CVEs más relevantes de la semana

Del 10/05/2025 al 17/05/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-4502

Descripción: A vulnerability has been found in Campcodes Sales and Inventory System 1.0 and classified as critical. This vulnerability affects unknown code of the file /pages/creditor_add.php. The manipulation 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: 2025-05-10

CVE-2025-4503

Descripción: A vulnerability was found in Campcodes Sales and Inventory System 1.0 and classified as critical. This issue affects some unknown processing of the file /pages/customer_update.php. The manipulation of the argument ID 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: 2025-05-10

CVE-2025-4504

Descripción: A vulnerability was found in SourceCodester Online College Library System 1.0. It has been classified as critical. Affected is an unknown function of the file /index.php. The manipulation of the argument Category 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: 2025-05-10

CVE-2025-4505

Descripción: A vulnerability was found in PHPGurukul Apartment Visitors Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /category.php. The manipulation of the argument categoryname 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: 2025-05-10

CVE-2025-4506

Descripción: A vulnerability was found in Campcodes Online Food Ordering System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /routers/menu-router.php. The manipulation of the argument 1_price 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: 2025-05-10

CVE-2025-4507

Descripción: A vulnerability classified as critical has been found in Campcodes Online Food Ordering System 1.0. This affects an unknown part of the file /routers/add-item.php. The manipulation of the argument price 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: 2025-05-10

CVE-2025-4508

Descripción: A vulnerability classified as critical was found in PHPGurukul e-Diary Management System 1.0. This vulnerability affects unknown code of the file /my-profile.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: 2025-05-10

CVE-2025-4509

Descripción: A vulnerability, which was classified as critical, has been found in PHPGurukul e-Diary Management System 1.0. This issue affects some unknown processing of the file /manage-notes.php. The manipulation of the argument ID 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: 2025-05-10

CVE-2025-4548

Descripción: A vulnerability classified as critical has been found in Campcodes Online Food Ordering System 1.0. This affects an unknown part of the file /routers/router.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: 2025-05-11

CVE-2025-4549

Descripción: A vulnerability classified as critical was found in Campcodes Online Food Ordering System 1.0. This vulnerability affects unknown code of the file /routers/register-router.php. The manipulation of the argument Name 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: 2025-05-11

CVE-2025-4550

Descripción: A vulnerability, which was classified as critical, has been found in PHPGurukul Apartment Visitors Management System 1.0. This issue affects some unknown processing of the file /admin/pass-details.php. The manipulation of the argument pid 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: 2025-05-11

CVE-2025-4553

Descripción: A vulnerability was found in PHPGurukul Apartment Visitors Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/bwdates-reports-details.php. The manipulation of the argument fromdate/todate 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: 2025-05-12

CVE-2025-4554

Descripción: A vulnerability was found in PHPGurukul Apartment Visitors Management System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/bwdates-passreports-details.php. The manipulation of the argument fromdate/todate 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: 2025-05-12

CVE-2025-4555

Descripción: The web management interface of Okcat Parking Management Platform from ZONG YU has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to directly access system functions. These functions include opening gates, viewing license plates and parking records, and restarting the system.

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-306

Tecnología: No especificado

Publicado el: 2025-05-12

CVE-2025-4556

Descripción: The web management interface of Okcat Parking Management Platform from ZONG YU has an Arbitrary File Upload vulnerability, allowing unauthenticated remote attackers to upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.

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: 2025-05-12

CVE-2025-4558

Descripción: The GPM from WormHole Tech has an Unverified Password Change vulnerability, allowing unauthenticated remote attackers to change any user's password and use the modified password to log into the system.

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: 2025-05-12

CVE-2023-49641

Descripción: Billing Software v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'username' parameter of the loginCheck.php resource does not validate the characters received and they are sent unfiltered to the database.

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: 2025-05-13

CVE-2025-26389

Descripción: A vulnerability has been identified in OZW672 (All versions < V8.0), OZW772 (All versions < V8.0). The web service in affected devices does not sanitize the input parameters required for the `exportDiagramPage` endpoint. This could allow an unauthenticated remote attacker to execute arbitrary code with root privileges.

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-78

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-26390

Descripción: A vulnerability has been identified in OZW672 (All versions < V6.0), OZW772 (All versions < V6.0). The web service of affected devices is vulnerable to SQL injection when checking authentication data. This could allow an unauthenticated remote attacker to bypass the check and authenticate as Administrator user.

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: 2025-05-13

CVE-2025-32469

Descripción: A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.5), RUGGEDCOM ROX MX5000RE (All versions < V2.16.5), RUGGEDCOM ROX RX1400 (All versions < V2.16.5), RUGGEDCOM ROX RX1500 (All versions < V2.16.5), RUGGEDCOM ROX RX1501 (All versions < V2.16.5), RUGGEDCOM ROX RX1510 (All versions < V2.16.5), RUGGEDCOM ROX RX1511 (All versions < V2.16.5), RUGGEDCOM ROX RX1512 (All v...

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-602

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-33024

Descripción: A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.5), RUGGEDCOM ROX MX5000RE (All versions < V2.16.5), RUGGEDCOM ROX RX1400 (All versions < V2.16.5), RUGGEDCOM ROX RX1500 (All versions < V2.16.5), RUGGEDCOM ROX RX1501 (All versions < V2.16.5), RUGGEDCOM ROX RX1510 (All versions < V2.16.5), RUGGEDCOM ROX RX1511 (All versions < V2.16.5), RUGGEDCOM ROX RX1512 (All v...

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-602

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-33025

Descripción: A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.5), RUGGEDCOM ROX MX5000RE (All versions < V2.16.5), RUGGEDCOM ROX RX1400 (All versions < V2.16.5), RUGGEDCOM ROX RX1500 (All versions < V2.16.5), RUGGEDCOM ROX RX1501 (All versions < V2.16.5), RUGGEDCOM ROX RX1510 (All versions < V2.16.5), RUGGEDCOM ROX RX1511 (All versions < V2.16.5), RUGGEDCOM ROX RX1512 (All v...

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-602

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-32756

Descripción: A stack-based buffer overflow vulnerability [CWE-121] in Fortinet FortiVoice versions 7.2.0, 7.0.0 through 7.0.6, 6.4.0 through 6.4.10, FortiRecorder versions 7.2.0 through 7.2.3, 7.0.0 through 7.0.5, 6.4.0 through 6.4.5, FortiMail versions 7.6.0 through 7.6.2, 7.4.0 through 7.4.4, 7.2.0 through 7.2.7, 7.0.0 through 7.0.8, FortiNDR versions 7.6.0, 7.4.0 through 7.4.7, 7.2.0 through 7.2.4, 7.0.0...

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-121

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-30387

Descripción: Improper limitation of a pathname to a restricted directory ('path traversal') in Azure 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-22

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-4660

Descripción: A remote code execution vulnerability exists in the Windows agent component of SecureConnector due to improper access controls on a named pipe. The pipe is accessible to the Everyone group and does not restrict remote connections, allowing any network-based attacker to connect without authentication. By interacting with this pipe, an attacker can redirect the agent to communicate with a rogue s...

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-276

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-45746

Descripción: In ZKT ZKBio CVSecurity 6.4.1_R an unauthenticated attacker can craft JWT token using the hardcoded secret to authenticate to the service console.

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-798

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-45861

Descripción: TOTOLINK A3002R v4.0.0-B20230531.1404 was discovered to contain a buffer overflow via the routername parameter in the formDnsv6 interface.

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-120

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-45865

Descripción: TOTOLINK A3002R v4.0.0-B20230531.1404 was discovered to contain a buffer overflow via the dnsaddr parameter in the formDhcpv6s interface.

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-120

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-43559

Descripción: ColdFusion versions 2025.1, 2023.13, 2021.19 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. A high-privileged attacker could leverage this vulnerability to bypass security mechanisms and execute code. Exploitation of this issue does not require user interaction and scope is changed.

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-20

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-43560

Descripción: ColdFusion versions 2025.1, 2023.13, 2021.19 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. A high-privileged attacker could leverage this vulnerability to bypass security mechanisms and execute code. Exploitation of this issue does not require user interaction and scope is changed.

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-20

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-43561

Descripción: ColdFusion versions 2025.1, 2023.13, 2021.19 and earlier are affected by an Incorrect Authorization vulnerability that could result in arbitrary code execution in the context of the current user. A high-privileged attacker could leverage this vulnerability to bypass authentication mechanisms and execute code. Exploitation of this issue does not require user interaction and scope is changed.

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-863

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-43562

Descripción: ColdFusion versions 2025.1, 2023.13, 2021.19 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could result in arbitrary code execution in the context of the current user. A high-privileged attacker could leverage this vulnerability to bypass security mechanisms and execute code. Exploitation of this issu...

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-78

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-43563

Descripción: ColdFusion versions 2025.1, 2023.13, 2021.19 and earlier are affected by an Improper Access Control vulnerability that could result in arbitrary file system read. An attacker could leverage this vulnerability to access or modify sensitive data without proper authorization. Exploitation of this issue does not require user interaction.

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-284

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-43564

Descripción: ColdFusion versions 2025.1, 2023.13, 2021.19 and earlier are affected by an Improper Access Control vulnerability that could result in arbitrary file system read. An attacker could leverage this vulnerability to access or modify sensitive data without proper authorization. Exploitation of this issue does not require user interaction.

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-863

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-43567

Descripción: Adobe Connect versions 12.8 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability that could be abused by an 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. A successful attacker can abuse this to achieve session takeover, increasi...

CVSS: 9.3 (CRITICAL)

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

Tipo: CWE-79

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-3917

Descripción: The □□□□SEO□□(□□□□/□□/Bing/□□□□) plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the download_remote_image_to_media_library function in all versions up to, and including, 2.0.6. 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: 2025-05-15

CVE-2025-4564

Descripción: The TicketBAI Facturas para WooCommerce plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation via the 'delpdf' action in all versions up to, and including, 3.18. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-co...

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-22

Tecnología: No especificado

Publicado el: 2025-05-15

CVE-2025-4389

Descripción: The Crawlomatic Multipage Scraper Post Generator plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the crawlomatic_generate_featured_image() function in all versions up to, and including, 2.6.8.1. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution poss...

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: 2025-05-17

CVE-2025-4391

Descripción: The Echo RSS Feed Post Generator plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the echo_generate_featured_image() function in all versions up to, and including, 5.4.8.1. 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: 2025-05-17

Resumen del Reporte

CVEs analizados: 39

Promedio CVSS: 8.86

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat ▯