CVEs más relevantes de la semana

Del 24/05/2025 al 31/05/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-5224

Descripción: A vulnerability classified as critical has been found in Campcodes Online Hospital Management System 1.0. Affected is an unknown function of the file /admin/add-doctor.php. The manipulation of the argument Doctorspecialization 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: 2025-05-27

CVE-2025-5225

Descripción: A vulnerability, which was classified as critical, was found in Campcodes Advanced Online Voting System 1.0. This affects an unknown part of the file /index.php. The manipulation of the argument voter 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: 2025-05-27

CVE-2025-5229

Descripción: A vulnerability was found in Campcodes Online Hospital Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/view-patient.php. The manipulation of the argument viewid 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: 2025-05-27

CVE-2025-41651

Descripción: Due to missing authentication on a critical function of the devices an unauthenticated remote attacker can execute arbitrary commands, potentially enabling unauthorized upload or download of configuration files and leading to full system compromise.

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-306

Tecnología: No especificado

Publicado el: 2025-05-27

CVE-2025-41652

Descripción: The devices are vulnerable to an authentication bypass due to flaws in the authorization mechanism. An unauthenticated remote attacker could exploit this weakness by performing brute-force attacks to guess valid credentials or by using MD5 collision techniques to forge authentication hashes, potentially compromising the device.

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-656

Tecnología: No especificado

Publicado el: 2025-05-27

CVE-2025-5246

Descripción: A vulnerability classified as critical was found in Campcodes Online Hospital Management System 1.0. This vulnerability affects unknown code of the file /hms/admin/query-details.php. The manipulation of the argument adminremark 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: 2025-05-27

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-2025-4607

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

Resumen del Reporte

CVEs analizados: 11

Promedio CVSS: 8.60

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat