CVEs más relevantes de la semana

Del 03/05/2025 al 10/05/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-4241

Descripción: A vulnerability classified as critical has been found in PHPGurukul Teacher Subject Allocation Management System 1.0. Affected is an unknown function of the file /admin/search.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: 2025-05-03

CVE-2025-4242

Descripción: A vulnerability classified as critical was found in PHPGurukul Online Birth Certificate System 2.0. Affected by this vulnerability is an unknown functionality of the file /admin/between-dates-report.php. The manipulation of the argument fromdate leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be af...

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: 2025-05-03

CVE-2025-4249

Descripción: A vulnerability was found in PHPGurukul e-Diary Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /manage-categories.php. The manipulation of the argument ID 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: 2025-05-04

CVE-2025-4262

Descripción: A vulnerability was found in PHPGurukul Online DJ Booking Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/user-search.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: 2025-05-05

CVE-2025-4263

Descripción: A vulnerability was found in PHPGurukul Online DJ Booking Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/booking-search.php. The manipulation of the argument searchdata 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: 2025-05-05

CVE-2025-4264

Descripción: A vulnerability classified as critical has been found in PHPGurukul Emergency Ambulance Hiring Portal 1.0. Affected is an unknown function of the file /admin/edit-ambulance.php. The manipulation of the argument dconnum 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: 2025-05-05

CVE-2025-4265

Descripción: A vulnerability classified as critical was found in PHPGurukul Emergency Ambulance Hiring Portal 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/contact-us.php. The manipulation of the argument mobnum leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as ...

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: 2025-05-05

CVE-2025-4266

Descripción: A vulnerability, which was classified as critical, has been found in PHPGurukul Notice Board System 1.0. Affected by this issue is some unknown functionality of the file /bwdates-reports-details.php?vid=2. The manipulation of the argument fromdate/tomdate 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: 2025-05-05

CVE-2025-45042

Descripción: Tenda AC9 v15.03.05.14 was discovered to contain a command injection vulnerability via the Telnet function.

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-77

Tecnología: No especificado

Publicado el: 2025-05-05

CVE-2024-57229

Descripción: NETGEAR RAX5 (AX1600 WiFi Router) V1.0.2.26 was discovered to contain a command injection vulnerability via the devname parameter in the reset_wifi function.

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-77

Tecnología: No especificado

Publicado el: 2025-05-05

CVE-2024-57230

Descripción: NETGEAR RAX5 (AX1600 WiFi Router) V1.0.2.26 was discovered to contain a command injection vulnerability via the ifname parameter in the apcli_do_enr_pin_wps function.

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-77

Tecnología: No especificado

Publicado el: 2025-05-05

CVE-2024-57231

Descripción: NETGEAR RAX5 (AX1600 WiFi Router) V1.0.2.26 was discovered to contain a command injection vulnerability via the ifname parameter in the apcli_do_enr_pbc_wps function.

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-77

Tecnología: No especificado

Publicado el: 2025-05-05

CVE-2024-57232

Descripción: NETGEAR RAX5 (AX1600 WiFi Router) V1.0.2.26 was discovered to contain a command injection vulnerability via the ifname parameter in the apcli_wps_gen_pincode function.

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-77

Tecnología: No especificado

Publicado el: 2025-05-05

CVE-2024-57233

Descripción: NETGEAR RAX5 (AX1600 WiFi Router) v1.0.2.26 was discovered to contain a command injection vulnerability via the iface parameter in the vif_disable function.

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-77

Tecnología: No especificado

Publicado el: 2025-05-05

CVE-2024-57234

Descripción: NETGEAR RAX5 (AX1600 WiFi Router) V1.0.2.26 was discovered to contain a command injection vulnerability via the ifname parameter in the apcli_cancel_wps function.

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-77

Tecnología: No especificado

Publicado el: 2025-05-05

CVE-2024-57235

Descripción: NETGEAR RAX5 (AX1600 WiFi Router) V1.0.2.26 was discovered to contain a command injection vulnerability via the iface parameter in the vif_enable function.

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-77

Tecnología: No especificado

Publicado el: 2025-05-05

CVE-2025-1909

Descripción: The BuddyBoss Platform Pro plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 2.7.01. This is due to insufficient verification on the user being supplied during the Apple OAuth authenticate request through the plugin. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have ...

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: 2025-05-05

CVE-2025-4303

Descripción: A vulnerability, which was classified as critical, has been found in PHPGurukul Human Metapneumovirus Testing Management System 1.0. Affected by this issue is some unknown functionality of the file /add-phlebotomist.php. The manipulation of the argument empid 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: 2025-05-06

CVE-2025-4309

Descripción: A vulnerability was found in PHPGurukul Art Gallery Management System 1.1. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/add-art-type.php. The manipulation of the argument arttype 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: 2025-05-06

CVE-2025-4332

Descripción: A vulnerability was found in PHPGurukul Company Visitor Management System 2.0 and classified as critical. Affected by this issue is some unknown functionality of the file /visitor-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: 2025-05-06

CVE-2024-49846

Descripción: Memory corruption while decoding of OTA messages from T3448 IE.

CVSS: 8.2 (HIGH)

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

Tipo: CWE-126

Tecnología: No especificado

Publicado el: 2025-05-06

CVE-2025-4358

Descripción: A vulnerability classified as critical has been found in PHPGurukul Company Visitor Management System 2.0. Affected is an unknown function of the file /admin-profile.php. The manipulation of the argument adminname 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: 2025-05-06

CVE-2024-12225

Descripción: A vulnerability was found in Quarkus in the quarkus-security-webauthn module. The Quarkus WebAuthn module publishes default REST endpoints for registering and logging users in while allowing developers to provide custom REST endpoints. When developers provide custom REST endpoints, the default endpoints remain accessible, potentially allowing attackers to obtain a login cookie that has no corre...

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-288

Tecnología: No especificado

Publicado el: 2025-05-06

CVE-2025-0855

Descripción: The PGS Core plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 5.8.0 via deserialization of untrusted input in the 'import_header' function. This makes it possible for unauthenticated attackers to inject a PHP Object. No known POP chain is present in the vulnerable software. If a POP chain is present via an additional plugin or theme installed on t...

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: 2025-05-06

CVE-2025-3844

Descripción: The PeproDev Ultimate Profile Solutions plugin for WordPress is vulnerable to Authentication Bypass in versions 1.9.1 to 7.5.2. This is due to handel_ajax_req() function not having proper restrictions on the change_user_meta functionality that makes it possible to set a OTP code and subsequently log in with that OTP code. This makes it possible for unauthenticated attackers to login as other us...

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: 2025-05-07

CVE-2025-4104

Descripción: The Frontend Dashboard plugin for WordPress is vulnerable to Privilege Escalation due to a missing capability check on the fed_wp_ajax_fed_login_form_post() function in versions 1.0 to 2.2.6. This makes it possible for unauthenticated attackers to reset the administrator's email and password, and 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-285

Tecnología: No especificado

Publicado el: 2025-05-07

CVE-2025-20188

Descripción: A vulnerability in the Out-of-Band Access Point (AP) Image Download feature of Cisco IOS XE Software for Wireless LAN Controllers (WLCs) could allow an unauthenticated, remote attacker to upload arbitrary files to an affected system.   This vulnerability is due to the presence of a hard-coded JSON Web Token (JWT) on an affected system. An attacker could exploit this vulnerability by sending cr...

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-798

Tecnología: No especificado

Publicado el: 2025-05-07

CVE-2025-29813

Descripción: An elevation of privilege vulnerability exists when Visual Studio improperly handles pipeline job tokens. An attacker who successfully exploited this vulnerability could extend their access to a project. To exploit this vulnerability, an attacker would first have to have access to the project and swap the short-term token for a long-term one. The update addresses the vulnerability by correcting...

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-302

Tecnología: No especificado

Publicado el: 2025-05-08

CVE-2025-29827

Descripción: Improper Authorization in Azure Automation allows an authorized attacker to elevate privileges over a network.

CVSS: 9.9 (CRITICAL)

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

Tipo: CWE-285

Tecnología: No especificado

Publicado el: 2025-05-08

CVE-2025-29972

Descripción: Server-Side Request Forgery (SSRF) in Azure allows an authorized attacker to perform spoofing over a network.

CVSS: 9.9 (CRITICAL)

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

Tipo: CWE-918

Tecnología: No especificado

Publicado el: 2025-05-08

CVE-2025-47733

Descripción: Server-Side Request Forgery (SSRF) in Microsoft Power Apps allows an unauthorized attacker to disclose information over a network

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: 2025-05-08

CVE-2025-3810

Descripción: The WPBookit plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 1.0.2. This is due to the plugin not properly validating a user's identity prior to updating their details like password and email through the edit_profile_data() function. This makes it possible for unauthenticated attackers to change arbitrary user's email address...

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-639

Tecnología: No especificado

Publicado el: 2025-05-09

CVE-2025-3811

Descripción: The WPBookit plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 1.0.2. This is due to the plugin not properly validating a user's identity prior to updating their details like email through the edit_newdata_customer_callback() function. This makes it possible for unauthenticated attackers to change arbitrary user's email address...

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-639

Tecnología: No especificado

Publicado el: 2025-05-09

CVE-2024-11617

Descripción: The Envolve Plugin plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'zetra_languageUpload' and 'zetra_fontsUpload' functions in all versions up to, and including, 1.0. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.

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: 2025-05-09

CVE-2025-2253

Descripción: The IMITHEMES Listing plugin is vulnerable to privilege escalation via account takeover in all versions up to, and including, 3.3. This is due to the plugin not properly validating a verification code value prior to updating their password through the imic_reset_password_init() function. This makes it possible for unauthenticated attackers to change any user's passwords, including 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-620

Tecnología: No especificado

Publicado el: 2025-05-09

CVE-2025-3605

Descripción: The Frontend Login and Registration Blocks plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 1.0.7. This is due to the plugin not properly validating a user's identity prior to updating their details like email via the flr_blocks_user_settings_handle_ajax_callback() function. This makes it possible for unauthenticated attackers...

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-639

Tecnología: No especificado

Publicado el: 2025-05-09

CVE-2025-4403

Descripción: The Drag and Drop Multiple File Upload for WooCommerce plugin for WordPress is vulnerable to arbitrary file uploads in all versions up to, and including, 1.1.6 due to accepting a user-supplied supported_type string and the uploaded filename without enforcing real extension or MIME checks within the upload() function. This makes it possible for unauthenticated attackers to upload arbitrary files...

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: 2025-05-09

Resumen del Reporte

CVEs analizados: 37

Promedio CVSS: 8.92

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat □