CVEs más relevantes de la semana

Del 23/12/2025 al 30/12/2025

Porque el primer paso para defender es conocer las amenazas.

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

CVE-2025-15226

Descripción: WMPro developed by Sunnet has a Arbitrary File Upload vulnerability, allowing unauthenticated remote attackers to upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.

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: 2025-12-29

CVE-2025-15228

Descripción: BPMFlowWebkit developed by WELLTEND TECHNOLOGY has a Arbitrary File Upload vulnerability, allowing unauthenticated remote attackers to upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.

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: 2025-12-29

CVE-2025-15194

Descripción: A vulnerability was found in D-Link DIR-600 up to 2.15WWb02. Affected by this vulnerability is an unknown functionality of the file hedwig.cgi of the component HTTP Header Handler. The manipulation of the argument Cookie results in stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been made public and could be used. This vulnerability only affects produc...

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: 2025-12-29

CVE-2025-15255

Descripción: A vulnerability was determined in Tenda W6-S 1.0.0.4(510). This impacts an unknown function of the file /bin/httpd of the component R7websSsecurityHandler. Executing manipulation of the argument Cookie can lead to stack-based buffer overflow. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.

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: 2025-12-30

Resumen del Reporte

CVEs analizados: 10

Promedio CVSS: 9.80

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat