CVEs más relevantes de la semana

Del 08/11/2025 al 15/11/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-12868

Descripción: New Site Server developed by CyberTutor has a Use of Client-Side Authentication vulnerability, allowing unauthenticated remote attackers to modify the frontend code to gain administrator privileges on the website.

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-603

Tecnología: No especificado

Publicado el: 2025-11-10

CVE-2025-42887

Descripción: Due to missing input sanitation, SAP Solution Manager allows an authenticated attacker to insert malicious code when calling a remote-enabled function module. This could provide the attacker with full control of the system hence leading to high impact on confidentiality, integrity and availability of the system.

CVSS: 9.9 (CRITICAL)

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

Tipo: CWE-94

Tecnología: No especificado

Publicado el: 2025-11-11

CVE-2025-42890

Descripción: SQL Anywhere Monitor (Non-GUI) baked credentials into the code,exposing the resources or functionality to unintended users and providing attackers with the possibility of arbitrary code execution.This could cause high impact on confidentiality integrity and availability of the system.

CVSS: 10.0 (CRITICAL)

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

Tipo: CWE-798

Tecnología: No especificado

Publicado el: 2025-11-11

CVE-2025-11170

Descripción: The WP□□□□□□□□□ for CPI plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the Cpiwm_Import_Controller::import function in all versions up to, and including, 1.0.2. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution 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-434

Tecnología: No especificado

Publicado el: 2025-11-11

CVE-2025-11457

Descripción: The EasyCommerce – AI-Powered, Fast & Beautiful WordPress Ecommerce Plugin plugin for WordPress is vulnerable to Privilege Escalation in versions 0.9.0-beta2 to 1.5.0. This is due to the /easycommerce/v1/orders REST API endpoint not properly restricting the ability for users to select roles during registration. This makes it possible for unauthenticated attackers to gain administrator-level acc...

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-269

Tecnología: No especificado

Publicado el: 2025-11-11

CVE-2025-12813

Descripción: The Holiday class post calendar plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 7.1 via the 'contents' parameter. This is due to a lack of sanitization of user-supplied data when creating a cache file. This makes it possible for unauthenticated attackers to execute code 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-94

Tecnología: No especificado

Publicado el: 2025-11-11

CVE-2025-12539

Descripción: The TNC Toolbox: Web Performance plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.4.2. This is due to the plugin storing cPanel API credentials (hostname, username, and API key) in files within the web-accessible wp-content directory without adequate protection in the "Tnc_Wp_Toolbox_Settings::save_settings" function. This makes it pos...

CVSS: 10.0 (CRITICAL)

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

Tipo: CWE-922

Tecnología: No especificado

Publicado el: 2025-11-11

CVE-2025-60724

Descripción: Heap-based buffer overflow in Microsoft Graphics Component allows an unauthorized attacker to execute code over a network.

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: 2025-11-11

CVE-2025-11366

Descripción: N-central < 2025.4 is vulnerable to authentication bypass via path traversal

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-22

Tecnología: No especificado

Publicado el: 2025-11-12

CVE-2025-11367

Descripción: The N-central Software Probe < 2025.4 is vulnerable to Remote Code Execution via deserialization

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-502

Tecnología: No especificado

Publicado el: 2025-11-12

CVE-2025-36096

Descripción: IBM AIX 7.2, and 7.3 and IBM VIOS 3.1, and 4.1 stores NIM private keys used in NIM environments in an insecure way which is susceptible to unauthorized access by an attacker using man in the middle techniques.

CVSS: 9.0 (CRITICAL)

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

Tipo: CWE-522

Tecnología: No especificado

Publicado el: 2025-11-13

CVE-2025-36250

Descripción: IBM AIX 7.2, and 7.3 and IBM VIOS 3.1, and 4.1 NIM server (formerly known as NIM master) service (nimesis) could allow a remote attacker to execute arbitrary commands due to improper process controls. This addresses additional attack vectors for a vulnerability that was previously addressed in CVE-2024-56346.

CVSS: 10.0 (CRITICAL)

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

Tipo: CWE-114

Tecnología: No especificado

Publicado el: 2025-11-13

CVE-2025-36251

Descripción: IBM AIX 7.2, and 7.3 and IBM VIOS 3.1, and 4.1 nimsh service SSL/TLS implementations could allow a remote attacker to execute arbitrary commands due to improper process controls. This addresses additional attack vectors for a vulnerability that was previously addressed in CVE-2024-56347.

CVSS: 9.6 (CRITICAL)

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

Tipo: CWE-114

Tecnología: No especificado

Publicado el: 2025-11-13

CVE-2025-13188

Descripción: A vulnerability was detected in D-Link DIR-816L 2_06_b09_beta. Affected by this vulnerability is the function authenticationcgi_main of the file /authentication.cgi. Performing manipulation of the argument Password results in stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit is now public and may be used. This vulnerability only affects products that are no...

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: 2025-11-14

Resumen del Reporte

CVEs analizados: 14

Promedio CVSS: 9.78

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat