CVEs más relevantes de la semana

Del 10/06/2025 al 17/06/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-5979

Descripción: A vulnerability classified as critical has been found in code-projects School Fees Payment System 1.0. This affects an unknown part of the file /branch.php. The manipulation of the argument ID 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: 2025-06-10

CVE-2025-5980

Descripción: A vulnerability classified as critical was found in code-projects Restaurant Order System 1.0. This vulnerability affects unknown code of the file /order.php. The manipulation of the argument tabidNoti 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: 2025-06-10

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

CVE-2025-6098

Descripción: A vulnerability was found in UTT □□ 750W up to 5.0. It has been classified as critical. This affects the function strcpy of the file /goform/setSysAdm of the component API. The manipulation of the argument passwd1 leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this discl...

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: 2025-06-16

CVE-2025-6169

Descripción: The WIMP website co-construction management platform from HAMASTAR Technology has a SQL Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read, modify, and delete database contents.

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: 2025-06-16

CVE-2025-6121

Descripción: A vulnerability, which was classified as critical, has been found in D-Link DIR-632 FW103B08. Affected by this issue is the function get_pure_content of the component HTTP POST Request Handler. The manipulation of the argument Content-Length leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. This vulnerability...

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: 2025-06-16

CVE-2025-49794

Descripción: A use-after-free vulnerability was found in libxml2. This issue occurs when parsing XPath elements under certain circumstances when the XML schematron has the <sch:name path="..."/> schema elements. This flaw allows a malicious actor to craft a malicious XML document used as input for libxml, resulting in the program's crash using libxml or other possible undefined behaviors.

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-825

Tecnología: No especificado

Publicado el: 2025-06-16

CVE-2025-49796

Descripción: A vulnerability was found in libxml2. Processing certain sch:name elements from the input XML file can trigger a memory corruption issue. This flaw allows an attacker to craft a malicious XML input file that can lead libxml to crash, resulting in a denial of service or other possible undefined behavior due to sensitive data being corrupted in memory.

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-125

Tecnología: No especificado

Publicado el: 2025-06-16

Resumen del Reporte

CVEs analizados: 11

Promedio CVSS: 9.11

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat