CVEs más relevantes de la semana

Del 13/09/2025 al 20/09/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-10392

Descripción: A vulnerability was detected in Mercury KM08-708H GiGA WiFi Wave2 1.1.14. This affects an unknown function of the component HTTP Header Handler. The manipulation of the argument Host results in stack-based buffer overflow. The attack can be executed remotely. The exploit is now public and may be used.

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: 2025-09-14

CVE-2025-10396

Descripción: A vulnerability was determined in SourceCodester Pet Grooming Management Software 1.0. Affected by this issue is some unknown functionality of the file /admin/edit_role.php. Executing manipulation of the argument ID can lead to sql injection. It is possible to launch the attack 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: 2025-09-14

CVE-2025-10402

Descripción: A flaw has been found in PHPGurukul Beauty Parlour Management System 1.1. The impacted element is an unknown function of the file /admin/readenq.php. Executing manipulation of the argument delid can lead to sql injection. The attack can be executed 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: 2025-09-14

CVE-2025-10403

Descripción: A vulnerability has been found in PHPGurukul Beauty Parlour Management System 1.1. This affects an unknown function of the file /admin/view-enquiry.php. The manipulation of the argument viewid leads to sql injection. The attack is possible to be carried out 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: 2025-09-14

CVE-2025-10404

Descripción: A vulnerability was found in itsourcecode Baptism Information Management System 1.0. This impacts an unknown function of the file /rptbaptismal.php. The manipulation of the argument ID results in sql injection. The attack may be performed from remote. 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: 2025-09-14

CVE-2025-10405

Descripción: A vulnerability was determined in itsourcecode Baptism Information Management System 1.0. Affected is an unknown function of the file /listbaptism.php. This manipulation of the argument bapt_id causes sql injection. It is possible to initiate the attack 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: 2025-09-14

CVE-2025-10410

Descripción: A security vulnerability has been detected in SourceCodester Link Status Checker 1.0. This vulnerability affects unknown code of the file index.php. The manipulation of the argument proxy leads to server-side request forgery. The attack may be initiated remotely. The exploit has been disclosed publicly 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-918

Tecnología: No especificado

Publicado el: 2025-09-14

CVE-2025-10413

Descripción: A vulnerability has been found in Campcodes Grocery Sales and Inventory System 1.0. The affected element is an unknown function of the file /ajax.php?action=delete_customer. Such manipulation of the argument ID 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: 2025-09-14

CVE-2025-10414

Descripción: A vulnerability was found in Campcodes Grocery Sales and Inventory System 1.0. The impacted element is an unknown function of the file /ajax.php?action=save_customer. Performing manipulation of the argument ID results in sql injection. The attack is possible to be carried out 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: 2025-09-14

CVE-2025-10415

Descripción: A vulnerability was determined in Campcodes Grocery Sales and Inventory System 1.0. This affects an unknown function of the file /ajax.php?action=save_supplier. Executing manipulation of the argument ID can lead to sql injection. The attack may be performed from remote. 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: 2025-09-14

CVE-2025-10416

Descripción: A vulnerability was identified in Campcodes Grocery Sales and Inventory System 1.0. This impacts an unknown function of the file /ajax.php?action=delete_supplier. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack 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: 2025-09-15

CVE-2025-10417

Descripción: A security flaw has been discovered in Campcodes Grocery Sales and Inventory System 1.0. Affected is an unknown function of the file /ajax.php?action=delete_product. The manipulation of the argument ID results in sql injection. It is possible to launch the attack 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: 2025-09-15

CVE-2025-10452

Descripción: Statistical Database System developed by Gotac has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to read, modify, and delete database contents with high-level privileges.

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: 2025-09-15

CVE-2025-10424

Descripción: A vulnerability was determined in 1000projects Online Student Project Report Submission and Evaluation System 1.0. The affected element is an unknown function of the file /admin/controller/faculty_controller.php. This manipulation of the argument new_image causes unrestricted upload. The attack is possible to be carried out 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-284

Tecnología: No especificado

Publicado el: 2025-09-15

CVE-2025-10425

Descripción: A vulnerability was identified in 1000projects Online Student Project Report Submission and Evaluation System 1.0. The impacted element is an unknown function of the file /admin/controller/student_controller.php. Such manipulation of the argument new_image leads to unrestricted upload. The attack may be performed from remote. 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-284

Tecnología: No especificado

Publicado el: 2025-09-15

CVE-2025-10426

Descripción: A security flaw has been discovered in itsourcecode Online Laundry Management System 1.0. This affects an unknown function of the file /login.php. Performing manipulation of the argument Username results in sql injection. It is possible to initiate the attack 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: 2025-09-15

CVE-2025-10432

Descripción: A vulnerability was found in Tenda AC1206 15.03.06.23. This vulnerability affects the function check_param_changed of the file /goform/AdvSetMacMtuWa of the component HTTP Request Handler. Performing manipulation of the argument wanMTU results in stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been made public and could be used.

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: 2025-09-15

CVE-2025-10435

Descripción: A security flaw has been discovered in Campcodes Computer Sales and Inventory System 1.0. The affected element is an unknown function of the file /pages/cust_edit1.php. The manipulation of the argument ID results in sql injection. The attack may be performed from remote. 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: 2025-09-15

CVE-2025-10444

Descripción: A security flaw has been discovered in Campcodes Online Job Finder System 1.0. This issue affects some unknown processing of the file /advancesearch.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: 2025-09-15

CVE-2025-10445

Descripción: A weakness has been identified in Campcodes Computer Sales and Inventory System 1.0. Impacted is an unknown function of the file /pages/us_transac.php?action=add. Executing manipulation of the argument Username 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: 2025-09-15

CVE-2025-10446

Descripción: A security vulnerability has been detected in Campcodes Computer Sales and Inventory System 1.0. The affected element is an unknown function of the file /pages/cust_searchfrm.php?action=edit. 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: 2025-09-15

CVE-2025-58045

Descripción: Dataease is an open source data analytics and visualization platform. In Dataease versions up to 2.10.12, the patch introduced to mitigate DB2 JDBC deserialization remote code execution attacks only blacklisted the rmi parameter. The ldap parameter in the DB2 JDBC connection string was not filtered, allowing attackers to exploit the DB2 JDBC connection string to trigger server-side request forg...

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-918

Tecnología: No especificado

Publicado el: 2025-09-15

CVE-2025-58046

Descripción: Dataease is an open-source data visualization and analysis platform. In versions up to and including 2.10.12, the Impala data source is vulnerable to remote code execution due to insufficient filtering in the getJdbc method of the io.dataease.datasource.type.Impala class. Attackers can construct malicious JDBC connection strings that exploit JNDI injection and trigger RMI deserialization, ultim...

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-74

Tecnología: No especificado

Publicado el: 2025-09-15

CVE-2025-58748

Descripción: Dataease is an open source data analytics and visualization platform. In Dataease versions up to 2.10.12 the H2 data source implementation (H2.java) does not verify that a provided JDBC URL starts with jdbc:h2. This lack of validation allows a crafted JDBC configuration that substitutes the Amazon Redshift driver and leverages the socketFactory and socketFactoryArg parameters to invoke org.spri...

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: 2025-09-15

CVE-2025-10473

Descripción: A security flaw has been discovered in yangzongzhuan RuoYi up to 4.8.1. This impacts the function filterKeyword of the file /com/ruoyi/common/utils/sql/SqlUtil.java of the component Blacklist Handler. The manipulation results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be exploited.

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: 2025-09-15

CVE-2025-10479

Descripción: A security flaw has been discovered in SourceCodester Online Student File Management System 1.0. The impacted element is an unknown function of the file /index.php. Performing manipulation of the argument stud_no results in sql injection. The attack may be initiated 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: 2025-09-15

CVE-2025-4688

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in BGS Interactive SINAV.LINK Exam Result Module allows SQL Injection.This issue affects SINAV.LINK Exam Result Module: before 1.2.

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: 2025-09-16

CVE-2025-7743

Descripción: Cleartext Transmission of Sensitive Information vulnerability in Dolusoft Omaspot allows Interception, Privilege Escalation.This issue affects Omaspot: before 12.09.2025.

CVSS: 9.6 (CRITICAL)

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

Tipo: CWE-319

Tecnología: No especificado

Publicado el: 2025-09-16

CVE-2025-7744

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Dolusoft Omaspot allows SQL Injection.This issue affects Omaspot: before 12.09.2025.

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: 2025-09-16

CVE-2024-13149

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), CWE - 200 - Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Arma Store Armalife allows SQL Injection.This issue affects Armalife: through 20250916.

NOTE: The vendor did not inform about the completion of the fixing process within the specified time. The CVE will be updated when ne...

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: 2025-09-16

CVE-2025-10562

Descripción: A flaw has been found in Campcodes Grocery Sales and Inventory System 1.0. This affects an unknown function of the file /ajax.php?action=save_product. This manipulation of the argument ID causes sql injection. Remote exploitation of the attack is possible. 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: 2025-09-16

CVE-2025-10564

Descripción: A vulnerability was found in Campcodes Grocery Sales and Inventory System 1.0. Affected is an unknown function of the file /ajax.php?action=delete_category. Performing manipulation of the argument ID results in sql injection. The attack is possible to be carried out 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: 2025-09-16

CVE-2025-10565

Descripción: A vulnerability was determined in Campcodes Grocery Sales and Inventory System 1.0. Affected by this vulnerability is an unknown functionality of the file /ajax.php?action=delete_receiving. Executing manipulation of the argument ID can lead to sql injection. The attack may be performed from remote. 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: 2025-09-16

CVE-2025-10439

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Yordam Informatics Yordam Library Automation System allows SQL Injection.This issue affects Yordam Library Automation System: from 21.5 & 21.6 before 21.7.

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: 2025-09-17

CVE-2025-10604

Descripción: A vulnerability was identified in PHPGurukul Online Discussion Forum 1.0. This affects an unknown part of the file /admin/edit_member.php. The manipulation of the argument ID leads to sql injection. The attack may be initiated 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: 2025-09-17

CVE-2025-59352

Descripción: Dragonfly is an open source P2P-based file distribution and image acceleration system. Prior to 2.1.0, the gRPC API and HTTP APIs allow peers to send requests that force the recipient peer to create files in arbitrary file system locations, and to read arbitrary files. This allows peers to steal other peers' secret data and to gain remote code execution (RCE) capabilities on the peer's machine....

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: 2025-09-17

CVE-2025-10624

Descripción: A security flaw has been discovered in PHPGurukul User Management System 1.0. This affects an unknown function of the file /login.php. Performing manipulation of the argument emailid results in sql injection. The attack can be initiated 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: 2025-09-17

CVE-2025-10662

Descripción: A vulnerability has been found in SeaCMS up to 13.3. The impacted element is an unknown function of the file /admin_members.php?ac=editsave. Such manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This affects another injection point than CVE-2025-25513.

CVSS: 4.7 (MEDIUM)

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

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-18

CVE-2025-10664

Descripción: A vulnerability was determined in PHPGurukul Small CRM 4.0. This impacts an unknown function of the file /create-ticket.php. Executing manipulation of the argument subject 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: 2025-09-18

CVE-2025-10666

Descripción: A security flaw has been discovered in D-Link DIR-825 up to 2.10. Affected by this vulnerability is the function sub_4106d4 of the file apply.cgi. The manipulation of the argument countdown_time results in buffer overflow. The attack can be executed remotely. The exploit has been released to the public and may be exploited. This vulnerability only affects products that are no longer supported b...

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: 2025-09-18

CVE-2025-10668

Descripción: A security vulnerability has been detected in itsourcecode Online Discussion Forum 1.0. This affects an unknown part of the file /members/compose_msg_admin.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: 2025-09-18

CVE-2025-10670

Descripción: A flaw has been found in itsourcecode E-Logbook with Health Monitoring System for COVID-19 1.0. This issue affects some unknown processing of the file /check_profile.php. Executing manipulation of the argument profile_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: 2025-09-18

CVE-2025-10673

Descripción: A vulnerability was determined in itsourcecode Student Information Management System 1.0. The impacted element is an unknown function of the file /admin/modules/class/index.php. This manipulation of the argument classId causes sql injection. The attack may be initiated 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: 2025-09-18

CVE-2025-10687

Descripción: A vulnerability was found in SourceCodester Responsive E-Learning System 1.0. This affects an unknown part of the file /admin/add_teacher.php. The manipulation of the argument Username results in sql injection. It is possible to launch the attack 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: 2025-09-18

CVE-2025-10688

Descripción: A vulnerability was determined in SourceCodester Pet Grooming Management Software 1.0. This vulnerability affects unknown code of the file /admin/operation/paid.php. This manipulation of the argument insta_amt causes sql injection. The attack can be initiated 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: 2025-09-18

CVE-2025-10690

Descripción: The Goza - Nonprofit Charity WordPress Theme theme for WordPress is vulnerable to unauthorized arbitrary file uploads due to a missing capability check on the 'beplus_import_pack_install_plugin' function in all versions up to, and including, 3.2.2. This makes it possible for unauthenticated attackers to upload zip files containing webshells disguised as plugins from remote locations to achieve ...

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: 2025-09-19

CVE-2025-5948

Descripción: The Service Finder Bookings plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 6.0. This is due to the plugin not properly validating a user's identity prior to claiming a business when using the claim_business AJAX action. This makes it possible for unauthenticated attackers to login as any user including admins. Please note th...

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: 2025-09-19

Resumen del Reporte

CVEs analizados: 47

Promedio CVSS: 7.97

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat