CVEs más relevantes de la semana

Del 21/10/2025 al 28/10/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-41723

Descripción: The importFile SOAP method is vulnerable to a directory traversal attack. An unauthenticated remote attacker bypass the path restriction and upload files to arbitrary locations.

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-35

Tecnología: No especificado

Publicado el: 2025-10-22

CVE-2025-57870

Descripción: A SQL Injection vulnerability exists in Esri ArcGIS Server versions 11.3, 11.4 and 11.5 on Windows, Linux and Kubernetes. This vulnerability allows a remote, unauthenticated attacker to execute arbitrary SQL commands via a specific ArcGIS Feature Service operation. Successful exploitation can potentially result in unauthorized access, modification, or deletion of data from the underlying Enterp...

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-89

Tecnología: No especificado

Publicado el: 2025-10-22

CVE-2025-11023

Descripción: Inclusion of Functionality from Untrusted Control Sphere, Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ArkSigner Software and Hardware Inc. AcBakImzala allows PHP Local File Inclusion.This issue affects AcBakImzala: before v5.1.4.

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-98

Tecnología: No especificado

Publicado el: 2025-10-23

CVE-2025-59273

Descripción: Improper access control in Azure Event Grid allows an unauthorized attacker to elevate privileges over a network.

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-284

Tecnología: No especificado

Publicado el: 2025-10-23

CVE-2025-59503

Descripción: Server-side request forgery (ssrf) in Azure Compute Gallery allows an authorized attacker to elevate privileges over a network.

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: 2025-10-23

CVE-2025-6440

Descripción: The WooCommerce Designer Pro plugin for WordPress, used by the Pricom - Printing Company & Design Services WordPress theme, is vulnerable to arbitrary file uploads due to missing file type validation in the 'wcdp_save_canvas_design_ajax' function in all versions up to, and including, 1.9.26. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's se...

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: 2025-10-24

CVE-2025-11253

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Aksis Technology Inc. Netty ERP allows SQL Injection.This issue affects Netty ERP: before V.1.1000.

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: 2025-10-24

CVE-2025-62717

Descripción: Emlog is an open source website building system. In version 2.5.23, Emlog Pro is vulnerable to a session verification code error due to a clearing logic error. This means the verification code could be reused anywhere an email verification code is required. This issue has been fixed in commit 1f726df.

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-287

Tecnología: No especificado

Publicado el: 2025-10-24

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-2025-12271

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-2025-36386

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

Resumen del Reporte

CVEs analizados: 24

Promedio CVSS: 8.57

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat