CVEs más relevantes de la semana

Del 25/10/2025 al 01/11/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-12208

Descripción: A vulnerability was found in SourceCodester Best House Rental Management System 1.0. This impacts the function login2 of the file /admin_class.php. Performing manipulation of the argument Username results in sql injection. The attack is possible to be carried out 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: 2025-10-27

CVE-2025-12210

Descripción: A vulnerability was identified in Tenda O3 1.0.0.10(2478). Affected by this vulnerability is the function SetValue/GetValue of the file /goform/AdvSetLanip. The manipulation of the argument lanIp leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.

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: 2025-10-27

CVE-2025-12211

Descripción: A security flaw has been discovered in Tenda O3 1.0.0.10(2478). Affected by this issue is the function SetValue/GetValue of the file /goform/setDmzInfo. The manipulation of the argument dmzIP results in stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited.

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: 2025-10-27

CVE-2025-12215

Descripción: A flaw has been found in projectworlds Online Shopping System 1.0. Impacted is an unknown function of the file /login_submit.php. Executing manipulation of the argument keywords 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: 2025-10-27

CVE-2025-12226

Descripción: A vulnerability was found in SourceCodester Best House Rental Management System 1.0. Impacted is the function save_house of the file /admin_class.php. Performing manipulation of the argument house_no results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used.

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-74

Tecnología: No especificado

Publicado el: 2025-10-27

CVE-2025-12232

Descripción: A vulnerability was detected in Tenda CH22 1.0.0.1. Affected by this vulnerability is the function fromSafeClientFilter of the file /goform/SafeClientFilter. Performing manipulation of the argument page results in buffer overflow. The attack can be initiated remotely. The exploit is now public and may be used.

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: 2025-10-27

CVE-2025-12237

Descripción: A vulnerability was identified in projectworlds Advanced Library Management System 1.0. Impacted is an unknown function of the file /index.php. Such manipulation of the argument keywords 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: 2025-10-27

CVE-2025-12239

Descripción: A weakness has been identified in TOTOLINK A3300R 17.0.0cu.557_B20221024. The impacted element is the function setDdnsCfg of the file /cgi-bin/cstecgi.cgi. Executing manipulation can lead to buffer overflow. The attack may be performed from remote. The exploit has been made available to the public and could be exploited.

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: 2025-10-27

CVE-2025-12240

Descripción: A security vulnerability has been detected in TOTOLINK A3300R 17.0.0cu.557_B20221024. This affects the function setDmzCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ip leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.

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: 2025-10-27

CVE-2025-12253

Descripción: A vulnerability was determined in AMTT Hotel Broadband Operation System 1.0. Affected by this vulnerability is an unknown functionality of the file /user/portal/get_expiredtime.php. This manipulation of the argument uid causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but...

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: 2025-10-27

CVE-2025-12257

Descripción: A security vulnerability has been detected in SourceCodester Online Student Result System 1.0. This issue affects some unknown processing of the file /view_result.php. The manipulation of the argument ID leads to sql injection. The attack is possible to be carried out 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: 2025-10-27

CVE-2025-12265

Descripción: A weakness has been identified in Tenda CH22 1.0.0.1. Affected by this issue is the function fromVirtualSer of the file /goform/VirtualSer. This manipulation of the argument page causes buffer overflow. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be exploited.

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: 2025-10-27

CVE-2025-12268

Descripción: A vulnerability has been found in LearnHouse up to 98dfad76aad70711a8113f6c1fdabfccf10509ca. Impacted is an unknown function of the file /api/v1/courses/ of the component Course Thumbnail Handler. The manipulation of the argument thumbnail leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. This product is u...

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: 2025-10-27

CVE-2025-12271

Descripción: A vulnerability was identified in Tenda CH22 1.0.0.1. This affects the function fromRouteStatic of the file /goform/RouteStatic. Such manipulation of the argument page leads to buffer overflow. The attack can be launched remotely. The exploit is publicly available and might be used.

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: 2025-10-27

CVE-2025-12272

Descripción: A security flaw has been discovered in Tenda CH22 1.0.0.1. This impacts the function fromAddressNat of the file /goform/addressNat. Performing manipulation of the argument page results in buffer overflow. The attack may be initiated remotely. The exploit has been released to the public and may be exploited.

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: 2025-10-27

CVE-2025-12273

Descripción: A weakness has been identified in Tenda CH22 1.0.0.1. Affected is the function fromwebExcptypemanFilter of the file /goform/webExcptypemanFilter. Executing manipulation of the argument page can lead to buffer overflow. The attack may be launched remotely. The exploit has been made available to the public and could be exploited.

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: 2025-10-27

CVE-2025-12309

Descripción: A weakness has been identified in code-projects Nero Social Networking Site 1.0. This affects an unknown part of the file /friendprofile.php. Executing manipulation of the argument ID can lead to sql injection. It is possible to launch 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: 2025-10-27

CVE-2025-12314

Descripción: A vulnerability was found in code-projects Food Ordering System 1.0. The impacted element is an unknown function of the file /admin/deleteitem.php. Performing manipulation of the argument itemID results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used.

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-74

Tecnología: No especificado

Publicado el: 2025-10-27

CVE-2025-12315

Descripción: A vulnerability was determined in code-projects Food Ordering System 1.0. This affects an unknown function of the file /admin/menu.php. Executing manipulation of the argument itemPrice can lead to sql injection. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.

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-74

Tecnología: No especificado

Publicado el: 2025-10-27

CVE-2025-12316

Descripción: A vulnerability was identified in code-projects Courier Management System 1.0. This impacts an unknown function of the file /courier/edit-courier.php. The manipulation of the argument OfficeName 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: 2025-10-27

CVE-2025-12325

Descripción: A vulnerability has been found in SourceCodester Best Salon Management System 1.0. This affects an unknown part of the file /panel/forgot-password.php. The manipulation of the argument email leads to sql injection. The attack can 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: 2025-10-27

CVE-2025-36386

Descripción: IBM Maximo Application Suite 9.0.0 through 9.0.15 and 9.1.0 through 9.1.4 could allow a remote attacker to bypass authentication mechanisms and gain unauthorized access to the application.

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-305

Tecnología: No especificado

Publicado el: 2025-10-28

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

Resumen del Reporte

CVEs analizados: 27

Promedio CVSS: 8.03

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat ▯