CVEs más relevantes de la semana

Del 03/06/2025 al 10/06/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-5510

Descripción: A vulnerability classified as critical was found in quequnlong shiyi-blog up to 1.2.1. This vulnerability affects unknown code of the file /app/sys/article/optimize. The manipulation of the argument url leads to server-side request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but...

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-918

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-2025-5553

Descripción: A vulnerability classified as critical was found in PHPGurukul Rail Pass Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /download-pass.php. The manipulation of the argument searchdata 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-2025-5560

Descripción: A vulnerability was found in PHPGurukul Curfew e-Pass Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /index.php. The manipulation of the argument searchdata 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-2025-5561

Descripción: A vulnerability was found in PHPGurukul Curfew e-Pass Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/view-pass-detail.php. The manipulation of the argument viewid 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-2025-5562

Descripción: A vulnerability was found in PHPGurukul Curfew e-Pass Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/edit-category-detail.php. The manipulation of the argument editid 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-2025-5573

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-2025-5574

Descripción: A vulnerability classified as critical has been found in PHPGurukul Dairy Farm Shop Management System 1.3. This affects an unknown part of the file /add-company.php. The manipulation of the argument companyname 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-2025-5575

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-2025-5592

Descripción: A vulnerability, which was classified as critical, has been found in FreeFloat FTP Server 1.0. Affected by this issue is some unknown functionality of the component PASSIVE Command Handler. The manipulation leads to buffer overflow. 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-119

Tecnología: No especificado

Publicado el: 2025-06-04

CVE-2025-5599

Descripción: A vulnerability classified as critical was found in PHPGurukul Student Result Management System 1.3. This vulnerability affects unknown code of the file /editmyexp.php. The manipulation of the argument emp1ctc 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-2025-5602

Descripción: A vulnerability, which was classified as critical, was found in Campcodes Hospital Management System 1.0. Affected is an unknown function of the file /admin/registration.php. The manipulation of the argument full_name 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-2025-5603

Descripción: A vulnerability has been found in Campcodes Hospital Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /registration.php. The manipulation of the argument full_name/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: 2025-06-04

CVE-2025-5604

Descripción: A vulnerability was found in Campcodes Hospital Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /user-login.php. The manipulation of the argument Username 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-2025-5606

Descripción: A vulnerability was found in Tenda AC18 15.03.05.05. It has been declared as critical. This vulnerability affects the function formSetIptv of the file /goform/SetIPTVCfg. The manipulation of the argument list leads to command 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-2025-5612

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-2025-5631

Descripción: A vulnerability was found in code-projects/anirbandutta9 Content Management System and News-Buzz 1.0. It has been classified as critical. Affected is an unknown function of the file /publicposts.php. The manipulation of the argument post 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-2025-5639

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-2025-5650

Descripción: A vulnerability classified as critical was found in 1000projects Online Notice Board 1.0. This vulnerability affects unknown code of the file /register.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. 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: 2025-06-05

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-2025-5685

Descripción: A vulnerability, which was classified as critical, was found in Tenda CH22 1.0.0.1. This affects the function formNatlimit of the file /goform/Natlimit. The manipulation of the argument page leads to stack-based 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-2025-47966

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-2025-5706

Descripción: A vulnerability was found in PHPGurukul Human Metapneumovirus Testing Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /new-user-testing.php. The manipulation of the argument state leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Other paramete...

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: 2025-06-06

CVE-2025-5707

Descripción: A vulnerability was found in PHPGurukul Human Metapneumovirus Testing Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /registered-user-testing.php. The manipulation of the argument testtype leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Other paramet...

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: 2025-06-06

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-2025-5759

Descripción: A vulnerability classified as critical was found in PHPGurukul Local Services Search Engine Management System 2.1. This vulnerability affects unknown code of the file /admin/edit-person-detail.php?editid=2. The manipulation of the argument editid 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: 2025-06-06

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

CVE-2025-5855

Descripción: A vulnerability, which was classified as critical, was found in Tenda AC6 15.03.05.16. This affects the function formSetRebootTimer of the file /goform/SetRebootTimer. The manipulation of the argument rebootTime leads to stack-based 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: 2025-06-09

CVE-2025-5856

Descripción: A vulnerability has been found in PHPGurukul BP Monitoring Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /registration.php. The manipulation of the argument emailid 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: 2025-06-09

CVE-2025-5860

Descripción: A vulnerability, which was classified as critical, was found in PHPGurukul Maid Hiring Management System 1.0. This affects an unknown part of the file /admin/search-booking-request.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: 2025-06-09

CVE-2025-5861

Descripción: A vulnerability has been found in Tenda AC7 15.03.06.44 and classified as critical. This vulnerability affects the function fromadvsetlanip of the file /goform/AdvSetLanip. The manipulation of the argument lanMask leads to buffer overflow. The attack can 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: 2025-06-09

CVE-2025-5862

Descripción: A vulnerability was found in Tenda AC7 15.03.06.44 and classified as critical. This issue affects the function formSetPPTPUserList of the file /goform/setPptpUserList. The manipulation of the argument list leads to 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: 2025-06-09

CVE-2025-5863

Descripción: A vulnerability was found in Tenda AC5 15.03.06.47. It has been classified as critical. Affected is the function formSetRebootTimer of the file /goform/SetRebootTimer. The manipulation of the argument rebootTime leads to stack-based buffer overflow. It is possible to launch 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: 2025-06-09

CVE-2025-5893

Descripción: Smart Parking Management System from Honding Technology has an Exposure of Sensitive Information vulnerability, allowing unauthenticated remote attackers to access a specific page 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: 2025-06-09

CVE-2025-42989

Descripción: RFC inbound processing does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. On successful exploitation the attacker could critically impact both integrity and availability of the application.

CVSS: 9.6 (CRITICAL)

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

Tipo: CWE-862

Tecnología: No especificado

Publicado el: 2025-06-10

CVE-2025-40585

Descripción: A vulnerability has been identified in Energy Services (All versions with G5DFR). Affected solutions using G5DFR contain default credentials. This could allow an attacker to gain control of G5DFR component and tamper with outputs from the device.

CVSS: 9.9 (CRITICAL)

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

Tipo: CWE-276

Tecnología: No especificado

Publicado el: 2025-06-10

CVE-2025-47110

Descripción: Adobe Commerce versions 2.4.8, 2.4.7-p5, 2.4.6-p10, 2.4.5-p12, 2.4.4-p13 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a high privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.

CVSS: 9.1 (CRITICAL)

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

Tipo: CWE-79

Tecnología: No especificado

Publicado el: 2025-06-10

Resumen del Reporte

CVEs analizados: 56

Promedio CVSS: 7.78

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat