CVEs más relevantes de la semana

Del 18/04/2025 al 25/04/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-3278

Descripción: The UrbanGo Membership plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 1.0.4. This is due to the plugin allowing users who are registering new accounts to set their own role or by supplying 'user_register_role' field. This makes it possible for unauthenticated attackers to gain elevated privileges by creating an account with the administrator role.

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: 2025-04-19

CVE-2025-1093

Descripción: The AIHub theme for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the generate_image function in all versions up to, and including, 1.3.7. 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: 2025-04-19

CVE-2021-4455

Descripción: The Wordpress Plugin Smart Product Review plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in all versions up to, and including, 1.0.4. 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: 2025-04-19

CVE-2025-43928

Descripción: In Infodraw Media Relay Service (MRS) 7.1.0.0, the MRS web server (on port 12654) allows reading arbitrary files via ../ directory traversal in the username field. Reading ServerParameters.xml may reveal administrator credentials in cleartext or with MD5 hashing.

CVSS: 5.8 (MEDIUM)

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

Tipo: CWE-24

Tecnología: No especificado

Publicado el: 2025-04-20

CVE-2025-1950

Descripción: IBM Hardware Management Console - Power Systems V10.2.1030.0 and V10.3.1050.0 could allow a local user to execute commands locally due to improper validation of libraries of an untrusted source.

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-114

Tecnología: No especificado

Publicado el: 2025-04-22

Resumen del Reporte

CVEs analizados: 5

Promedio CVSS: 8.90

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat