

CVEs más relevantes de la semana

Del 16/08/2025 al 23/08/2025

Porque el primer paso para defender es conocer las amenazas.



CVE-2025-9087

Descripción: A vulnerability has been found in Tenda AC20 16.03.08.12. This affects the function `set_qosMib_list` of the file `/goform/SetNetControlList` of the component `SetNetControlList` Endpoint. The manipulation of the argument list 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: 2025-08-16



CVE-2025-9088

Descripción: A vulnerability was found in Tenda AC20 16.03.08.12. This vulnerability affects the function `save_virtualser_data` of the file `/goform/formSetVirtualSer`. The manipulation of the argument list leads to stack-based 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: 2025-08-16



CVE-2025-9089

Descripción: A vulnerability was determined in Tenda AC20 16.03.08.12. This issue affects the function sub_48E628 of the file /goform/SetIpMacBind. The manipulation of the argument list 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: 2025-08-17



CVE-2025-9090

Descripción: A vulnerability was identified in Tenda AC20 16.03.08.12. Affected is the function webFormDefine of the file /goform/telnet of the component Telnet Service. The manipulation leads to 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-74

Tecnología: No especificado

Publicado el: 2025-08-17



CVE-2025-27909

Descripción: IBM Concert Software 1.0.0 through 1.1.0 uses cross-origin resource sharing (CORS) which could allow an attacker to carry out privileged actions as the domain name is not being limited to only trusted domains.

CVSS: 5.4 (MEDIUM)

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

Tipo: CWE-942

Tecnología: No especificado

Publicado el: 2025-08-18



CVE-2025-6758

Descripción: The Real Spaces - WordPress Properties Directory Theme theme for WordPress is vulnerable to privilege escalation via the 'imic_agent_register' function in all versions up to, and including, 3.6. This is due to a lack of restriction in the registration role. This makes it possible for unauthenticated attackers to arbitrarily choose their role, including the Administrator role, during user regist...

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: 2025-08-19



CVE-2025-8723

Descripción: The Cloudflare Image Resizing plugin for WordPress is vulnerable to Remote Code Execution due to missing authentication and insufficient sanitization within its `hook_rest_pre_dispatch()` method in all versions up to, and including, 1.5.6. This makes it possible for unauthenticated attackers to inject arbitrary PHP into the codebase, achieving remote code execution.

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-94

Tecnología: No especificado

Publicado el: 2025-08-19



CVE-2025-9154

Descripción: A flaw has been found in itsourcecode Online Tour and Travel Management System 1.0. This issue affects some unknown processing of the file /user/page-login.php. This manipulation of the argument email causes sql injection. The attack may be initiated remotely. The exploit has been published 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: 2025-08-19



CVE-2025-9155

Descripción: A vulnerability has been found in itsourcecode Online Tour and Travel Management System 1.0. Impacted is an unknown function of the file /user/forget_password.php. Such 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: 2025-08-19



CVE-2025-9156

Descripción: A vulnerability was found in itsourcecode Sports Management System 1.0. The affected element is an unknown function of the file /Admin/sports.php. Performing manipulation of the argument code results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could 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: 2025-08-19



CVE-2025-9187

Descripción: Memory safety bugs present in Firefox 141 and Thunderbird 141. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 142 and Thunderbird < 142.

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: 2025-08-19



CVE-2025-24322

Descripción: An unsafe default authentication vulnerability exists in the Initial Setup Authentication functionality of Tenda AC6 V5.0 V02.03.01.110. A specially crafted network request can lead to arbitrary code execution. An attacker can browse to the device to trigger this vulnerability.

CVSS: 8.1 (HIGH)

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

Tipo: CWE-304

Tecnología: No especificado

Publicado el: 2025-08-20



CVE-2025-27129

Descripción: An authentication bypass vulnerability exists in the HTTP authentication functionality of Tenda AC6 V5.0 V02.03.01.110. A specially crafted HTTP request can lead to arbitrary code execution. An attacker can send packets to trigger this vulnerability.

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: 2025-08-20



CVE-2025-31355

Descripción: A firmware update vulnerability exists in the Firmware Signature Validation functionality of Tenda AC6 V5.0 V02.03.01.110. A specially crafted malicious file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.

CVSS: 7.2 (HIGH)

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

Tipo: CWE-494

Tecnología: No especificado

Publicado el: 2025-08-20



CVE-2025-32010

Descripción: A stack-based buffer overflow vulnerability exists in the Cloud API functionality of Tenda AC6 V5.0 V02.03.01.110. A specially crafted HTTP response can lead to arbitrary code execution. An attacker can send an HTTP response to trigger this vulnerability.

CVSS: 8.1 (HIGH)

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

Tipo: CWE-121

Tecnología: No especificado

Publicado el: 2025-08-20



CVE-2025-8895

Descripción: The WP Webhooks plugin for WordPress is vulnerable to arbitrary file copy due to missing validation of user-supplied input in all versions up to, and including, 3.3.5. This makes it possible for unauthenticated attackers to copy arbitrary files on the affected site's server to arbitrary locations. This can be used to copy the contents of wp-config.php into a text file which can then be accessed...

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: 2025-08-21



CVE-2025-9302

Descripción: A vulnerability was identified in PHPGurukul User Management System 1.0. This vulnerability affects unknown code of the file /signup.php. Such manipulation of the argument emailid leads to sql injection. The attack can be executed remotely. The exploit is publicly available and might 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: 2025-08-21



CVE-2025-9304

Descripción: A weakness has been identified in SourceCodester Online Bank Management System 1.0. Impacted is an unknown function of the file /bank/show.php. Executing manipulation of the argument ID can lead to sql injection. The attack may be performed from a remote location. The exploit has been made available to the public and could be exploited.

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: 2025-08-21



CVE-2025-9305

Descripción: A security vulnerability has been detected in SourceCodester Online Bank Management System 1.0. The affected element is an unknown function of the file /bank/mnotice.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed publicly 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: 2025-08-21



CVE-2025-9307

Descripción: A flaw has been found in PHPGurukul Online Course Registration 3.1. This affects an unknown function of the file /admin/session.php. This manipulation of the argument sesssion causes sql injection. The attack can be initiated remotely. The exploit has been published 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: 2025-08-21



CVE-2025-9311

Descripción: A vulnerability was identified in itsourcecode Apartment Management System 1.0. Affected by this issue is some unknown functionality of the file /fair/addfair.php. The manipulation of the argument ID leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might 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: 2025-08-21



CVE-2025-53763

Descripción: Improper access control in Azure Databricks 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-284

Tecnología: No especificado

Publicado el: 2025-08-21



CVE-2025-53795

Descripción: Improper authorization in Microsoft PC Manager allows an unauthorized attacker to elevate privileges 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-285

Tecnología: No especificado

Publicado el: 2025-08-21



CVE-2025-9254

Descripción: WebITR developed by Uniong has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to log into the system as arbitrary users by exploiting a specific functionality.

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: 2025-08-22



CVE-2025-7642

Descripción: The Simpler Checkout plugin for WordPress is vulnerable to Authentication Bypass in versions 0.7.0 to 1.1.9. This is due to the plugin not properly verifying a user's identity prior to logging them in as an admin through the `simplerwc_woocommerce_order_created()` function. This makes it possible for unauthenticated attackers to log in as other users based on their order ID, which can be an admin...

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: 2025-08-23



CVE-2025-5821

Descripción: The Case Theme User plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 1.0.3. This is due to the plugin not properly logging a user in with the data that was previously verified through the `facebook_ajax_login_callback()`. This makes it possible for unauthenticated attackers to log in as administrative users, as long as they have an existing account...

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: 2025-08-23



Resumen del Reporte

CVEs analizados: 26

Promedio CVSS: 8.35

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat ☺

