CVEs más relevantes de la semana

Del 24/06/2025 al 01/07/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-4378

Descripción: Cleartext Transmission of Sensitive Information, Use of Hard-coded Credentials vulnerability in Ataturk University ATA-AOF Mobile Application allows Authentication Abuse, Authentication Bypass.This issue affects ATA-AOF Mobile Application: before 20.06.2025.

CVSS: 10.0 (CRITICAL)

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

Tipo: CWE-319

Tecnología: No especificado

Publicado el: 2025-06-24

CVE-2025-20281

Descripción: A vulnerability in a specific API of Cisco ISE and Cisco ISE-PIC could allow an unauthenticated, remote attacker to execute arbitrary code on the underlying operating system as root. The attacker does not require any valid credentials to exploit this vulnerability. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sub...

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-74

Tecnología: No especificado

Publicado el: 2025-06-25

CVE-2025-6611

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/createBrand.php. The manipulation of the argument brandStatus 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: 2025-06-25

CVE-2025-6612

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/removeCategories.php. The manipulation of the argument categoriesId 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: 2025-06-25

CVE-2025-20282

Descripción: A vulnerability in an internal API of Cisco ISE and Cisco ISE-PIC could allow an unauthenticated, remote attacker to upload arbitrary files to an affected device and then execute those files on the underlying operating system as root.   This vulnerability is due a lack of file validation checks that would prevent uploaded files from being placed in privileged directories on an affected system....

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-269

Tecnología: No especificado

Publicado el: 2025-06-25

CVE-2025-6618

Descripción: A vulnerability was found in TOTOLINK CA300-PoE 6.2c.884. It has been classified as critical. Affected is the function SetWLanApcliSettings of the file wps.so. The manipulation of the argument PIN leads to os command injection. It is possible to launch 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-77

Tecnología: No especificado

Publicado el: 2025-06-25

CVE-2025-6619

Descripción: A vulnerability was found in TOTOLINK CA300-PoE 6.2c.884. It has been declared as critical. Affected by this vulnerability is the function setUpgradeFW of the file upgrade.so. The manipulation of the argument FileName leads to os command injection. 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-77

Tecnología: No especificado

Publicado el: 2025-06-25

CVE-2025-6620

Descripción: A vulnerability was found in TOTOLINK CA300-PoE 6.2c.884. It has been rated as critical. Affected by this issue is the function setUpgradeUboot of the file upgrade.so. The manipulation of the argument FileName leads to os command injection. The attack may 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-77

Tecnología: No especificado

Publicado el: 2025-06-25

CVE-2025-6621

Descripción: A vulnerability classified as critical has been found in TOTOLINK CA300-PoE 6.2c.884. This affects the function QuickSetting of the file ap.so. The manipulation of the argument hour/minute leads to os command injection. 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-77

Tecnología: No especificado

Publicado el: 2025-06-25

CVE-2025-36038

Descripción: IBM WebSphere Application Server 8.5 and 9.0 could allow a remote attacker to execute arbitrary code on the system with a specially crafted sequence of serialized objects.

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-502

Tecnología: No especificado

Publicado el: 2025-06-25

CVE-2025-6665

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/editBrand.php. The manipulation of the argument editBrandStatus 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: 2025-06-25

CVE-2025-6668

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/fetchSelectedBrand.php. The manipulation of the argument brandId 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: 2025-06-25

CVE-2025-4334

Descripción: The Simple User Registration plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 6.3. This is due to insufficient restrictions on user meta values that can be supplied during registration. This makes it possible for unauthenticated attackers to register as an administrator.

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: 2025-06-26

CVE-2025-6561

Descripción: Certain hybrid DVR models ((HBF-09KD and HBF-16NK)) from Hunt Electronic have an Exposure of Sensitive Information vulnerability, allowing unauthenticated remote attackers to directly access a system configuration file and obtain plaintext administrator credentials.

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-256

Tecnología: No especificado

Publicado el: 2025-06-26

CVE-2025-6688

Descripción: The Simple Payment plugin for WordPress is vulnerable to Authentication Bypass in versions 1.3.6 to 2.3.8. This is due to the plugin not properly verifying a user's identity prior to logging them in through the create_user() function. This makes it possible for unauthenticated attackers to log in as administrative users.

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: 2025-06-27

CVE-2024-12827

Descripción: The DWT - Directory & Listing WordPress Theme theme for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 3.3.6. This is due to the plugin not properly checking for an empty token value prior to resetting a user's password through the dwt_listing_reset_password() function. This makes it possible for unauthenticated attackers to change arb...

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-620

Tecnología: No especificado

Publicado el: 2025-06-27

CVE-2024-11739

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Case Informatics Case ERP allows SQL Injection.This issue affects Case ERP: before V2.0.1.

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-89

Tecnología: No especificado

Publicado el: 2025-06-27

CVE-2024-12143

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Mobilteg Mobile Informatics Mikro Hand Terminal - MikroDB allows SQL Injection.This issue affects . NOTE: The vendor did not inform about the completion of the fixing process within the specified time. The CVE will be updated when new information becomes available.

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-89

Tecnología: No especificado

Publicado el: 2025-06-27

CVE-2024-12150

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Eron Software Wowwo CRM allows Blind SQL Injection.This issue affects . NOTE: The vendor did not inform about the completion of the fixing process within the specified time. The CVE will be updated when new information becomes available.

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-89

Tecnología: No especificado

Publicado el: 2025-06-27

CVE-2024-12364

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Mavi Ye□il Software Guest Tracking Software allows SQL Injection.This issue affects . NOTE: The vendor did not inform about the completion of the fixing process within the specified time. The CVE will be updated when new information becomes available.

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-89

Tecnología: No especificado

Publicado el: 2025-06-27

CVE-2025-5304

Descripción: The PT Project Notebooks plugin for WordPress is vulnerable to Privilege Escalation due to missing authorization in the wpnb_pto_new_users_add() function in versions 1.0.0 through 1.1.3. This makes it possible for unauthenticated attackers to elevate their privileges to that of an administrator.

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-862

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-2025-6835

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-2025-6840

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-2025-6900

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

Resumen del Reporte

CVEs analizados: 36

Promedio CVSS: 8.24

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat ▯