CVEs más relevantes de la semana

Del 30/09/2025 al 07/10/2025

Porque el primer paso para defender es conocer las amenazas.

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-2025-59681

Descripción: An issue was discovered in Django 4.2 before 4.2.25, 5.1 before 5.1.13, and 5.2 before 5.2.7. QuerySet.annotate(), QuerySet.alias(), QuerySet.aggregate(), and QuerySet.extra() are subject to SQL injection in column aliases, when using a suitably crafted dictionary, with dictionary expansion, as the **kwargs passed to these methods (on MySQL and MariaDB).

CVSS: 7.1 (HIGH)

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

Tipo: CWE-89

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-2025-61603

Descripción: WeGIA is a Web manager for charitable institutions. Versions 3.4.12 and below include an SQL Injection vulnerability which was identified in the /controle/control.php endpoint, specifically in the descricao parameter. This vulnerability allows attackers to execute arbitrary SQL commands, compromising the confidentiality, integrity, and availability of the database. This issue is fixed in versio...

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-2025-61605

Descripción: WeGIA is an open source web manager with a focus on charitable institutions. Versions 3.4.12 and below contain an SQL Injection vulnerability which was identified in the /pet/profile_pet.php endpoint, specifically in the id_pet parameter. This vulnerability allows attackers to execute arbitrary SQL commands, compromising the confidentiality, integrity, and availability of the database. 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-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-2025-49844

Descripción: Redis is an open source, in-memory database that persists on disk. Versions 8.2.1 and below allow an authenticated user to use a specially crafted Lua script to manipulate the garbage collector, trigger a use-after-free and potentially lead to remote code execution. The problem exists in all versions of Redis with Lua scripting. This issue is fixed in version 8.2.2. To workaround this issue wit...

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-416

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

CVE-2025-11334

Descripción: A security flaw has been discovered in Campcodes Online Apartment Visitor Management System 1.0. Affected is an unknown function of the file /visitor-detail.php. The manipulation of the argument editid 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: 2025-10-06

CVE-2023-49886

Descripción: IBM Standards Processing Engine 10.0.1.10 could allow a remote attacker to execute arbitrary code on the system, caused by an unsafe java deserialization. By sending specially crafted input, an attacker could exploit this vulnerability to execute arbitrary code on the system.

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: 2025-10-06

CVE-2025-36356

Descripción: IBM Security Verify Access and IBM Security Verify Access Docker 10.0.0.0 through 10.0.9.0 and 11.0.0.0 through 11.0.1.0 could allow a locally authenticated user to escalate their privileges to root due to execution with more privileges than required.

CVSS: 9.3 (CRITICAL)

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

Tipo: CWE-250

Tecnología: No especificado

Publicado el: 2025-10-06

CVE-2025-0603

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Callvision Healthcare Callvision Emergency Code allows SQL Injection, Blind SQL Injection.This issue affects Callvision Emergency Code: before V3.0.

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: 2025-10-07

Resumen del Reporte

CVEs analizados: 24

Promedio CVSS: 9.51

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat