CVEs más relevantes de la semana

Del 22/07/2025 al 29/07/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-54447

Descripción: Unrestricted Upload of File with Dangerous Type vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.

CVSS: 8.1 (HIGH)

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

Tipo: CWE-434

Tecnología: No especificado

Publicado el: 2025-07-23

CVE-2025-54450

Descripción: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.

CVSS: 7.2 (HIGH)

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

Tipo: CWE-22

Tecnología: No especificado

Publicado el: 2025-07-23

CVE-2025-54452

Descripción: Improper Authentication vulnerability in Samsung Electronics MagicINFO 9 Server allows Authentication Bypass.This issue affects MagicINFO 9 Server: less than 21.1080.0.

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: 2025-07-23

CVE-2025-54453

Descripción: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.

CVSS: 8.8 (HIGH)

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

Tipo: CWE-22

Tecnología: No especificado

Publicado el: 2025-07-23

CVE-2025-54454

Descripción: Use of Hard-coded Credentials vulnerability in Samsung Electronics MagicINFO 9 Server allows Authentication Bypass.This issue affects MagicINFO 9 Server: less than 21.1080.0.

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-798

Tecnología: No especificado

Publicado el: 2025-07-23

CVE-2025-54455

Descripción: Use of Hard-coded Credentials vulnerability in Samsung Electronics MagicINFO 9 Server allows Authentication Bypass.This issue affects MagicINFO 9 Server: less than 21.1080.0.

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-798

Tecnología: No especificado

Publicado el: 2025-07-23

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

CVE-2025-6918

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Ncvav Virtual PBX Software allows SQL Injection.This issue affects Virtual PBX Software: before 09.07.2025.

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: 2025-07-28

CVE-2025-26469

Descripción: An incorrect default permissions vulnerability exists in the CServerSettings::SetRegistryValues functionality of MedDream PACS Premium 7.3.3.840. A specially crafted application can decrypt credentials stored in a configuration-related registry key. An attacker can execute a malicious script or application to exploit this vulnerability.

CVSS: 9.3 (CRITICAL)

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

Tipo: CWE-732

Tecnología: No especificado

Publicado el: 2025-07-28

CVE-2025-27724

Descripción: A privilege escalation vulnerability exists in the login.php functionality of meddream MedDream PACS Premium 7.3.3.840. A specially crafted .php file can lead to elevated capabilities. An attacker can upload a malicious file to trigger this vulnerability.

CVSS: 9.3 (CRITICAL)

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

Tipo: CWE-284

Tecnología: No especificado

Publicado el: 2025-07-28

Resumen del Reporte

CVEs analizados: 24

Promedio CVSS: 9.33

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat