin/update_student.php. This manipulation of the argument stud_id causes sql injection. The attack is possible to be carried out 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: 2025-12-13

CVE-2025-14637

Descripción: A weakness has been identified in itsourcecode Online Pet Shop Management System 1.0. This vulnerability affects unknown code of the file /pet1/addcnp.php. This manipulation of the argument cnpname 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: 2025-12-13

CVE-2025-14638

Descripción: A security vulnerability has been detected in itsourcecode Online Pet Shop Management System 1.0. This issue affects some unknown processing of the file /pet1/update_cnp.php. Such manipulation of the argument 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: 2025-12-14

CVE-2025-14639

Descripción: A vulnerability was detected in itsourcecode Student Management System 1.0. Impacted is an unknown function of the file /uprec.php. Performing manipulation of the argument 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: 2025-12-14

CVE-2025-14640

Descripción: A flaw has been found in code-projects Student File Management System 1.0. The affected element is an unknown function of the file /admin/save_student.php. Executing manipulation of the argument stud_no 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: 2025-12-14

CVE-2025-14643

Descripción: A vulnerability was found in code-projects Simple Attendance Record System 2.0. The affected element is an unknown function of the file /check.php. Performing manipulation of the argument student results in sql injection. Remote exploitation of the attack is possible. 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: 2025-12-14

CVE-2025-14644

Descripción: A vulnerability was determined in itsourcecode Student Management System 1.0. The impacted element is an unknown function of the file /update_subject.php. Executing manipulation of the argument ID can lead to sql injection. The attack can be executed 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: 2025-12-14

CVE-2025-14645

Descripción: A vulnerability was identified in code-projects Student File Management System 1.0. This affects an unknown function of the file /admin/delete_user.php. The manipulation of the argument user_id 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: 2025-12-14

CVE-2025-14646

Descripción: A security flaw has been discovered in code-projects Student File Management System 1.0. This impacts an unknown function of the file /admin/delete_student.php. The manipulation of the argument stud_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: 2025-12-14

CVE-2025-14649

Descripción: A vulnerability was detected in itsourcecode Online Cake Ordering System 1.0. Affected by this issue is some unknown functionality of the file /cakeshop/supplier.php. Performing manipulation of the argument supplier 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: 2025-12-14

CVE-2025-14650

Descripción: A flaw has been found in itsourcecode Online Cake Ordering System 1.0. This affects an unknown part of the file /cakeshop/product.php. Executing manipulation of the argument Product 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: 2025-12-14

CVE-2025-14652

Descripción: A vulnerability was found in itsourcecode Online Cake Ordering System 1.0. This issue affects some unknown processing of the file /admindetail.php?action=edit. The manipulation of the argument ID results in sql injection. The attack may 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: 2025-12-14

CVE-2025-14653

Descripción: A vulnerability was determined in itsourcecode Student Management System 1.0. Impacted is an unknown function of the file /addrecord.php. This manipulation of the argument ID causes sql injection. Remote exploitation of the attack is possible. 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: 2025-12-14

CVE-2025-14661

Descripción: A vulnerability has been found in itsourcecode Student Managemen System 1.0. Affected by this issue is some unknown functionality of the file /advisers.php. Such manipulation of the argument sy leads to sql injection. The attack can 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: 2025-12-14

CVE-2025-14664

Descripción: A vulnerability was identified in Campcodes Supplier Management System 1.0. This issue affects some unknown processing of the file /admin/view_unit.php. The manipulation of the argument chkId[] 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: 2025-12-14

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-2025-67906

Descripción: In MISP before 2.5.28, app/View/Elements/Workflows/executionPath.ctp allows XSS in the workflow execution path.

CVSS: 5.4 (MEDIUM)

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

Tipo: CWE-79

Tecnología: No especificado

Publicado el: 2025-12-15

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

CVE-2023-53874

Descripción: GOM Player 2.3.90.5360 contains a buffer overflow vulnerability in the equalizer preset name input field that allows attackers to crash the application. Attackers can overwrite the preset name with 260 'A' characters to trigger a buffer overflow and cause application instability.

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-120

Tecnología: No especificado

Publicado el: 2025-12-15

CVE-2023-53877

Descripción: Bus Reservation System 1.1 contains a SQL injection vulnerability in the pickup_id parameter that allows attackers to manipulate database queries. Attackers can exploit boolean-based, error-based, and time-based blind SQL injection techniques to steal information from the database.

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: 2025-12-15

CVE-2025-64725

Descripción: Weblate is a web based localization tool. In versions prior to 5.15, it was possible to accept an invitation opened by a different user. Version 5.15. contains a patch. As a workaround, avoid leaving one's Weblate sessions with an invitation opened unattended.

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-286

Tecnología: No especificado

Publicado el: 2025-12-15

CVE-2025-59385

Descripción: An authentication bypass by spoofing vulnerability has been reported to affect several QNAP operating system versions. The remote attackers can then exploit the vulnerability to access resources which are not otherwise accessible without proper authentication.

We have already fixed the vulnerability in the following versions: QTS 5.2.7.3297 build 20251024 and later QuTS hero h5.2.7.3297 build ...

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-290

Tecnología: No especificado

Publicado el: 2025-12-16

CVE-2025-62849

Descripción: An SQL injection vulnerability has been reported to affect several QNAP operating system versions. The remote attackers can then exploit the vulnerability to execute unauthorized code or commands.

We have already fixed the vulnerability in the following versions: QTS 5.2.7.3297 build 20251024 and later QuTS hero h5.2.7.3297 build 20251024 and later QuTS hero h5.3.1.3292 build 20251024 and later

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: 2025-12-16

CVE-2025-59374

Descripción: "UNSUPPORTED WHEN ASSIGNED" Certain versions of the ASUS Live Update client were distributed with unauthorized modifications introduced through a supply chain compromise. The modified builds could cause devices meeting specific targeting conditions to perform unintended actions. Only devices that met these conditions and installed the compromised versions were affected. The Live Update client h...

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-506

Tecnología: No especificado

Publicado el: 2025-12-17

CVE-2025-62521

Descripción: ChurchCRM is an open-source church management system. Prior to version 5.21.0, a pre-authentication remote code execution vulnerability in ChurchCRM's setup wizard allows unauthenticated attackers to inject arbitrary PHP code during the initial installation process, leading to complete server compromise. The vulnerability exists in `setup/routes/setup.php` where user input from the setup form i...

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-94

Tecnología: No especificado

Publicado el: 2025-12-17

CVE-2025-34434

Descripción: AVideo versions prior to 20.1 with the ImageGallery plugin enabled is vulnerable to unauthenticated file upload and deletion. Plugin endpoints responsible for managing gallery images fail to enforce authentication checks and do not validate ownership, allowing unauthenticated attackers to upload or delete images associated with any image-based video.

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: CWE-306

Tecnología: No especificado

Publicado el: 2025-12-17

CVE-2025-14832

Descripción: A vulnerability was identified in itsourcecode Online Cake Ordering System 1.0. The affected element is an unknown function of the file /updateproduct.php?action=edit. Such manipulation of the argument ID leads to sql injection. It is possible to launch the attack 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: 2025-12-17

CVE-2025-67791

Descripción: An issue was discovered in DriveLock 24.1 through 24.1.*, 24.2 through 24.2.*, and 25.1 through 25.1.*. An incomplete configuration (agent authentication) in DriveLock tenant allows attackers to impersonate any DriveLock agent on the network against the DES (DriveLock Enterprise Service).

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: 2025-12-17

CVE-2025-14833

Descripción: A security flaw has been discovered in code-projects Online Appointment Booking System 1.0. The impacted element is an unknown function of the file /admin/deletemanagerclinic.php. Performing manipulation of the argument clinic results in sql injection. The attack can be initiated 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: 2025-12-17

CVE-2025-47372

Descripción: Memory Corruption when a corrupted ELF image with an oversized file size is read into a buffer without authentication.

CVSS: 9.0 (CRITICAL)

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

Tipo: CWE-120

Tecnología: No especificado

Publicado el: 2025-12-18

CVE-2025-14878

Descripción: A security flaw has been discovered in Tenda WH450 1.0.0.18. This impacts an unknown function of the file /goform/wirelessRestart of the component HTTP Request Handler. The manipulation of the argument GO results in stack-based buffer overflow. The attack may be performed from remote. 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: 2025-12-18

CVE-2025-64663

Descripción: Custom Question Answering Elevation of Privilege Vulnerability

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-918

Tecnología: No especificado

Publicado el: 2025-12-18

CVE-2025-65037

Descripción: Improper control of generation of code ('code injection') in Azure Container Apps allows an unauthorized attacker to execute code over a network.

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-94

Tecnología: No especificado

Publicado el: 2025-12-18

CVE-2025-65041

Descripción: Improper authorization in Microsoft Partner Center allows an unauthorized attacker to elevate privileges over a network.

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-285

Tecnología: No especificado

Publicado el: 2025-12-18

CVE-2025-14733

Descripción: An Out-of-bounds Write vulnerability in WatchGuard Fireware OS may allow a remote unauthenticated attacker to execute arbitrary code. This vulnerability affects both the Mobile User VPN with IKEv2 and the Branch Office VPN using IKEv2 when configured with a dynamic gateway peer.This vulnerability affects Fireware OS 11.10.2 up to and including 11.12.4_Update1, 12.0 up to and including 12.11.5 a...

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: 2025-12-19

CVE-2025-1928

Descripción: Improper Restriction of Excessive Authentication Attempts vulnerability in Restajet Information Technologies Inc. Online Food Delivery System allows Password Recovery Exploitation.This issue affects Online Food Delivery System: through 19122025.

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-307

Tecnología: No especificado

Publicado el: 2025-12-19

CVE-2025-14964

Descripción: A vulnerability has been found in TOTOLINK T10 4.1.8cu.5083_B20200521. This affects the function sprintf of the file /cgi-bin/cstecgi.cgi. Such manipulation of the argument loginAuthUrl leads to stack-based buffer overflow. The attack may be performed from remote.

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: 2025-12-19

CVE-2025-13329

Descripción: The File Uploader for WooCommerce plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the callback function for the 'add-image-data' REST API endpoint in all versions up to, and including, 1.0.3. This makes it possible for unauthenticated attackers to upload arbitrary files to the Uploadcare service and subsequently download them on the affected s...

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: 2025-12-20

CVE-2025-13619

Descripción: The Flex Store Users plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.1.0. This is due to the 'fsUserHandle::signup' and the 'fsSellerRole::add_role_seller' functions 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 admin...

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: 2025-12-20

Resumen del Reporte

CVEs analizados: 55

Promedio CVSS: 8.54

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat