CVEs más relevantes de la semana

Del 07/06/2025 al 14/06/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-5855

Descripción: A vulnerability, which was classified as critical, was found in Tenda AC6 15.03.05.16. This affects the function formSetRebootTimer of the file /goform/SetRebootTimer. The manipulation of the argument rebootTime leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the 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: 2025-06-09

CVE-2025-5856

Descripción: A vulnerability has been found in PHPGurukul BP Monitoring Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /registration.php. The manipulation of the argument emailid 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: 2025-06-09

CVE-2025-5860

Descripción: A vulnerability, which was classified as critical, was found in PHPGurukul Maid Hiring Management System 1.0. This affects an unknown part of the file /admin/search-booking-request.php. The manipulation of the argument searchdata leads to sql injection. It is possible to initiate the attack 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: 2025-06-09

CVE-2025-5861

Descripción: A vulnerability has been found in Tenda AC7 15.03.06.44 and classified as critical. This vulnerability affects the function fromadvsetlanip of the file /goform/AdvSetLanip. The manipulation of the argument lanMask leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the 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: 2025-06-09

CVE-2025-5862

Descripción: A vulnerability was found in Tenda AC7 15.03.06.44 and classified as critical. This issue affects the function formSetPPTPUserList of the file /goform/setPptpUserList. The manipulation of the argument list leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the 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: 2025-06-09

CVE-2025-5863

Descripción: A vulnerability was found in Tenda AC5 15.03.06.47. It has been classified as critical. Affected is the function formSetRebootTimer of the file /goform/SetRebootTimer. The manipulation of the argument rebootTime 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: 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: 2025-06-09

CVE-2025-5893

Descripción: Smart Parking Management System from Honding Technology has an Exposure of Sensitive Information vulnerability, allowing unauthenticated remote attackers to access a specific page and obtain plaintext administrator credentials.

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-256

Tecnología: No especificado

Publicado el: 2025-06-09

CVE-2025-42989

Descripción: RFC inbound processing□does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. On successful exploitation the attacker could critically impact both integrity and availability of the application.

CVSS: 9.6 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:H

Tipo: CWE-862

Tecnología: No especificado

Publicado el: 2025-06-10

CVE-2025-5906

Descripción: A vulnerability classified as critical has been found in code-projects Laundry System 1.0. This affects an unknown part of the file /data/. The manipulation leads to missing authentication. It is possible to initiate the attack 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-287

Tecnología: No especificado

Publicado el: 2025-06-10

CVE-2025-40585

Descripción: A vulnerability has been identified in Energy Services (All versions with G5DFR). Affected solutions using G5DFR contain default credentials. This could allow an attacker to gain control of G5DFR component and tamper with outputs from the device.

CVSS: 9.9 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:L

Tipo: CWE-276

Tecnología: No especificado

Publicado el: 2025-06-10

CVE-2025-47110

Descripción: Adobe Commerce versions 2.4.8, 2.4.7-p5, 2.4.6-p10, 2.4.5-p12, 2.4.4-p13 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a high privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.

CVSS: 9.1 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Tipo: CWE-79

Tecnología: No especificado

Publicado el: 2025-06-10

CVE-2025-32711

Descripción: Ai command injection in M365 Copilot allows an unauthorized attacker to disclose information over a network.

CVSS: 9.3 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N

Tipo: CWE-77

Tecnología: No especificado

Publicado el: 2025-06-11

CVE-2025-4973

Descripción: The Workreap plugin for WordPress, used by the Workreap - Freelance Marketplace WordPress Theme, is vulnerable to authentication bypass in all versions up to, and including, 3.3.1. This is due to the plugin not properly verifying a user's identity prior to logging them in when verifying an account with an email address. This makes it possible for unauthenticated attackers to log in as registere...

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: 2025-06-12

CVE-2025-5288

Descripción: The REST API | Custom API Generator For Cross Platform And Import Export In WP plugin for WordPress is vulnerable to Privilege Escalation due to a missing capability check on the process_handler() function in versions 1.0.0 to 2.0.3. This makes it possible for unauthenticated attackers to POST an arbitrary import_api URL, import specially crafted JSON, and thereby create a new user with full Ad...

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: 2025-06-13

CVE-2025-6065

Descripción: The Image Resizer On The Fly plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the 'delete' task in all versions up to, and including, 1.1. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).

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-22

Tecnología: No especificado

Publicado el: 2025-06-14

Resumen del Reporte

CVEs analizados: 15

Promedio CVSS: 8.90

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat □