CVEs más relevantes de la semana

Del 19/04/2025 al 26/04/2025

Porque el primer paso para defender es conocer las amenazas.

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

CVE-2025-3065

Descripción: The Database Toolset plugin is vulnerable to arbitrary file deletion due to insufficient file path validation in a function in all versions up to, and including, 1.8.4. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).

CVSS: 9.1 (CRITICAL)

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

Tipo: CWE-22

Tecnología: No especificado

Publicado el: 2025-04-24

CVE-2025-3603

Descripción: The Flynax Bridge plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 2.2.0. This is due to the plugin not properly validating a user's identity prior to updating their details like password. This makes it possible for unauthenticated attackers to change arbitrary user's passwords, including administrators, and leverage that to g...

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-620

Tecnología: No especificado

Publicado el: 2025-04-24

CVE-2025-3604

Descripción: The Flynax Bridge plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 2.2.0. This is due to the plugin not properly validating a user's identity prior to updating their details like email. This makes it possible for unauthenticated attackers to change arbitrary user's email addresses, including administrators, and leverage that t...

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: 2025-04-24

CVE-2025-2470

Descripción: The Service Finder Bookings plugin for WordPress, used by the Service Finder - Directory and Job Board WordPress Theme, is vulnerable to privilege escalation in all versions up to, and including, 5.1. This is due to a lack of restriction on user role in the 'nsl_registration_store_extra_input' function. This makes it possible for unauthenticated attackers to register an account on the site with...

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-266

Tecnología: No especificado

Publicado el: 2025-04-25

Resumen del Reporte

CVEs analizados: 6

Promedio CVSS: 8.93

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat □