CVEs más relevantes de la semana

Del 29/07/2025 al 05/08/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-5954

Descripción: The Service Finder SMS System plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 2.0.0. This is due to the plugin not restricting user role selection at the time of registration through the aonesms_fn_savedata_after_signup() function. This makes it possible for unauthenticated attackers to register as an administrator 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-269

Tecnología: No especificado

Publicado el: 2025-08-01

CVE-2025-5947

Descripción: The Service Finder Bookings plugin for WordPress is vulnerable to privilege escalation via authentication bypass in all versions up to, and including, 6.0. This is due to the plugin not properly validating a user's cookie value prior to logging them in through the service_finder_switch_back() function. This makes it possible for unauthenticated attackers to login as any user including admins.

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-639

Tecnología: No especificado

Publicado el: 2025-08-01

CVE-2025-7710

Descripción: The Brave Conversion Engine (PRO) plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 0.7.7. This is due to the plugin not properly restricting a claimed identity while authenticating with Facebook. This makes it possible for unauthenticated attackers to log in as other users, including administrators.

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: 2025-08-02

CVE-2025-8497

Descripción: A vulnerability was found in code-projects Online Medicine Guide 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /cusfindphar2.php. The manipulation of the argument Search leads to sql injection. The attack may be launched 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: 2025-08-03

CVE-2025-8498

Descripción: A vulnerability was found in code-projects Online Medicine Guide 1.0. It has been classified as critical. This affects an unknown part of the file /cart/index.php. The manipulation of the argument uname leads to sql injection. It is possible to initiate the attack 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: 2025-08-03

CVE-2025-8499

Descripción: A vulnerability was found in code-projects Online Medicine Guide 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /cusfindambulence2.php. The manipulation of the argument Search 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: 2025-08-03

CVE-2025-8502

Descripción: A vulnerability classified as critical was found in code-projects Online Medicine Guide 1.0. Affected by this vulnerability is an unknown functionality of the file /changepass.php. The manipulation of the argument ups leads to sql injection. The attack can be launched 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: 2025-08-03

CVE-2025-8503

Descripción: A vulnerability, which was classified as critical, has been found in code-projects Online Medicine Guide 1.0. Affected by this issue is some unknown functionality of the file /adaddmed.php. The manipulation of the argument mname leads to sql injection. The attack may be launched 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: 2025-08-03

Resumen del Reporte

CVEs analizados: 8

Promedio CVSS: 8.24

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat