

# CVEs más relevantes de la semana

Del 20/12/2025 al 27/12/2025

Porque el primer paso para defender es conocer las amenazas.



# 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-2025-15011

Descripción: A vulnerability was found in code-projects Simple Stock System 1.0. Impacted is an unknown function of the file /logout.php. The manipulation of the argument uname 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: 2025-12-22



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-2025-15012

Descripción: A vulnerability was determined in code-projects Refugee Food Management System 1.0. The affected element is an unknown function of the file /home/home.php. This manipulation of the argument a 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: 2025-12-22



CVE-2025-15034

Descripción: A security flaw has been discovered in its source code Student Management System 1.0. This affects an unknown part of the file /record.php. The manipulation of the argument ID 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: 2025-12-23



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



CVE-2025-15044

Descripción: A vulnerability was detected in Tenda WH450 1.0.0.18. Impacted is an unknown function of the file /goform/NatStaticSetting. The manipulation of the argument page results in stack-based buffer overflow. The attack may be performed from remote. The exploit is now 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: 2025-12-23



# CVE-2025-15045

Descripción: A flaw has been found in Tenda WH450 1.0.0.18. The affected element is an unknown function of the file /goform/Natlimit of the component HTTP Request Handler. This manipulation of the argument page causes stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been published 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: 2025-12-23



CVE-2025-15046

Descripción: A vulnerability has been found in Tenda WH450 1.0.0.18. The impacted element is an unknown function of the file /goform/PPTPClient of the component HTTP Request Handler. Such manipulation of the argument netmsk leads to stack-based buffer overflow. It is possible to launch the attack remotely. 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: 2025-12-23



CVE-2025-15047

Descripción: A vulnerability was found in Tenda WH450 1.0.0.18. This affects an unknown function of the file /goform/PPTPDClient of the component HTTP Request Handler. Performing manipulation of the argument Username results in stack-based buffer overflow. The attack can be initiated remotely. The exploit has been made public and could 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: 2025-12-23



CVE-2025-13773

Descripción: The Print Invoice & Delivery Notes for WooCommerce plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 5.8.0 via the 'WooCommerce\_Delivery\_Notes::update' function. This is due to missing capability check in the 'WooCommerce\_Delivery\_Notes::update' function, PHP enabled in Dompdf, and missing escape in the 'template.php' file. This makes it possible ...

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-94

Tecnología: No especificado

Publicado el: 2025-12-24



CVE-2025-13915

Descripción: IBM API Connect 10.0.8.0 through 10.0.8.5, and 10.0.11.0 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: 2025-12-26



## Resumen del Reporte

CVEs analizados: 14

Promedio CVSS: 9.26

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat ☺

