CVEs más relevantes de la semana

Del 27/09/2025 al 04/10/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-11057

Descripción: A vulnerability has been found in SourceCodester Pet Grooming Management Software 1.0. Affected by this issue is some unknown functionality of the file /admin/print_inv.php. 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: 2025-09-27

CVE-2025-11061

Descripción: A vulnerability was found in Campcodes Online Learning Management System 1.0. This affects an unknown part of the file /admin/edit_student.php. Performing manipulation of the argument cys 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: 2025-09-27

CVE-2025-11062

Descripción: A vulnerability was determined in Campcodes Online Learning Management System 1.0. This vulnerability affects unknown code of the file /admin/save_student.php. Executing manipulation of the argument class_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: 2025-09-27

CVE-2025-11063

Descripción: A vulnerability was identified in Campcodes Online Learning Management System 1.0. This issue affects some unknown processing of the file /admin/edit_department.php. The manipulation of the argument d 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: 2025-09-27

CVE-2025-11064

Descripción: A security flaw has been discovered in Campcodes Online Learning Management System 1.0. Impacted is an unknown function of the file /admin/teachers.php. The manipulation of the argument department 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: 2025-09-27

CVE-2025-11066

Descripción: A flaw has been found in code-projects Online Bidding System 1.0. This impacts an unknown function of the file /administrator/bidlist.php. Executing manipulation of the argument ID can lead to sql injection. The attack may be launched 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: 2025-09-27

CVE-2025-11070

Descripción: A vulnerability was identified in Projectworlds Online Shopping System 1.0. This affects an unknown part of the file /store/cart_add.php. Such manipulation of the argument ID leads to sql injection. 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-74

Tecnología: No especificado

Publicado el: 2025-09-27

CVE-2025-11074

Descripción: A flaw has been found in code-projects Project Monitoring System 1.0. The impacted element is an unknown function of the file /login.php. This manipulation of the argument username/password 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: 2025-09-27

CVE-2025-11075

Descripción: A vulnerability has been found in Campcodes Online Learning Management System 1.0. This affects an unknown function of the file /admin/de_activate.php. Such 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: 2025-09-27

CVE-2025-11076

Descripción: A vulnerability was found in Campcodes Online Learning Management System 1.0. This impacts an unknown function of the file /admin/edit_teacher.php. Performing manipulation of the argument department 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: 2025-09-27

CVE-2025-11077

Descripción: A vulnerability was determined in Campcodes Online Learning Management System 1.0. Affected is an unknown function of the file /admin/add_content.php. Executing manipulation of the argument Title can lead to sql injection. The attack can be executed 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: 2025-09-27

CVE-2025-11079

Descripción: A security flaw has been discovered in Campcodes Farm Management System 1.0. Affected by this issue is some unknown functionality. The manipulation results in file and directory information exposure. The attack may be performed from remote. The exploit has been released to the public and may be exploited.

CVSS: 5.3 (MEDIUM)

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

Tipo: CWE-200

Tecnología: No especificado

Publicado el: 2025-09-27

CVE-2025-11094

Descripción: A security vulnerability has been detected in code-projects E-Commerce Website 1.0. This affects an unknown part of the file /pages/admin_product_details.php. Such manipulation of the argument prod_id 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: 2025-09-28

CVE-2025-11101

Descripción: A security flaw has been discovered in itsourcecode Open Source Job Portal 1.0. This impacts an unknown function of the file /jobportal/admin/company/index.php?view=edit. Performing manipulation of the argument ID 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: 2025-09-28

CVE-2025-11102

Descripción: A weakness has been identified in Campcodes Online Learning Management System 1.0. Affected is an unknown function of the file /admin/edit_content.php. Executing manipulation of the argument Title can lead to sql injection. The attack can be launched 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: 2025-09-28

CVE-2025-11105

Descripción: A flaw has been found in code-projects Simple Scheduling System 1.0. This affects an unknown part of the file /schedulingsystem/addsubject.php. This manipulation of the argument subcode 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: 2025-09-28

CVE-2025-11106

Descripción: A vulnerability has been found in code-projects Simple Scheduling System 1.0. This vulnerability affects unknown code of the file /schedulingsystem/addfaculty.php. Such manipulation of the argument falname 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: 2025-09-28

CVE-2025-11107

Descripción: A vulnerability was found in code-projects Simple Scheduling System 1.0. This issue affects some unknown processing of the file /schedulingsystem/addcourse.php. Performing manipulation of the argument corcode 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: 2025-09-28

CVE-2025-11108

Descripción: A vulnerability was determined in code-projects Simple Scheduling System 1.0. Impacted is an unknown function of the file /schedulingsystem/addroom.php. Executing manipulation of the argument room 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: 2025-09-28

CVE-2025-11109

Descripción: A vulnerability was identified in Campcodes Computer Sales and Inventory System 1.0. The affected element is an unknown function of the file /pages/us_edit.php?action=edit. 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: 2025-09-28

CVE-2025-11110

Descripción: A security flaw has been discovered in Campcodes Online Learning Management System 1.0. The impacted element is an unknown function of the file /admin/school_year.php. The manipulation of the argument school_year 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: 2025-09-28

CVE-2025-11111

Descripción: A weakness has been identified in Campcodes Advanced Online Voting Management System 1.0. This affects an unknown function of the file /admin/candidates_edit.php. This manipulation of the argument ID causes sql injection. The attack can 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: 2025-09-28

CVE-2025-11115

Descripción: A vulnerability has been found in code-projects Simple Scheduling System 1.0. Affected by this issue is some unknown functionality of the file /addtime.php. The manipulation of the argument starttime/endtime leads to sql injection. Remote exploitation of the attack is possible. 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: 2025-09-28

CVE-2025-11116

Descripción: A vulnerability was found in code-projects Simple Scheduling System 1.0. This affects an unknown part of the file /add.home.php. The manipulation of the argument faculty results in sql injection. The attack can be executed remotely. The exploit has been made public and could 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: 2025-09-28

CVE-2025-11118

Descripción: A vulnerability was identified in CodeAstro Student Grading System 1.0. This issue affects some unknown processing of the file /adminLogin.php. Such manipulation of the argument staffId leads to sql injection. 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-74

Tecnología: No especificado

Publicado el: 2025-09-28

CVE-2025-11126

Descripción: A security flaw has been discovered in Apeman ID71 218.53.203.117. This vulnerability affects unknown code of the file /system/www/system.ini. The manipulation results in hard-coded credentials. The attack may be performed from remote. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.

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-259

Tecnología: No especificado

Publicado el: 2025-09-29

CVE-2025-11139

Descripción: A vulnerability was determined in Bjskzy Zhiyou ERP up to 11.0. Affected is the function uploadStudioFile of the component com.artery.form.services.FormStudioUpdater. This manipulation of the argument filepath causes path traversal. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but...

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-22

Tecnología: No especificado

Publicado el: 2025-09-29

CVE-2025-11140

Descripción: A vulnerability was identified in Bjskzy Zhiyou ERP up to 11.0. Affected by this vulnerability is the function openForm of the component com.artery.richclient.RichClientService. Such manipulation of the argument contentString leads to xml external entity reference. The attack can be executed remotely. The exploit is publicly available and might be used. The vendor was contacted early about this...

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-610

Tecnología: No especificado

Publicado el: 2025-09-29

CVE-2024-13150

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Fayton Software and Consulting Services fayton.Pro ERP allows SQL Injection.This issue affects fayton.Pro ERP: through 20250929.

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: 2025-09-29

CVE-2025-34207

Descripción: Vasion Print (formerly PrinterLogic) Virtual Appliance Host prior to 22.0.1049 and Application prior to 20.0.2786 (VA and SaaS deployments) configure the SSH client within Docker instances with the following options: `UserKnownHostsFile=/dev/null`, `StrictHostKeyChecking=no`, and `ForwardAgent yes`. These settings disable verification of the remote host's SSH key and automatically forward the ...

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: 2025-09-29

CVE-2025-54592

Descripción: FreshRSS is a free, self-hostable RSS aggregator. Versions 1.26.3 and below do not properly terminate the session during logout. After a user logs out, the session cookie remains active and unchanged. The unchanged cookie could be reused by an attacker if a new session were to be started. This failure to invalidate the session can lead to session hijacking and fixation vulnerabilities. This iss...

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-613

Tecnología: No especificado

Publicado el: 2025-09-29

CVE-2025-8625

Descripción: The Copypress Rest API plugin for WordPress is vulnerable to Remote Code Execution via copyreap_handle_image() Function in versions 1.1 to 1.2. The plugin falls back to a hard-coded JWT signing key when no secret is defined and does not restrict which file types can be fetched and saved as attachments. As a result, unauthenticated attackers can forge a valid token to gain elevated privileges an...

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-321

Tecnología: No especificado

Publicado el: 2025-09-30

CVE-2025-9762

Descripción: The Post By Email plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the save_attachments function in all versions up to, and including, 1.0.4b. 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-78

Tecnología: No especificado

Publicado el: 2025-09-30

CVE-2020-36852

Descripción: The Custom Searchable Data Entry System plugin for WordPress is vulnerable to unauthenticated database wiping in versions up to, and including 1.7.1, due to a missing capability check and lack of sufficient validation on the ghazale_sds_delete_entries_table_row() function. This makes it possible for unauthenticated attackers to completely wipe database tables such as wp_users.

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-862

Tecnología: No especificado

Publicado el: 2025-10-01

CVE-2025-59735

Descripción: Operating system command injection vulnerability in AndSoft's e-TMS v25.03. This vulnerability allows an attacker to execute operating system commands on the server by sending a POST request. The relationship between parameter and assigned identifier is a 'm' parameter in '/clt/LOGINFRM.ASP'.

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: 2025-10-02

CVE-2025-59736

Descripción: Operating system command injection vulnerability in AndSoft's e-TMS v25.03. This vulnerability allows an attacker to execute operating system commands on the server by sending a POST request. The relationship between parameter and assigned identifier is a 'm' parameter in '/clt/LOGINFRM_DJO.ASP'.

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: 2025-10-02

CVE-2025-59737

Descripción: Operating system command injection vulnerability in AndSoft's e-TMS v25.03. This vulnerability allows an attacker to execute operating system commands on the server by sending a POST request. The relationship between parameter and assigned identifier is a 'm' parameter in '/clt/LOGINFRM_LXA.ASP'.

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: 2025-10-02

CVE-2025-59738

Descripción: Operating system command injection vulnerability in AndSoft's e-TMS v25.03. This vulnerability allows an attacker to execute operating system commands on the server by sending a POST request. The relationship between parameter and assigned identifier is a 'm' parameter in '/clt/LOGINFRM_BET.ASP'.

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: 2025-10-02

CVE-2025-59739

Descripción: Operating system command injection vulnerability in AndSoft's e-TMS v25.03. This vulnerability allows an attacker to execute operating system commands on the server by sending a POST request. The relationship between parameter and assigned identifier is a 'm' parameter in '/clt/LOGINFRM_original.ASP'.

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: 2025-10-02

CVE-2025-59740

Descripción: Operating system command injection vulnerability in AndSoft's e-TMS v25.03. This vulnerability allows an attacker to execute operating system commands on the server by sending a POST request. The relationship between parameter and assigned identifier is a 'm' parameter in '/clt/LOGINFRM_CAT.ASP'.

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: 2025-10-02

CVE-2025-59741

Descripción: Operating system command injection vulnerability in AndSoft's e-TMS v25.03. This vulnerability allows an attacker to execute operating system commands on the server by sending a POST request. The relationship between parameter and assigned identifier is a 'm' parameter in '/CLT/LOGINERRORFRM.ASP'.

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: 2025-10-02

CVE-2025-59742

Descripción: SQL injection vulnerability in AndSoft's e-TMS v25.03. This vulnerability could allow an attacker to retrieve, create, update, and delete databases by sending a POST request. The relationship between parameter and assigned identifier is a 'USRMAIL' parameter in'/inc/login/TRACK_REQUESTFRMSQL.ASP'.

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: 2025-10-02

CVE-2025-59743

Descripción: SQL injection vulnerability in AndSoft's e-TMS v25.03. This vulnerability could allow an attacker to retrieve, create, update, and delete databases by sending a POST request. The relationship between parameter and assigned identifier is a 'SessionID' cookie in '/inc/connect/CONNECTION.ASP'.

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: 2025-10-02

CVE-2025-6388

Descripción: The Spirit Framework plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 1.2.14. This is due to the custom_actions() function not properly validating a user's identity prior to authenticating them to the site. This makes it possible for unauthenticated attackers to log in as any user, including administrators, granted they have access to the adminis...

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: 2025-10-03

CVE-2025-10726

Descripción: The WPRecovery plugin for WordPress is vulnerable to SQL Injection via the 'data[id]' parameter in all versions up to, and including, 2.0. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be ...

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-89

Tecnología: No especificado

Publicado el: 2025-10-03

CVE-2025-7721

Descripción: The JoomSport – for Sports: Team & League, Football, Hockey & more plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 5.7.3 via the task parameter. This makes it possible for unauthenticated attackers to include and execute arbitrary .php files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access 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-98

Tecnología: No especificado

Publicado el: 2025-10-03

CVE-2025-9209

Descripción: The RestroPress – Online Food Ordering System plugin for WordPress is vulnerable to Authentication Bypass in versions 3.0.0 to 3.1.9.2. This is due to the plugin exposing user private tokens and API data via the /wp-json/wp/v2/users REST API endpoint. This makes it possible for unauthenticated attackers to forge JWT tokens for other users, including administrators, and authenticate as them.

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-200

Tecnología: No especificado

Publicado el: 2025-10-03

CVE-2025-9286

Descripción: The Appy Pie Connect for WooCommerce plugin for WordPress is vulnerable to Privilege Escalation due to missing authorization within the reset_user_password() REST handler in all versions up to, and including, 1.1.2. This makes it possible for unauthenticated attackers to to reset the password of arbitrary users, including administrators, thereby gaining administrative access.

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: 2025-10-03

CVE-2025-9485

Descripción: The OAuth Single Sign On – SSO (OAuth Client) plugin for WordPress is vulnerable to Improper Verification of Cryptographic Signature in versions up to, and including, 6.26.12. This is due to the plugin performing unsafe JWT token processing without verification or validation in the `get_resource_owner_from_id_token` function. This makes it possible for unauthenticated attackers to bypass authen...

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-347

Tecnología: No especificado

Publicado el: 2025-10-04

Resumen del Reporte

CVEs analizados: 49

Promedio CVSS: 8.33

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat ▯