CVEs más relevantes de la semana

Del 19/07/2025 al 26/07/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2015-10138

Descripción: The Work The Flow File Upload plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the jQuery-File-Upload-9.5.0 server and test files in versions up to, and including, 2.5.2. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected sites 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: 2025-07-19

CVE-2025-7838

Descripción: A vulnerability has been found in Campcodes Online Movie Theater Seat Reservation System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/manage_seat.php. The manipulation of the argument ID 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: 2025-07-19

CVE-2025-7862

Descripción: A vulnerability has been found in TOTOLINK T6 4.1.5cu.748_B20211015 and classified as critical. Affected by this vulnerability is the function setTelnetCfg of the file /cgi-bin/cstecgi.cgi of the component Telnet Service. The manipulation of the argument telnet_enabled with the input 1 leads to missing authentication. The attack can be launched remotely. The exploit has been disclosed to the pu...

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: 2025-07-20

CVE-2025-7343

Descripción: The SFT developed by Digiwin 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: 2025-07-21

CVE-2025-7921

Descripción: Certain modem models developed by Askey has a Stack-based Buffer Overflow vulnerability, allowing unauthenticated remote attackers to control the program's execution flow and potentially execute arbitrary code.

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-121

Tecnología: No especificado

Publicado el: 2025-07-21

CVE-2025-7933

Descripción: A vulnerability classified as critical was found in Campcodes Sales and Inventory System 1.0. This vulnerability affects unknown code of the file /pages/settings_update.php of the component Setting Handler. The manipulation of the argument ID 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: 2025-07-21

CVE-2012-10020

Descripción: The FoxyPress plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the uploadify.php file in versions up to, and including, 0.4.2.1. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected sites 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: 2025-07-22

CVE-2015-10137

Descripción: The Website Contact Form With File Upload plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'upload_file()' function in versions up to, and including, 1.3.4. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected sites 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: 2025-07-22

CVE-2025-6187

Descripción: The bSecure plugin for WordPress is vulnerable to Privilege Escalation due to missing authorization within its order_info REST endpoint in versions 1.3.7 through 1.7.9. The plugin registers the /webhook/v2/order_info/ route with a permission_callback that always returns true, effectively bypassing all authentication. This makes it possible for unauthenticated attackers who know any user's email...

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: 2025-07-22

CVE-2025-4285

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Rolantis Information Technologies Agentis allows SQL Injection.This issue affects Agentis: before 4.32.

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-89

Tecnología: No especificado

Publicado el: 2025-07-22

CVE-2025-41687

Descripción: An unauthenticated remote attacker may use a stack based buffer overflow in the u-link Management API to gain full access on the affected devices.

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-121

Tecnología: No especificado

Publicado el: 2025-07-23

CVE-2025-7437

Descripción: The Ebook Store plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the ebook_store_save_form function in all versions up to, and including, 5.8012. 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: 2025-07-24

CVE-2025-7852

Descripción: The WPBookit plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the image_upload_handle() function hooked via the 'add_new_customer' route in all versions up to, and including, 1.0.6. The plugin's image-upload handler calls move_uploaded_file() on client-supplied files without restricting allowed extensions or MIME types, nor sanitizing the filen...

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: 2025-07-24

CVE-2025-6380

Descripción: The ONLYOFFICE Docs plugin for WordPress is vulnerable to Privilege Escalation due to missing authorization within its oo.callback REST endpoint in versions 1.1.0 to 2.2.0. The plugin's permission callback only verifies that the supplied, encrypted attachment ID maps to an existing attachment post, but does not verify the requester's identity or capabilities. This makes it possible for unauthen...

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: 2025-07-24

CVE-2025-6441

Descripción: The Webinar Solution: Create live/evergreen/automated/instant webinars, stream & Zoom Meetings | WebinarIgnition plugin for WordPress is vulnerable to unauthenticated login token generation due to a missing capability check on the `webinarignition_sign_in_support_staff` and `webinarignition_register_support` functions in all versions up to, and including, 4.03.31. This makes it possible for una...

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: 2025-07-24

CVE-2025-4822

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Bayraktar Solar Energies ScadaWatt Otopilot allows SQL Injection.This issue affects ScadaWatt Otopilot: before 27.05.2025.

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: 2025-07-24

CVE-2025-5243

Descripción: Unrestricted Upload of File with Dangerous Type, Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in SMG Software Information Portal allows Code Injection, Upload a Web Shell to a Web Server, Code Inclusion.This issue affects Information Portal: before 13.06.2025.

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: 2025-07-24

CVE-2025-4784

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Moderec Tourtella allows SQL Injection.This issue affects Tourtella: before 26.05.2025.

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: 2025-07-24

CVE-2025-41420

Descripción: A cross-site scripting (xss) vulnerability exists in the userLogin cancelUri parameter functionality of WWBN AVideo 14.4 and dev master commit 8a8954ff. A specially crafted HTTP request can lead to arbitrary Javascript execution. An attacker can get a user to visit a webpage to trigger this vulnerability.

CVSS: 9.6 (CRITICAL)

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

Tipo: CWE-79

Tecnología: No especificado

Publicado el: 2025-07-24

CVE-2025-46410

Descripción: A cross-site scripting (xss) vulnerability exists in the managerPlaylists PlaylistOwnerUsersId parameter functionality of WWBN AVideo 14.4 and dev master commit 8a8954ff. A specially crafted HTTP request can lead to arbitrary Javascript execution. An attacker can get a user to visit a webpage to trigger this vulnerability.

CVSS: 9.6 (CRITICAL)

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

Tipo: CWE-79

Tecnología: No especificado

Publicado el: 2025-07-24

CVE-2025-50128

Descripción: A cross-site scripting (xss) vulnerability exists in the videoNotFound 404ErrorMsg parameter functionality of WWBN AVideo 14.4 and dev master commit 8a8954ff. A specially crafted HTTP request can lead to arbitrary Javascript execution. An attacker can get a user to visit a webpage to trigger this vulnerability.

CVSS: 9.6 (CRITICAL)

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

Tipo: CWE-79

Tecnología: No especificado

Publicado el: 2025-07-24

CVE-2025-53084

Descripción: A cross-site scripting (xss) vulnerability exists in the videosList page parameter functionality of WWBN AVideo 14.4 and dev master commit 8a8954ff. A specially crafted HTTP request can lead to arbitrary Javascript execution. An attacker can get a user to visit a webpage to trigger this vulnerability.

CVSS: 9.0 (CRITICAL)

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

Tipo: CWE-79

Tecnología: No especificado

Publicado el: 2025-07-24

CVE-2015-10143

Descripción: The Platform theme for WordPress is vulnerable to unauthorized modification of data that can lead to privilege escalation due to a missing capability check on the *_ajax_save_options() function in all versions up to 1.4.4 (exclusive). This makes it possible for unauthenticated attackers to update arbitrary options on the WordPress site. This can be leveraged to update the default role for regis...

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: 2025-07-25

CVE-2019-25224

Descripción: The WP Database Backup plugin for WordPress is vulnerable to OS Command Injection in versions before 5.2 via the mysqldump function. This vulnerability allows unauthenticated attackers to execute arbitrary commands on the host operating system.

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-78

Tecnología: No especificado

Publicado el: 2025-07-25

CVE-2025-6895

Descripción: The Melapress Login Security plugin for WordPress is vulnerable to Authentication Bypass due to missing authorization within the get_valid_user_based_on_token() function in versions 2.1.0 to 2.1.1. This makes it possible for unauthenticated attackers who know an arbitrary user meta value to bypass authentication checks and log in as that user.

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: 2025-07-26

Resumen del Reporte

CVEs analizados: 25

Promedio CVSS: 9.46

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat