CVEs más relevantes de la semana

Del 02/08/2025 al 09/08/2025

Porque el primer paso para defender es conocer las amenazas.

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-2025-8468

Descripción: A vulnerability was found in code-projects Wazifa System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /controllers/reset.php. The manipulation of the argument email 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: 2025-08-02

CVE-2025-8469

Descripción: A vulnerability classified as critical has been found in SourceCodester Online Hotel Reservation System 1.0. This affects an unknown part of the file /admin/deletegallery.php. The manipulation of the argument ID 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: 2025-08-02

CVE-2025-8470

Descripción: A vulnerability classified as critical was found in SourceCodester Online Hotel Reservation System 1.0. This vulnerability affects unknown code of the file /admin/deleteroom.php. The manipulation of the argument ID 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: 2025-08-02

CVE-2025-8471

Descripción: A vulnerability, which was classified as critical, has been found in projectworlds Online Admission System 1.0. This issue affects some unknown processing of the file /adminlogin.php. The manipulation of the argument a_id leads to sql injection. The attack may 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: 2025-08-02

CVE-2025-8493

Descripción: A vulnerability classified as critical was found in code-projects Intern Membership Management System 1.0. This vulnerability affects unknown code of the file /admin/edit_student_query.php. The manipulation of the argument ID 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: 2025-08-02

CVE-2025-8494

Descripción: A vulnerability, which was classified as critical, has been found in code-projects Intern Membership Management System 1.0. This issue affects some unknown processing of the file /admin/delete_student.php. The manipulation of the argument ID leads to sql injection. The attack may 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-2025-54349

Descripción: In iperf before 3.19.1, iperf_auth.c has an off-by-one error and resultant heap-based buffer overflow.

CVSS: 6.5 (MEDIUM)

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

Tipo: CWE-193

Tecnología: No especificado

Publicado el: 2025-08-03

CVE-2025-54351

Descripción: In iperf before 3.19.1, net.c has a buffer overflow when --skip-rx-copy is used (for MSG_TRUNC in recv).

CVSS: 8.9 (HIGH)

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

Tipo: CWE-420

Tecnología: No especificado

Publicado el: 2025-08-03

CVE-2025-8495

Descripción: A vulnerability, which was classified as critical, was found in code-projects Intern Membership Management System 1.0. Affected is an unknown function of the file /admin/edit_admin_query.php. The manipulation of the argument Username leads to sql injection. It is possible to launch 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-2025-8496

Descripción: A vulnerability has been found in projectworlds Online Admission System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /viewform.php. The manipulation of the argument ID 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-2025-8497

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

CVE-2025-8504

Descripción: A vulnerability, which was classified as critical, was found in code-projects Kitchen Treasure 1.0. This affects an unknown part of the file /userregistration.php. The manipulation of the argument photo leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.

CVSS: 6.3 (MEDIUM)

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

Tipo: CWE-284

Tecnología: No especificado

Publicado el: 2025-08-03

CVE-2025-44954

Descripción: RUCKUS SmartZone (SZ) before 6.1.2p3 Refresh Build has a hardcoded SSH private key for a root-equivalent user account.

CVSS: 9.0 (CRITICAL)

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

Tipo: CWE-1394

Tecnología: No especificado

Publicado el: 2025-08-04

CVE-2025-6994

Descripción: The Reveal Listing plugin by smartdatasoft for WordPress is vulnerable to privilege escalation in versions up to, and including, 3.3. This is due to the plugin allowing users who are registering new accounts to set their own role or by supplying 'listing_user_role' field. This makes it possible for unauthenticated attackers to gain elevated privileges by creating an account with the administrat...

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: 2025-08-06

CVE-2025-53767

Descripción: Azure OpenAI Elevation of Privilege Vulnerability

CVSS: 10.0 (CRITICAL)

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

Tipo: CWE-918

Tecnología: No especificado

Publicado el: 2025-08-07

CVE-2025-53792

Descripción: Azure Portal Elevation of Privilege Vulnerability

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-285

Tecnología: No especificado

Publicado el: 2025-08-07

CVE-2025-8730

Descripción: A vulnerability was found in Belkin F9K1009 and F9K1010 2.00.04/2.00.09 and classified as critical. Affected by this issue is some unknown functionality of the component Web Interface. The manipulation leads to hard-coded credentials. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did no...

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-259

Tecnología: No especificado

Publicado el: 2025-08-08

CVE-2025-8731

Descripción: A vulnerability was found in TRENDnet TI-G160i, TI-PG102i and TPL-430AP up to 20250724. It has been classified as critical. This affects an unknown part of the component SSH Service. The manipulation leads to use of default credentials. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosu...

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-1392

Tecnología: No especificado

Publicado el: 2025-08-08

Resumen del Reporte

CVEs analizados: 23

Promedio CVSS: 8.00

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat