# CVEs más relevantes de la semana

Del 01/07/2025 al 08/07/2025

Porque el primer paso para defender es conocer las amenazas.

# CVE-2025-4380

Descripción: The Ads Pro Plugin - Multi-Purpose WordPress Advertising Manager plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 4.89 via the 'bsa_template' parameter of the `bsa_preview_callback` function. This makes it possible for unauthenticated attackers to include and execute arbitrary files on the server, allowing the execution of any PHP code in those fi...

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-98

Tecnología: No especificado

Publicado el: 2025-07-02

# CVE-2025-4689

Descripción: The Ads Pro Plugin - Multi-Purpose WordPress Advertising Manager plugin for WordPress is vulnerable to Local File Inclusion which leads to Remote Code Execution in all versions up to, and including, 4.89. This is due to the presence of a SQL Injection vulnerability and Local File Inclusion vulnerability that can be chained with an image upload. This makes it possible for unauthenticated attacke...

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-98

Tecnología: No especificado

Publicado el: 2025-07-02

# CVE-2025-5746

Descripción: The Drag and Drop Multiple File Upload (Pro) - WooCommerce plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the dnd_upload_cf7_upload_chunks() function in version 5.0 - 5.0.5 (when bundled with the PrintSpace theme) and all versions up to, and including, 1.7.1 (in the standalone version). This makes it possible for unauthenticated attackers to ...

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: 2025-07-02

# CVE-2024-13786

Descripción: The education theme for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.6.10 via deserialization of untrusted input in the 'themerex_callback_view_more_posts' function. This makes it possible for unauthenticated attackers to inject a PHP Object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless a...

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: 2025-07-02

# CVE-2025-41672

Descripción: A remote unauthenticated attacker may use default certificates to generate JWT Tokens and gain full access to the tool and all connected devices.

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-1188

Tecnología: No especificado

Publicado el: 2025-07-07

# CVE-2025-3626

Descripción: A remote attacker with administrator account can gain full control of the device due to improper neutralization of special elements used in an OS Command ('OS Command Injection') while uploading a config file via webUI.

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: 2025-07-07

# CVE-2025-42963

Descripción: A critical vulnerability in SAP NetWeaver Application server for Java Log Viewer enables authenticated administrator users to exploit unsafe Java object deserialization. Successful exploitation can lead to full operating system compromise, granting attackers complete control over the affected system. This results in a severe impact on the confidentiality, integrity, and availability of the appl...

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-502

Tecnología: No especificado

Publicado el: 2025-07-08

# CVE-2025-42964

Descripción: SAP NetWeaver Enterprise Portal Administration is vulnerable when a privileged user can upload untrusted or malicious content which, when deserialized, could potentially lead to a compromise of confidentiality, integrity, and availability of the host system.

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-502

Tecnología: No especificado

Publicado el: 2025-07-08

# CVE-2025-42966

Descripción: SAP NetWeaver XML Data Archiving Service allows an authenticated attacker with administrative privileges to exploit an insecure Java deserialization vulnerability by sending a specially crafted serialized Java object. This could lead to high impact on confidentiality, integrity, and availability of the application.

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-502

Tecnología: No especificado

Publicado el: 2025-07-08

# CVE-2025-42967

Descripción: SAP S/4HANA and SAP SCM Characteristic Propagation has remote code execution vulnerability. This allows an attacker with user level privileges to create a new report with his own code potentially gaining full control of the affected SAP system causing high impact on confidentiality, integrity, and availability of the application.

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: 2025-07-08

# CVE-2025-42980

Descripción: SAP NetWeaver Enterprise Portal Federated Portal Network is vulnerable when a privileged user can upload untrusted or malicious content which, when deserialized, could potentially lead to a compromise of confidentiality, integrity, and availability of the host system.

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-502

Tecnología: No especificado

Publicado el: 2025-07-08

# CVE-2025-25270

Descripción: An unauthenticated remote attacker can alter the device configuration in a way to get remote code execution as root with specific configurations.

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-913

Tecnología: No especificado

Publicado el: 2025-07-08

# CVE-2025-40736

Descripción: A vulnerability has been identified in SINEC NMS (All versions < V4.0). The affected application exposes an endpoint that allows an unauthorized modification of administrative credentials. This could allow an unauthenticated attacker to reset the superadmin password and gain full control of the application (ZDI-CAN-26569).

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-306

Tecnología: No especificado

Publicado el: 2025-07-08

CVE-2025-21450

Descripción: Cryptographic issue occurs due to use of insecure connection method while downloading.

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-287

Tecnología: No especificado

Publicado el: 2025-07-08

# Resumen del Reporte

CVEs analizados: 14

Promedio CVSS: 9.40

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat