CVEs más relevantes de la semana

Del 16/12/2025 al 23/12/2025

Porque el primer paso para defender es conocer las amenazas.

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

CVE-2025-15006

Descripción: A weakness has been identified in Tenda WH450 1.0.0.18. Affected by this vulnerability is an unknown functionality of the file /goform/CheckTools of the component HTTP Request Handler. This manipulation of the argument ipaddress causes stack-based buffer overflow. The attack can be initiated remotely. The exploit has been made available to the public and could 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: 2025-12-22

CVE-2025-15007

Descripción: A security vulnerability has been detected in Tenda WH450 1.0.0.18. Affected by this issue is some unknown functionality of the file /goform/L7Im of the component HTTP Request Handler. Such manipulation of the argument page leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.

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: 2025-12-22

CVE-2025-15010

Descripción: A vulnerability has been found in Tenda WH450 1.0.0.18. This issue affects some unknown processing of the file /goform/SafeUrlFilter. The manipulation of the argument page leads to stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.

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: 2025-12-22

CVE-2025-15016

Descripción: Enterprise Cloud Database developed by Ragic has a Hard-coded Cryptographic Key vulnerability, allowing unauthenticated remote attackers to exploit the fixed key to generate verification information and log into the system as any user.

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: 2025-12-22

CVE-2025-14388

Descripción: The PhastPress plugin for WordPress is vulnerable to Unauthenticated Arbitrary File Read via null byte injection in all versions up to, and including, 3.7. This is due to a discrepancy between the extension validation in `getExtensionForURL()` which operates on URL-decoded paths, and `appendNormalized()` which strips everything after a null byte before constructing the filesystem path. This mak...

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-158

Tecnología: No especificado

Publicado el: 2025-12-23

Resumen del Reporte

CVEs analizados: 21

Promedio CVSS: 9.49

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat