CVEs más relevantes de la semana

Del 28/06/2025 al 05/07/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-6819

Descripción: A vulnerability has been found in code-projects Inventory Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /php_action/removeBrand.php. The manipulation of the argument brandId 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: 2025-06-28

CVE-2025-6820

Descripción: A vulnerability was found in code-projects Inventory Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /php_action/createProduct.php. The manipulation of the argument productName 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: 2025-06-28

CVE-2025-6821

Descripción: A vulnerability was found in code-projects Inventory Management System 1.0. It has been classified as critical. This affects an unknown part of the file /php_action/createOrder.php. The manipulation 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: 2025-06-28

CVE-2025-6822

Descripción: A vulnerability was found in code-projects Inventory Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /php_action/removeProduct.php. The manipulation of the argument productId 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: 2025-06-28

CVE-2025-6823

Descripción: A vulnerability was found in code-projects Inventory Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /php_action/editProduct.php. The manipulation of the argument editProductName 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: 2025-06-28

CVE-2025-6827

Descripción: A vulnerability, which was classified as critical, was found in code-projects Inventory Management System 1.0. This affects an unknown part of the file /php_action/editOrder.php. The manipulation 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: 2025-06-28

CVE-2025-6828

Descripción: A vulnerability has been found in code-projects Inventory Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /orders.php. The manipulation of the argument i 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: 2025-06-28

CVE-2025-6834

Descripción: A vulnerability was found in code-projects Inventory Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /php_action/editPayment.php. The manipulation of the argument orderId 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: 2025-06-29

CVE-2025-6835

Descripción: A vulnerability was found in code-projects Library System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /student-issue-book.php. The manipulation of the argument reg 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: 2025-06-29

CVE-2025-6836

Descripción: A vulnerability classified as critical has been found in code-projects Library System 1.0. Affected is an unknown function of the file /profile.php. The manipulation of the argument phone leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.

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: 2025-06-29

CVE-2025-6837

Descripción: A vulnerability classified as critical was found in code-projects Library System 1.0. Affected by this vulnerability is an unknown functionality of the file /profile.php. The manipulation of the argument image leads to unrestricted upload. The attack can be launched 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: 2025-06-29

CVE-2025-6840

Descripción: A vulnerability, which was classified as critical, was found in code-projects Product Inventory System 1.0. This affects an unknown part of the file /index.php of the component Login. The manipulation of the argument Username 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: 2025-06-29

CVE-2025-6844

Descripción: A vulnerability was found in code-projects Simple Forum 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /signin.php. The manipulation of the argument User 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: 2025-06-29

CVE-2025-6845

Descripción: A vulnerability was found in code-projects Simple Forum 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /register1.php. The manipulation of the argument User 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: 2025-06-29

CVE-2025-6847

Descripción: A vulnerability classified as critical was found in code-projects Simple Forum 1.0. This vulnerability affects unknown code of the file /forum_edit.php. The manipulation of the argument iii leads to sql injection. The attack can be initiated 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-74

Tecnología: No especificado

Publicado el: 2025-06-29

CVE-2025-6863

Descripción: A vulnerability classified as critical was found in PHPGurukul Local Services Search Engine Management System 2.1. Affected by this vulnerability is an unknown functionality of the file /admin/edit-category-detail.php. The manipulation of the argument editid 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: 2025-06-29

CVE-2025-6871

Descripción: A vulnerability classified as critical has been found in SourceCodester Simple Company Website 1.0. This affects an unknown part of the file /classes/Login.php. The manipulation of the argument Username 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: 2025-06-29

CVE-2025-53074

Descripción: Out-of-bounds Read vulnerability in Samsung Open Source rLottie allows Overflow Buffers.This issue affects rLottie: V0.2.

CVSS: 9.1 (CRITICAL)

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

Tipo: CWE-125

Tecnología: No especificado

Publicado el: 2025-06-30

CVE-2025-53076

Descripción: Improper Input Validation vulnerability in Samsung Open Source rLottie allows Overread Buffers.This issue affects rLottie: V0.2.

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-20

Tecnología: No especificado

Publicado el: 2025-06-30

CVE-2025-6897

Descripción: A vulnerability classified as critical was found in D-Link DI-7300G+ 19.12.25A1. Affected by this vulnerability is an unknown functionality of the file httpd_debug.asp. The manipulation of the argument Time leads to os command injection. The exploit has been disclosed to the public and may be used.

CVSS: 5.5 (MEDIUM)

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

Tipo: CWE-77

Tecnología: No especificado

Publicado el: 2025-06-30

CVE-2025-6900

Descripción: A vulnerability has been found in code-projects Library System 1.0 and classified as critical. This vulnerability affects unknown code of the file /add-book.php. The manipulation of the argument image leads to unrestricted upload. The attack can be initiated 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: 2025-06-30

CVE-2025-6906

Descripción: A vulnerability classified as critical has been found in code-projects Car Rental System 1.0. This affects an unknown part of the file /login.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: 2025-06-30

CVE-2025-6907

Descripción: A vulnerability classified as critical was found in code-projects Car Rental System 1.0. This vulnerability affects unknown code of the file /book_car.php. The manipulation of the argument fname 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: 2025-06-30

CVE-2025-6934

Descripción: The Opal Estate Pro – Property Management and Submission plugin for WordPress, used by the FullHouse - Real Estate Responsive WordPress Theme, is vulnerable to privilege escalation via in all versions up to, and including, 1.7.5. This is due to a lack of role restriction during registration in the 'on_regiser_user' function. This makes it possible for unauthenticated attackers to arbitrarily ch...

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: 2025-07-01

CVE-2025-41648

Descripción: An unauthenticated remote attacker can bypass the login to the web application of the affected devices making it possible to access and change all available settings of the IndustrialPI.

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-704

Tecnología: No especificado

Publicado el: 2025-07-01

CVE-2025-41656

Descripción: An unauthenticated remote attacker can run arbitrary commands on the affected devices with high privileges because the authentication for the Node_RED server is not configured by default.

CVSS: 10.0 (CRITICAL)

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

Tipo: CWE-306

Tecnología: No especificado

Publicado el: 2025-07-01

CVE-2025-4689

Descripción: The Ads Pro Plugin - Multi-Purpose WordPress Advertising Manager plugin for WordPress is vulnerable to Local File Inclusion which leads to Remote Code Execution in all versions up to, and including, 4.89. This is due to the presence of a SQL Injection vulnerability and Local File Inclusion vulnerability that can be chained with an image upload. This makes it possible for unauthenticated attacke...

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-98

Tecnología: No especificado

Publicado el: 2025-07-02

CVE-2025-5746

Descripción: The Drag and Drop Multiple File Upload (Pro) - WooCommerce plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the dnd_upload_cf7_upload_chunks() function in version 5.0 - 5.0.5 (when bundled with the PrintSpace theme) and all versions up to, and including, 1.7.1 (in the standalone version). This makes it possible for unauthenticated attackers to ...

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-434

Tecnología: No especificado

Publicado el: 2025-07-02

CVE-2024-13786

Descripción: The education theme for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.6.10 via deserialization of untrusted input in the 'themerex_callback_view_more_posts' function. This makes it possible for unauthenticated attackers to inject a PHP Object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless a...

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-502

Tecnología: No especificado

Publicado el: 2025-07-02

Resumen del Reporte

CVEs analizados: 29

Promedio CVSS: 7.81

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat