CVEs más relevantes de la semana

Del 14/06/2025 al 21/06/2025

Porque el primer paso para defender es conocer las amenazas.

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

CVE-2025-1562

Descripción: The Recover WooCommerce Cart Abandonment, Newsletter, Email Marketing, Marketing Automation By FunnelKit plugin for WordPress is vulnerable to unauthorized arbitrary plugin installation due to a missing capability check on the install_or_activate_addon_plugins() function and a weak nonce hash in all versions up to, and including, 3.5.3. This makes it possible for unauthenticated attackers to in...

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: 2025-06-18

CVE-2025-20260

Descripción: A vulnerability in the PDF scanning processes of ClamAV could allow an unauthenticated, remote attacker to cause a buffer overflow condition, cause a denial of service (DoS) condition, or execute arbitrary code on an affected device. This vulnerability exists because memory buffers are allocated incorrectly when PDF files are processed. An attacker could exploit this vulnerability by submitt...

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-122

Tecnología: No especificado

Publicado el: 2025-06-18

CVE-2025-4738

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Yirmibes Software MY ERP allows SQL Injection.This issue affects MY ERP: before 1.170.

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: 2025-06-19

CVE-2025-33117

Descripción: IBM QRadar SIEM 7.5 through 7.5.0 Update Package 12 could allow a privileged user to modify configuration files that would allow the upload of a malicious autoupdate file to execute arbitrary commands.

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-73

Tecnología: No especificado

Publicado el: 2025-06-19

Resumen del Reporte

CVEs analizados: 9

Promedio CVSS: 9.57

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat