CVEs más relevantes de la semana

Del 04/11/2025 al 11/11/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-47776

Descripción: Mantis Bug Tracker (MantisBT) is an open source issue tracker. Due to incorrect use of loose (==) instead of strict (===) comparison in the authentication code in versions 2.27.1 and below.PHP type juggling will cause certain MD5 hashes matching scientific notation to be interpreted as numbers. Instances using the MD5 login method allow an attacker who knows the victim's username and has access...

CVSS: 9.1 (CRITICAL)

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

Tipo: CWE-305

Tecnología: No especificado

Publicado el: 2025-11-04

CVE-2025-11749

Descripción: The AI Engine plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.1.3 via the /mcp/v1/ REST API endpoint that exposes the 'Bearer Token' value when 'No-Auth URL' is enabled. This makes it possible for unauthenticated attackers to extract the bearer token, which can be used to gain access to a valid session and perform many actions like cr...

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-200

Tecnología: No especificado

Publicado el: 2025-11-05

CVE-2025-12674

Descripción: The KiotViet Sync plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the create_media() function in all versions up to, and including, 1.8.5. 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: 2025-11-05

CVE-2025-47151

Descripción: A type confusion vulnerability exists in the lasso_node_impl_init_from_xml functionality of Entr&#39;ouvert Lasso 2.5.1 and 2.8.2. A specially crafted SAML response can lead to an arbitrary code execution. An attacker can send a malformed SAML response to trigger 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-843

Tecnología: No especificado

Publicado el: 2025-11-05

CVE-2025-20354

Descripción: A vulnerability in the Java Remote Method Invocation (RMI) process of Cisco Unified CCX could allow an unauthenticated, remote attacker to upload arbitrary files and execute arbitrary commands with root permissions on an affected system. This vulnerability is due to improper authentication mechanisms that are associated to specific Cisco Unified CCX features. An attacker could exploit this v...

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: 2025-11-05

CVE-2025-20358

Descripción: A vulnerability in the Contact Center Express (CCX) Editor application of Cisco Unified CCX could allow an unauthenticated, remote attacker to bypass authentication and obtain administrative permissions pertaining to script creation and execution.   This vulnerability is due to improper authentication mechanisms in the communication between the CCX Editor and an affected Unified CCX server. An...

CVSS: 9.4 (CRITICAL)

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

Tipo: CWE-306

Tecnología: No especificado

Publicado el: 2025-11-05

CVE-2025-45378

Descripción: Dell CloudLink, versions 8.0 through 8.1.2, contain vulnerability on restricted shell. A Privileged user with known password can break into command shell of CloudLink server and gain access of shell and escalate privilege, gain unauthorized access of system.

If ssh is enabled with web credentials of server, attack is possible through network with known privileged user/password.

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-78

Tecnología: No especificado

Publicado el: 2025-11-05

CVE-2025-62161

Descripción: Youki is a container runtime written in Rust. In versions 0.5.6 and below, the initial validation of the source /dev/null is insufficient, allowing container escape when youki utilizes bind mounting the container's /dev/null as a file mask. This issue is fixed in version 0.5.7.

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-61

Tecnología: No especificado

Publicado el: 2025-11-06

CVE-2025-62596

Descripción: Youki is a container runtime written in Rust. In versions 0.5.6 and below, youki's apparmor handling performs insufficiently strict write-target validation, and when combined with path substitution during pathname resolution, can allow writes to unintended procfs locations. While resolving a path component-by-component, a shared-mount race can substitute intermediate components and redirect the...

CVSS: 10.0 (CRITICAL)

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

Tipo: CWE-61

Tecnología: No especificado

Publicado el: 2025-11-06

CVE-2025-64163

Descripción: DataEase is an open source data visualization analysis tool. In versions 2.10.14 and below, the vendor added a blacklist to filter ldap:// and ldaps://. However, omission of protection for the dns:// protocol results in an SSRF vulnerability. This issue is fixed in version 2.10.15.

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-918

Tecnología: No especificado

Publicado el: 2025-11-06

CVE-2025-64164

Descripción: Dataease is an open source data visualization analysis tool. In versions 2.10.14 and below, DataEase did not properly filter when establishing JDBC connections to Oracle, resulting in a risk of JNDI injection (Java Naming and Directory Interface injection). This issue is fixed in version 2.10.15.

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: 2025-11-06

CVE-2025-27918

Descripción: An issue was discovered in AnyDesk before 9.0.0. It has an integer overflow and resultant heap-based buffer overflow via a UDP packet during processing of an Identity user image within the Discovery feature, or when establishing a connection between any two clients.

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-190

Tecnología: No especificado

Publicado el: 2025-11-06

CVE-2025-12352

Descripción: The Gravity Forms plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the copy_post_image() function in all versions up to, and including, 2.9.20. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. This only impacts sites that have allow_url_fo...

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: 2025-11-07

CVE-2025-10230

Descripción: A flaw was found in Samba, in the front-end WINS hook handling: NetBIOS names from registration packets are passed to a shell without proper validation or escaping. Unsanitized NetBIOS name data from WINS registration packets are inserted into a shell command and executed by the Samba Active Directory Domain Controller's wins hook, allowing an unauthenticated network attacker to achieve remote ...

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-78

Tecnología: No especificado

Publicado el: 2025-11-07

CVE-2025-12866

Descripción: EIP Plus developed by Hundred Plus has a Weak Password Recovery Mechanism vulnerability, allowing unauthenticated remote attacker to predict or brute-force the 'forgot password' link, thereby successfully resetting any user's password.

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-640

Tecnología: No especificado

Publicado el: 2025-11-10

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

Resumen del Reporte

CVEs analizados: 22

Promedio CVSS: 9.77

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat ▯