CVEs más relevantes de la semana

Del 07/10/2025 al 14/10/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-11401

Descripción: A flaw has been found in SourceCodester Hotel and Lodge Management System 1.0. Affected is an unknown function of the file /pages/save_curr.php. This manipulation of the argument currcode causes sql injection. The attack is possible to be carried out remotely. The exploit has been published 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: 2025-10-07

CVE-2025-11402

Descripción: A vulnerability has been found in SourceCodester Hotel and Lodge Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /del_curr.php. Such manipulation of the argument ID leads to sql injection. The attack may be performed from remote. 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: 2025-10-07

CVE-2025-11403

Descripción: A vulnerability was found in SourceCodester Hotel and Lodge Management System 1.0. Affected by this issue is some unknown functionality of the file /del_booking.php. Performing manipulation of the argument ID results in sql injection. It is possible to initiate the attack remotely. The exploit has been made public and could 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: 2025-10-07

CVE-2025-11404

Descripción: A vulnerability was determined in SourceCodester Hotel and Lodge Management System 1.0. This affects an unknown part of the file /pages/save_tax.php. Executing manipulation of the argument percentage can lead to sql injection. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized.

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: 2025-10-07

CVE-2025-11405

Descripción: A vulnerability was identified in SourceCodester Hotel and Lodge Management System 1.0. This vulnerability affects unknown code of the file /del_tax.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might 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: 2025-10-07

CVE-2025-11415

Descripción: A vulnerability was identified in PHPGurukul Beauty Parlour Management System 1.1. Affected by this issue is some unknown functionality of the file /admin/customer-list.php. Such manipulation of the argument delid leads to sql injection. It is possible to launch 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: 2025-10-07

CVE-2025-11416

Descripción: A security flaw has been discovered in PHPGurukul Beauty Parlour Management System 1.1. This affects an unknown part of the file /admin/invoices.php. Performing manipulation of the argument delid 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: 2025-10-07

CVE-2025-11418

Descripción: A security vulnerability has been detected in Tenda CH22 up to 1.0.0.1. This issue affects the function formWrlsafeset of the file /goform/AdvSetWrlsafeset of the component HTTP Request Handler. The manipulation of the argument mit_ssid_index leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed publicly 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: 2025-10-08

CVE-2025-11420

Descripción: A vulnerability was detected in code-projects E-Commerce Website 1.0. Impacted is an unknown function of the file /pages/edit_order_details.php. The manipulation of the argument order_id results in sql injection. The attack may be launched 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: 2025-10-08

CVE-2025-11422

Descripción: A vulnerability has been found in Campcodes Advanced Online Voting Management System 1.0. The impacted element is an unknown function of the file /admin/login.php. Such manipulation of the argument Username 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: 2025-10-08

CVE-2025-11423

Descripción: A vulnerability was found in Tenda CH22 1.0.0.1. This affects the function formSafeEmailFilter of the file /goform/SafeEmailFilter. Performing manipulation of the argument page results in memory corruption. The attack is possible to be carried out remotely. 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: 2025-10-08

CVE-2025-11424

Descripción: A vulnerability was determined in code-projects Web-Based Inventory and POS System 1.0. This impacts an unknown function of the file /login.php. Executing manipulation of the argument emailid 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: 2025-10-08

CVE-2025-10587

Descripción: The Community Events plugin for WordPress is vulnerable to SQL Injection via the event_category parameter in all versions up to, and including, 1.5.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries...

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: 2025-10-08

CVE-2025-11430

Descripción: A vulnerability was found in SourceCodester Simple E-Commerce Bookstore 1.0. The affected element is an unknown function of the file /cart.php. The manipulation of the argument remove results in sql injection. The attack can be executed 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: 2025-10-08

CVE-2025-11431

Descripción: A vulnerability was determined in code-projects Web-Based Inventory and POS System 1.0. The impacted element is an unknown function of the file /transaction.php. This manipulation of the argument shopid causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.

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: 2025-10-08

CVE-2025-11432

Descripción: A vulnerability was identified in itsourcecode Leave Management System 1.0. This affects an unknown function of the file /reset.php. Such manipulation of the argument employid 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: 2025-10-08

CVE-2025-11434

Descripción: A weakness has been identified in itsourcecode Student Transcript Processing System 1.0. Affected is an unknown function of the file /login.php. Executing manipulation of the argument uname can lead to sql injection. It is possible to launch the attack 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: 2025-10-08

CVE-2025-11469

Descripción: A weakness has been identified in SourceCodester Hotel and Lodge Management System 1.0. The affected element is an unknown function of the file /pages/save_customer.php. Executing manipulation of the argument Contact can lead to sql injection. The attack can be executed remotely. The exploit has been made available to the public and could 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: 2025-10-08

CVE-2025-11471

Descripción: A vulnerability was detected in SourceCodester Hotel and Lodge Management System 1.0. This affects an unknown function of the file /edit_customer.php. The manipulation of the argument ID results in sql injection. The attack may be performed from remote. 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: 2025-10-08

CVE-2025-11472

Descripción: A flaw has been found in SourceCodester Hotel and Lodge Management System 1.0. This impacts an unknown function of the file /edit_room.php. This manipulation of the argument ID causes sql injection. It is possible to initiate 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: 2025-10-08

CVE-2025-11473

Descripción: A vulnerability has been found in SourceCodester Hotel and Lodge Management System 1.0. Affected is an unknown function of the file /edit_curr.php. Such manipulation of the argument currsymbol 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: 2025-10-08

CVE-2025-11474

Descripción: A vulnerability was found in SourceCodester Hotel and Lodge Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /edit_booking.php. Performing manipulation of the argument Name results in sql injection. The attack can be initiated remotely. The exploit has been made public and could 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: 2025-10-08

CVE-2025-11475

Descripción: A vulnerability was determined in projectworlds Advanced Library Management System 1.0. Affected by this issue is some unknown functionality of the file /view_member.php. Executing manipulation of the argument user_id can lead to sql injection. The attack can 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: 2025-10-08

CVE-2025-11476

Descripción: A vulnerability was identified in SourceCodester Simple E-Commerce Bookstore 1.0. This affects an unknown part of the file /index.php. The manipulation of the argument login_username 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: 2025-10-08

CVE-2025-11477

Descripción: A security flaw has been discovered in SourceCodester Wedding Reservation Management System 1.0. This vulnerability affects unknown code of the file /global.php. The manipulation of the argument User results in sql injection. The attack may be launched 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: 2025-10-08

CVE-2025-11479

Descripción: A security vulnerability has been detected in SourceCodester Wedding Reservation Management System 1.0. Impacted is the function insertReservation of the file function.php. Such manipulation of the argument number leads to sql injection. The attack can be executed 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: 2025-10-08

CVE-2025-11480

Descripción: A vulnerability was detected in SourceCodester Simple E-Commerce Bookstore 1.0. The affected element is an unknown function of the file /register.php. Performing manipulation of the argument register_username results in sql injection. The attack is possible to be carried out 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: 2025-10-08

CVE-2025-11481

Descripción: A flaw has been found in varunsardana004 Blood-Bank-And-Donation-Management-System up to dc9e0393d826fbc85fad9755b5bc12cba1919df2. The impacted element is an unknown function of the file /donate_blood.php. Executing manipulation of the argument fullname can lead to sql injection. The attack may be performed from remote. The exploit has been published and may be used. This product utilizes a rol...

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: 2025-10-08

CVE-2025-11486

Descripción: A vulnerability was identified in SourceCodester Farm Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /buyNow.php. Such manipulation of the argument Name leads to sql injection. The attack can be launched remotely. The exploit is publicly available and might 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: 2025-10-08

CVE-2025-11487

Descripción: A security flaw has been discovered in SourceCodester Farm Management System 1.0. Affected by this issue is some unknown functionality of the file /uploadProduct.php. Performing manipulation of the argument Type results in sql injection. The attack may be initiated 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: 2025-10-08

CVE-2025-11503

Descripción: A vulnerability was determined in PHPGurukul Beauty Parlour Management System 1.1. This issue affects some unknown processing of the file /admin/manage-services.php. Executing manipulation of the argument delid 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: 2025-10-08

CVE-2025-11505

Descripción: A vulnerability was identified in PHPGurukul Beauty Parlour Management System 1.1. Impacted is an unknown function of the file /admin/new-appointment.php. The manipulation of the argument delid 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: 2025-10-08

CVE-2025-11506

Descripción: A security flaw has been discovered in PHPGurukul Beauty Parlour Management System 1.1. The affected element is an unknown function of the file /admin/search-appointment.php. The manipulation of the argument searchdata 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: 2025-10-08

CVE-2025-11507

Descripción: A weakness has been identified in PHPGurukul Beauty Parlour Management System 1.1. The impacted element is an unknown function of the file /admin/search-invoices.php. This manipulation of the argument searchdata 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: 2025-10-08

CVE-2025-11508

Descripción: A security vulnerability has been detected in code-projects Voting System 1.0. This affects an unknown function of the file /admin/voters_add.php. Such manipulation of the argument photo leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.

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-284

Tecnología: No especificado

Publicado el: 2025-10-08

CVE-2025-11509

Descripción: A vulnerability was detected in code-projects E-Commerce Website 1.0. This impacts an unknown function of the file /pages/product_add.php. Performing manipulation of the argument prod_name results in sql injection. The attack may be initiated remotely. The exploit is now 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: 2025-10-08

CVE-2025-11511

Descripción: A flaw has been found in code-projects E-Commerce Website 1.0. Affected is an unknown function of the file /pages/supplier_add.php. Executing manipulation of the argument supp_email can lead to sql injection. The attack may be launched remotely. The exploit has been published 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: 2025-10-08

CVE-2025-11513

Descripción: A vulnerability was determined in code-projects E-Commerce Website 1.0. This affects an unknown part of the file /pages/supplier_update.php. This manipulation of the argument supp_id causes sql injection. 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-74

Tecnología: No especificado

Publicado el: 2025-10-09

CVE-2025-10586

Descripción: The Community Events plugin for WordPress is vulnerable to SQL Injection via the 'event_venue' parameter in all versions up to, and including, 1.5.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries ...

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: 2025-10-09

CVE-2025-7526

Descripción: The WP Travel Engine – Tour Booking Plugin – Tour Operator Software plugin for WordPress is vulnerable to arbitrary file deletion (via renaming) due to insufficient file path validation in the set_user_profile_image function in all versions up to, and including, 6.6.7. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote c...

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: 2025-10-09

CVE-2025-7634

Descripción: The WP Travel Engine – Tour Booking Plugin – Tour Operator Software plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 6.6.7 via the mode 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 c...

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: 2025-10-09

CVE-2025-11522

Descripción: The Search & Go - Directory WordPress Theme theme for WordPress is vulnerable to Authentication Bypass via account takeover in all versions up to, and including, 2.7. This is due to insufficient user validation in the search_and_go_elated_check_facebook_user() function This makes it possible for unauthenticated attackers to gain access to other user's accounts, including administrators, when Fa...

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: 2025-10-09

CVE-2025-59978

Descripción: An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Juniper Networks Junos Space allows an attacker to store script tags directly in web pages that, when viewed by another user, enable the attacker to execute commands with the target's administrative permissions. This issue affects all versions of Junos Space before 24.1R4.

CVSS: 9.0 (CRITICAL)

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

Tipo: CWE-79

Tecnología: No especificado

Publicado el: 2025-10-09

CVE-2025-59218

Descripción: Azure Entra ID Elevation of Privilege Vulnerability

CVSS: 9.6 (CRITICAL)

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

Tipo: CWE-284

Tecnología: No especificado

Publicado el: 2025-10-09

CVE-2025-59246

Descripción: Azure Entra ID Elevation of Privilege 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-306

Tecnología: No especificado

Publicado el: 2025-10-09

CVE-2025-11533

Descripción: The WP Freeio plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.2.21. This is due to the process_register() function not restricting what user roles a user can register with. This makes it possible for unauthenticated attackers to supply the 'administrator' role during registration and gain administrator access to the site.

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: 2025-10-11

CVE-2025-6553

Descripción: The Ovatheme Events Manager plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the process_checkout() function in all versions up to, and including, 1.8.5. 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: 2025-10-11

CVE-2025-6439

Descripción: The WooCommerce Designer Pro plugin for WordPress, used by the Pricom - Printing Company & Design Services WordPress theme, is vulnerable to arbitrary file deletion due to insufficient file path validation in the 'wcdp_save_canvas_design_ajax' function in all versions up to, and including, 1.9.26. This makes it possible for unauthenticated attackers to delete all files in an arbitrary directory...

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: 2025-10-11

CVE-2025-42910

Descripción: Due to missing verification of file type or content, SAP Supplier Relationship Management allows an authenticated attacker to upload arbitrary files. These files could include executables which might be downloaded and executed by the user which could host malware. On successful exploitation an attacker could cause high impact on confidentiality, integrity and availability of the application.

CVSS: 9.0 (CRITICAL)

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

Tipo: CWE-434

Tecnología: No especificado

Publicado el: 2025-10-14

CVE-2025-42937

Descripción: SAP Print Service (SAPSprint) performs insufficient validation of path information provided by users. An unauthenticated attacker could traverse to the parent directory and over-write system files causing high impact on confidentiality integrity and availability of the application.

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-35

Tecnología: No especificado

Publicado el: 2025-10-14

CVE-2025-40765

Descripción: A vulnerability has been identified in TeleControl Server Basic V3.1 (All versions >= V3.1.2.2 < V3.1.2.3). The affected application contains an information disclosure vulnerability. This could allow an unauthenticated remote attacker to obtain password hashes of users and to login to and perform authenticated operations of the database service.

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: 2025-10-14

CVE-2025-40771

Descripción: A vulnerability has been identified in SIMATIC CP 1542SP-1 (6GK7542-6UX00-0XE0) (All versions < V2.4.24), SIMATIC CP 1542SP-1 IRC (6GK7542-6VX00-0XE0) (All versions < V2.4.24), SIMATIC CP 1543SP-1 (6GK7543-6WX00-0XE0) (All versions < V2.4.24), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (6AG2542-6VX00-4XE0) (All versions < V2.4.24), SIPLUS ET 200SP CP 1543SP-1 ISEC (6AG1543-6WX00-7XE0) (All version...

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: 2025-10-14

CVE-2025-10610

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in SFS Consulting Information Processing Industry and Foreign Trade Inc. Winsure allows Blind SQL Injection.This issue affects Winsure: through Version dated 21.08.2025.

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: 2025-10-14

Resumen del Reporte

CVEs analizados: 53

Promedio CVSS: 7.82

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat