CVEs más relevantes de la semana

Del 27/05/2025 al 03/06/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-5298

Descripción: A vulnerability, which was classified as critical, was found in Campcodes Online Hospital Management System 1.0. Affected is an unknown function of the file /admin/betweendates-detailsreports.php. The manipulation of the argument fromdate/todate 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: 2025-05-28

CVE-2025-3357

Descripción: IBM Tivoli Monitoring 6.3.0.7 through 6.3.0.7 Service Pack 19 could allow a remote attacker to execute arbitrary code due to improper validation of an index value of a dynamically allocated array.

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-1285

Tecnología: No especificado

Publicado el: 2025-05-28

CVE-2025-4967

Descripción: Esri Portal for ArcGIS 11.4 and prior allows a remote, unauthenticated attacker to bypass the Portal's SSRF protections.

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-918

Tecnología: No especificado

Publicado el: 2025-05-29

CVE-2025-5360

Descripción: A vulnerability classified as critical was found in Campcodes Online Hospital Management System 1.0. This vulnerability affects unknown code of the file /book-appointment.php. The manipulation of the argument doctor 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: 2025-05-30

CVE-2025-5361

Descripción: A vulnerability, which was classified as critical, has been found in Campcodes Online Hospital Management System 1.0. This issue affects some unknown processing of the file /contact.php. The manipulation of the argument fullname 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: 2025-05-30

CVE-2025-5362

Descripción: A vulnerability, which was classified as critical, was found in Campcodes Online Hospital Management System 1.0. Affected is an unknown function of the file /admin/doctor-specilization.php. The manipulation of the argument doctorspecilization 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: 2025-05-30

CVE-2025-5363

Descripción: A vulnerability has been found in Campcodes Online Hospital Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /doctor/index.php. The manipulation of the argument Username 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: 2025-05-30

CVE-2025-5364

Descripción: A vulnerability was found in Campcodes Online Hospital Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /doctor/add-patient.php. The manipulation of the argument patname 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: 2025-05-30

CVE-2025-5365

Descripción: A vulnerability was found in Campcodes Online Hospital Management System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/patient-search.php. The manipulation of the argument searchdata 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: 2025-05-31

CVE-2025-5367

Descripción: A vulnerability was found in PHPGurukul Online Shopping Portal Project 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /category.php. The manipulation of the argument Product 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: 2025-05-31

CVE-2025-4607

Descripción: The PSW Front-end Login & Registration plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.12 via the customer_registration() function. This is due to the use of a weak, low-entropy OTP mechanism in the forget() function. This makes it possible for unauthenticated attackers to initiate a password reset for any user, including administrators, and el...

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-330

Tecnología: No especificado

Publicado el: 2025-05-31

CVE-2025-4631

Descripción: The Profitori plugin for WordPress is vulnerable to Privilege Escalation due to a missing capability check on the stocktend_object endpoint in versions 2.0.6.0 to 2.1.1.3. This makes it possible to trigger the save_object_as_user() function for objects whose '_datatype' is set to 'users',. This allows unauthenticated attackers to write arbitrary strings straight into the user's wp_capabilities ...

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-285

Tecnología: No especificado

Publicado el: 2025-05-31

CVE-2025-5408

Descripción: A vulnerability was found in WAVLINK QUANTUM D2G, QUANTUM D3G, WL-WN530G3A, WL-WN530HG3, WL-WN532A3 and WL-WN576K up to V1410_240222 and classified as critical. Affected by this issue is the function sys_login of the file /cgi-bin/login.cgi of the component HTTP POST Request Handler. The manipulation of the argument login_page leads to buffer overflow. The attack may be launched remotely. The ...

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-119

Tecnología: No especificado

Publicado el: 2025-06-01

CVE-2025-4797

Descripción: The Golo - City Travel Guide WordPress Theme theme for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 1.7.0. This is due to the plugin not properly validating a user's identity prior to setting an authorization cookie. This makes it possible for unauthenticated attackers to log in as any user, including administrators, provided they kn...

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: 2025-06-03

CVE-2025-25022

Descripción: IBM QRadar Suite Software 1.10.12.0 through 1.11.2.0 and IBM Cloud Pak for Security 1.10.0.0 through 1.10.11.0 could allow an unauthenticated user in the environment to obtain highly sensitive information in configuration files.

CVSS: 9.6 (CRITICAL)

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

Tipo: CWE-260

Tecnología: No especificado

Publicado el: 2025-06-03

Resumen del Reporte

CVEs analizados: 15

Promedio CVSS: 8.41

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat □