CVEs más relevantes de la semana

Del 31/05/2025 al 07/06/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-5408

Descripción: A vulnerability was found in WAVLINK QUANTUM D2G, QUANTUM D3G, WL-WN530G3A, WL-WN530HG3, WL-WN532A3 and WL-WN576 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-2025-5502

Descripción: A vulnerability, which was classified as critical, has been found in TOTOLINK X15 1.0.0-B20230714.1105. Affected by this issue is the function formMapReboot of the file /boafrm/formMapReboot. The manipulation of the argument deviceMacAddr leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early ...

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: 2025-06-03

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

CVE-2025-49001

Descripción: DataEase is an open source business intelligence and data visualization tool. Prior to version 2.10.10, secret verification does not take effect successfully, so a user can use any secret to forge a JWT token. The vulnerability has been fixed in v2.10.10. No known workarounds are 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-287

Tecnología: No especificado

Publicado el: 2025-06-03

CVE-2025-49002

Descripción: DataEase is an open source business intelligence and data visualization tool. Versions prior to version 2.10.10 have a flaw in the patch for CVE-2025-32966 that allow the patch to be bypassed through case insensitivity because INIT and RUNSCRIPT are prohibited. The vulnerability has been fixed in v2.10.10. No known workarounds are 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-290

Tecnología: No especificado

Publicado el: 2025-06-03

CVE-2025-5573

Descripción: A vulnerability was found in D-Link DCS-932L 2.18.01. It has been rated as critical. Affected by this issue is the function setSystemWizard/setSystemControl of the file /setSystemWizard. The manipulation of the argument AdminID leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects product...

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: 2025-06-04

CVE-2025-5575

Descripción: A vulnerability classified as critical was found in PHPGurukul Dairy Farm Shop Management System 1.3. This vulnerability affects unknown code of the file /add-product.php. The manipulation of the argument productname 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: 2025-06-04

CVE-2025-5576

Descripción: A vulnerability, which was classified as critical, has been found in PHPGurukul Dairy Farm Shop Management System 1.3. This issue affects some unknown processing of the file /bwdate-report-details.php. The manipulation of the argument fromdate/todate 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: 2025-06-04

CVE-2025-5577

Descripción: A vulnerability, which was classified as critical, was found in PHPGurukul Dairy Farm Shop Management System 1.3. Affected is an unknown function of the file /profile.php. The manipulation of the argument mobilenumber 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: 2025-06-04

CVE-2025-5578

Descripción: A vulnerability has been found in PHPGurukul Dairy Farm Shop Management System 1.3 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /sales-report-details.php. The manipulation of the argument fromdate/todate 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: 2025-06-04

CVE-2025-5579

Descripción: A vulnerability was found in PHPGurukul Dairy Farm Shop Management System 1.3 and classified as critical. Affected by this issue is some unknown functionality of the file /search-product.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: 2025-06-04

CVE-2025-5580

Descripción: A vulnerability was found in CodeAstro Real Estate Management System 1.0. It has been classified as critical. This affects an unknown part of the file /login.php. The manipulation of the argument email 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: 2025-06-04

CVE-2025-5581

Descripción: A vulnerability was found in CodeAstro Real Estate Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/index.php. The manipulation of the argument User 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: 2025-06-04

CVE-2025-5582

Descripción: A vulnerability was found in CodeAstro Real Estate Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /profile.php. The manipulation of the argument content leads to sql injection. The attack may 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: 2025-06-04

CVE-2025-5583

Descripción: A vulnerability classified as critical has been found in CodeAstro Real Estate Management System 1.0. Affected is an unknown function of the file /register.php. The manipulation 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: 2025-06-04

CVE-2025-5612

Descripción: A vulnerability has been found in PHPGurukul Online Fire Reporting System 1.2 and classified as critical. This vulnerability affects unknown code of the file /reporting.php. The manipulation of the argument fullname leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.

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: 2025-06-04

CVE-2025-5613

Descripción: A vulnerability was found in PHPGurukul Online Fire Reporting System 1.2 and classified as critical. This issue affects some unknown processing of the file /request-details.php. The manipulation of the argument requestid leads to sql injection. The attack may 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: 2025-06-04

CVE-2025-5617

Descripción: A vulnerability classified as critical has been found in PHPGurukul Online Fire Reporting System 1.2. This affects an unknown part of the file /admin/manage-teams.php. The manipulation of the argument teamid 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: 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: 2025-06-04

CVE-2025-5618

Descripción: A vulnerability classified as critical was found in PHPGurukul Online Fire Reporting System 1.2. This vulnerability affects unknown code of the file /admin/edit-team.php. The manipulation of the argument teamid 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: 2025-06-04

CVE-2025-5619

Descripción: A vulnerability, which was classified as critical, has been found in Tenda CH22 1.0.0.1. This issue affects the function formaddUserName of the file /goform/addUserName. The manipulation of the argument Password leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.

CVSS: 8.8 (HIGH)

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

Tipo: CWE-119

Tecnología: No especificado

Publicado el: 2025-06-04

CVE-2025-5620

Descripción: A vulnerability, which was classified as critical, was found in D-Link DIR-816 1.10CNB05. Affected is the function setipsec_config of the file /goform/setipsec_config. The manipulation of the argument localIP/remoteIP 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. This vulnerability only affects products...

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-77

Tecnología: No especificado

Publicado el: 2025-06-05

CVE-2025-5621

Descripción: A vulnerability has been found in D-Link DIR-816 1.10CNB05 and classified as critical. Affected by this vulnerability is the function qosClassifier of the file /goform/qosClassifier. The manipulation of the argument dip_address/sip_address leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This vulnerability only aff...

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-77

Tecnología: No especificado

Publicado el: 2025-06-05

CVE-2025-5625

Descripción: A vulnerability was found in Campcodes Online Teacher Record Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /search-teacher.php. The manipulation of the argument searchteacher 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: 2025-06-05

CVE-2025-5626

Descripción: A vulnerability classified as critical has been found in Campcodes Online Teacher Record Management System 1.0. Affected is an unknown function of the file /admin/edit-subjects-detail.php. The manipulation of the argument editid 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: 2025-06-05

CVE-2025-5629

Descripción: A vulnerability, which was classified as critical, was found in Tenda AC10 up to 15.03.06.47. This affects the function formSetPPTPServer of the file /goform/SetPptpServerCfg of the component HTTP Handler. The manipulation of the argument startIp/endIp leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.

CVSS: 8.8 (HIGH)

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

Tipo: CWE-119

Tecnología: No especificado

Publicado el: 2025-06-05

CVE-2025-5639

Descripción: A vulnerability was found in PHPGurukul Notice Board System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /forgot-password.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: 2025-06-05

CVE-2025-5701

Descripción: The HyperComments plugin for WordPress is vulnerable to unauthorized modification of data that can lead to privilege escalation due to a missing capability check on the hc_request_handler function in all versions up to, and including, 1.2.2. This makes it possible for unauthenticated attackers to update arbitrary options on the WordPress site. This can be leveraged to update the default role fo...

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: 2025-06-05

CVE-2025-5663

Descripción: A vulnerability has been found in PHPGurukul Auto Taxi Stand Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/search-autoortaxi.php. The manipulation of the argument searchdata 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: 2025-06-05

CVE-2025-47966

Descripción: Exposure of sensitive information to an unauthorized actor in Power Automate allows an unauthorized attacker to elevate privileges over a network.

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-200

Tecnología: No especificado

Publicado el: 2025-06-05

CVE-2025-5486

Descripción: The WP Email Debug plugin for WordPress is vulnerable to privilege escalation due to a missing capability check on the WPMDBUG_handle_settings() function in versions 1.0 to 1.1.0. This makes it possible for unauthenticated attackers to enable debugging and send all emails to an attacker controlled address and then trigger a password reset for an administrator to gain access to 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: 2025-06-06

CVE-2025-41646

Descripción: An unauthorized remote attacker can bypass the authentication of the affected software package by misusing an incorrect type conversion. This leads to full compromise of 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-704

Tecnología: No especificado

Publicado el: 2025-06-06

Resumen del Reporte

CVEs analizados: 32

Promedio CVSS: 7.87

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat