CVEs más relevantes de la semana

Del 06/09/2025 al 13/09/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-10031

Descripción: A security vulnerability has been detected in Campcodes Grocery Sales and Inventory System 1.0. Impacted is an unknown function of the file /ajax.php?action=delete_sales. The manipulation of the argument ID leads to sql injection. Remote exploitation of the attack is possible. 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: 2025-09-06

CVE-2025-10033

Descripción: A vulnerability has been found in itsourcecode Online Discussion Forum 1.0. This affects an unknown function of the file /admin. Such manipulation of the argument Username leads to sql injection. The attack may be performed from remote. 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: 2025-09-06

CVE-2025-10062

Descripción: A vulnerability was determined in itsourcecode Student Information Management System 1.0. This affects an unknown part of the file /admin/login.php. Executing manipulation of the argument uname can lead to sql injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.

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: 2025-09-06

CVE-2025-10068

Descripción: A flaw has been found in itsourcecode Online Discussion Forum 1.0. This affects an unknown function of the file /admin/admin_forum/add_views.php. Executing manipulation of the argument ID can lead to sql injection. It is possible to launch the attack 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: 2025-09-07

CVE-2025-10076

Descripción: A weakness has been identified in SourceCodester Online Polling System 1.0. This affects an unknown function of the file /manage-profile.php. This manipulation of the argument email causes sql injection. The attack may be initiated remotely. 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: 2025-09-08

CVE-2025-10077

Descripción: A security vulnerability has been detected in SourceCodester Online Polling System 1.0. This impacts an unknown function of the file /registeracc.php. Such manipulation of the argument email leads to sql injection. The attack may be launched 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: 2025-09-08

CVE-2025-10078

Descripción: A vulnerability was detected in SourceCodester Online Polling System 1.0. Affected is an unknown function of the file /admin/candidates.php. Performing manipulation of the argument ID results in sql injection. Remote exploitation of the attack is possible. The exploit is now 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: 2025-09-08

CVE-2025-10082

Descripción: A vulnerability has been found in SourceCodester Online Polling System 1.0. Affected is an unknown function of the file /admin/manage-admins.php. Such manipulation of the argument email leads to sql injection. The attack can be executed 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: 2025-09-08

CVE-2025-10097

Descripción: A vulnerability was identified in SimStudioAI sim up to 1.0.0. This impacts an unknown function of the file apps/sim/app/api/function/execute/route.ts. The manipulation of the argument code leads to code injection. The attack is possible to be carried out remotely.

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: 2025-09-08

CVE-2025-10100

Descripción: A vulnerability was detected in SourceCodester Simple Forum Discussion System 1.0. This impacts an unknown function of the file /admin_class.php?action=login. Performing manipulation of the argument Username results in sql injection. It is possible to initiate the attack remotely. The exploit is now 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: 2025-09-08

CVE-2025-10102

Descripción: A security flaw has been discovered in code-projects Online Event Judging System 1.0. This affects an unknown function of the file /index.php. Performing manipulation of the argument Username results in sql injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may 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: 2025-09-08

CVE-2025-10103

Descripción: A weakness has been identified in code-projects Online Event Judging System 1.0. This impacts an unknown function of the file /home.php. Executing manipulation of the argument main_event can lead to sql injection. The attack may be performed from remote. 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: 2025-09-08

CVE-2025-9113

Descripción: The Doccure theme for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'doccure_temp_upload_to_media' function in all versions up to, and including, 1.4.8. 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: 2025-09-08

CVE-2025-9114

Descripción: The Doccure theme for WordPress is vulnerable to Arbitrary User Password Change in versions up to, and including, 1.4.8. This is due to the plugin providing user-controlled access to objects, letting a user bypass authorization and access system resources. This makes it possible for unauthenticated attackers to change user passwords and potentially take over administrator accounts.

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: 2025-09-08

CVE-2025-10104

Descripción: A security vulnerability has been detected in code-projects Online Event Judging System 1.0. Affected is an unknown function of the file /review_search.php. The manipulation of the argument txtsearch 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: 2025-09-08

CVE-2025-10108

Descripción: A vulnerability was found in Campcodes Online Loan Management System 1.0. This vulnerability affects unknown code of the file /ajax.php?action=delete_loan. Performing manipulation of the argument ID results in sql injection. The attack may be initiated remotely. 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: 2025-09-08

CVE-2025-10109

Descripción: A vulnerability was determined in Campcodes Online Loan Management System 1.0. This issue affects some unknown processing of the file /ajax.php?action=delete_payment. Executing manipulation of the argument ID can lead to sql injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.

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: 2025-09-08

CVE-2025-10111

Descripción: A security flaw has been discovered in itsourcecode Student Information Management System 1.0. The affected element is an unknown function of the file /admin/modules/instructor/index.php. The manipulation of the argument ID results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may 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: 2025-09-08

CVE-2025-10112

Descripción: A weakness has been identified in itsourcecode Student Information Management System 1.0. The impacted element is an unknown function of the file /admin/modules/department/index.php. This manipulation of the argument ID causes sql injection. The attack is possible to be carried out remotely. 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: 2025-09-09

CVE-2025-10113

Descripción: A security vulnerability has been detected in itsourcecode Student Information Management System 1.0. This affects an unknown function of the file /admin/modules/room/index.php. Such manipulation of the argument ID leads to sql injection. The attack may be performed from remote. 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: 2025-09-09

CVE-2025-10114

Descripción: A vulnerability was found in PHPGurukul Small CRM 4.0. Affected by this issue is some unknown functionality of the file /profile.php. The manipulation of the argument Name results in sql injection. The attack can be launched remotely. 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: 2025-09-09

CVE-2025-10118

Descripción: A security vulnerability has been detected in itsourcecode E-Logbook with Health Monitoring System for COVID-19 1.0. The affected element is an unknown function of the file /login.php. The manipulation of the argument Username leads to sql injection. The attack is possible to be carried out 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: 2025-09-09

CVE-2025-42922

Descripción: SAP NetWeaver AS Java allows an attacker authenticated as a non-administrative user to use a flaw in an available service to upload an arbitrary file. This file when executed can lead to a full compromise of confidentiality, integrity and availability of the system.

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-94

Tecnología: No especificado

Publicado el: 2025-09-09

CVE-2025-42944

Descripción: Due to a deserialization vulnerability in SAP NetWeaver, an unauthenticated attacker could exploit the system through the RMI-P4 module by submitting malicious payload to an open port. The deserialization of such untrusted Java objects could lead to arbitrary OS command execution, posing a high impact to the application's confidentiality, integrity, and availability.

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-502

Tecnología: No especificado

Publicado el: 2025-09-09

CVE-2025-42958

Descripción: Due to a missing authentication check in the SAP NetWeaver application on IBM i-series, the application allows high privileged unauthorized users to read, modify, or delete sensitive information, as well as access administrative or privileged functionalities. This results in a high impact on the confidentiality, integrity, and availability of the application.

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-250

Tecnología: No especificado

Publicado el: 2025-09-09

CVE-2025-10134

Descripción: The Goza - Nonprofit Charity WordPress Theme theme for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the alone_import_pack_restore_data() function in all versions up to, and including, 3.2.2. 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 ...

CVSS: 9.1 (CRITICAL)

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

Tipo: CWE-73

Tecnología: No especificado

Publicado el: 2025-09-09

CVE-2025-40795

Descripción: A vulnerability has been identified in SIMATIC PCS neo V4.1 (All versions), SIMATIC PCS neo V5.0 (All versions), User Management Component (UMC) (All versions < V2.15.1.3). Affected products contain a stack-based buffer overflow vulnerability in the integrated UMC component. This could allow an unauthenticated remote attacker to execute arbitrary code or to cause a denial of service condition.

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: 2025-09-09

CVE-2025-40804

Descripción: A vulnerability has been identified in SIMATIC Virtualization as a Service (SIVaaS) (All versions). The affected application exposes a network share without any authentication. This could allow an attacker to access or alter sensitive data without proper authorization.

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-732

Tecnología: No especificado

Publicado el: 2025-09-09

CVE-2025-54261

Descripción: ColdFusion versions 2025.3, 2023.15, 2021.21 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary code execution by an attacker. Scope is changed.

CVSS: 9.0 (CRITICAL)

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

Tipo: CWE-22

Tecnología: No especificado

Publicado el: 2025-09-09

CVE-2025-55232

Descripción: Deserialization of untrusted data in Microsoft High Performance Compute Pack (HPC) allows an unauthorized attacker to execute code 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-502

Tecnología: No especificado

Publicado el: 2025-09-09

CVE-2025-55234

Descripción: SMB Server might be susceptible to relay attacks depending on the configuration. An attacker who successfully exploited these vulnerabilities could perform relay attacks and make the users subject to elevation of privilege attacks. The SMB Server already supports mechanisms for hardening against relay attacks:

SMB Server signing SMB Server Extended Protection for Authentication (EPA)

Microsof...

CVSS: 8.8 (HIGH)

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

Tipo: CWE-287

Tecnología: No especificado

Publicado el: 2025-09-09

CVE-2025-8570

Descripción: The BeyondCart Connector plugin for WordPress is vulnerable to Privilege Escalation due to improper JWT secret management and authorization within the determine_current_user filter in versions 1.4.2 through 2.1.0. This makes it possible for unauthenticated attackers to craft valid tokens and assume any user's identity.

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: 2025-09-11

CVE-2025-40687

Descripción: SQL Injection in Online Fire Reporting System v1.2 by PHPGurukul. This vulnerability allows an attacker to retrieve, create, update and delete database via

'mobilenumber', 'teamleadname' and 'teammember' parameters in the endpoint '/ofrs/admin/add-team.php'.

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: 2025-09-11

CVE-2025-40689

Descripción: SQL Injection in Online Fire Reporting System v1.2 by PHPGurukul. This vulnerability allows an attacker to retrieve, create, update and delete database via

'remark', 'status' and 'requestid' parameters in the endpoint '/ofrs/admin/request-details.php'.

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: 2025-09-11

CVE-2025-40690

Descripción: SQL Injection in Online Fire Reporting System v1.2 by PHPGurukul. This vulnerability allows an attacker to retrieve, create, update and delete database via 'teamid' parameter in the endpoint '/ofrs/admin/edit-team.php'.

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: 2025-09-11

CVE-2025-40691

Descripción: SQL Injection in Online Fire Reporting System v1.2 by PHPGurukul. This vulnerability allows an attacker to retrieve, create, update and delete database via

'todate' parameter in the endpoint '/ofrs/admin/bwdates-report-result.php'.

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: 2025-09-11

CVE-2025-40692

Descripción: SQL Injection in Online Fire Reporting System v1.2 by PHPGurukul. This vulnerability allows an attacker to retrieve, create, update and delete database via

'requestid' parameter in the endpoint '/ofrs/details.php'.

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: 2025-09-11

CVE-2025-10264

Descripción: Certain models of NVR developed by Digiever has an Exposure of Sensitive Information vulnerability, allowing unauthenticated remoter attackers to access the system configuration file and obtain plaintext credentials of the NVR and its connected cameras.

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-497

Tecnología: No especificado

Publicado el: 2025-09-12

CVE-2025-10265

Descripción: Certain models of NVR developed by Digiever has an OS Command Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary OS commands and execute them on 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-78

Tecnología: No especificado

Publicado el: 2025-09-12

CVE-2025-10266

Descripción: NUP Pro developed by NewType Infortech has a SQL Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read, modify, and delete database contents.

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: 2025-09-12

Resumen del Reporte

CVEs analizados: 40

Promedio CVSS: 8.44

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat