CVEs más relevantes de la semana

Del 29/11/2025 al 06/12/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-13615

Descripción: The StreamTube Core plugin for WordPress is vulnerable to Arbitrary User Password Change in versions up to, and including, 4.78. 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. Note...

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: 2025-11-30

CVE-2025-13787

Descripción: A flaw has been found in ZenTao up to 21.7.6-8564. The affected element is the function file::delete of the file module/file/control.php of the component File Handler. Executing manipulation of the argument fileID can lead to improper privilege management. It is possible to launch the attack remotely. Upgrading to version 21.7.7 is sufficient to fix this issue. You should upgrade the affected c...

CVSS: 5.4 (MEDIUM)

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

Tipo: CWE-266

Tecnología: No especificado

Publicado el: 2025-11-30

CVE-2025-13788

Descripción: A vulnerability has been found in Chanjet CRM up to 20251106. The impacted element is an unknown function of the file /tools/upgradeattribute.php. The manipulation of the argument gblOrgID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.

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: 2025-11-30

CVE-2025-13814

Descripción: A security flaw has been discovered in moxi159753 Mogu Blog v2 up to 5.2. Impacted is the function LocalFileServiceImpl.uploadPictureByUrl of the file /file/uploadPicsByUrl. The manipulation results in server-side request forgery. The attack can be launched remotely. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did no...

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-918

Tecnología: No especificado

Publicado el: 2025-12-01

CVE-2025-13815

Descripción: A weakness has been identified in moxi159753 Mogu Blog v2 up to 5.2. The affected element is an unknown function of the file /file/pictures. This manipulation of the argument filedatas causes unrestricted upload. The attack may be initiated remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond...

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-284

Tecnología: No especificado

Publicado el: 2025-12-01

CVE-2025-63531

Descripción: A SQL injection vulnerability exists in the Blood Bank Management System 1.0 within the receiverLogin.php component. The application fails to properly sanitize user-supplied input in SQL queries, allowing an attacker to inject arbitrary SQL code. By manipulating the remail and rpassword fields, an attacker can bypass authentication and gain unauthorized access to the system.

CVSS: 10.0 (CRITICAL)

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

Tipo: CWE-89

Tecnología: No especificado

Publicado el: 2025-12-01

CVE-2025-66205

Descripción: Frappe is a full-stack web application framework. Prior to 15.86.0 and 14.99.2, a certain endpoint was vulnerable to error-based SQL injection due to lack of validation of parameters. Some information like version could be retrieved. This vulnerability is fixed in 15.86.0 and 14.99.2.

CVSS: 7.1 (HIGH)

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

Tipo: CWE-89

Tecnología: No especificado

Publicado el: 2025-12-01

CVE-2025-66301

Descripción: Grav is a file-based Web platform. Prior to 1.8.0-beta.27, due to improper authorization checks when modifying critical fields on a POST request to /admin/pages/{page_name}, an editor with only permissions to change basic content on the form is now able to change the functioning of the form through modifying the content of the data[_json][header][form] which is the YAML frontmatter which includ...

CVSS: 9.6 (CRITICAL)

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

Tipo: CWE-285

Tecnología: No especificado

Publicado el: 2025-12-01

CVE-2025-13872

Descripción: Blind Server-Side Request Forgery (SSRF) in the survey-import feature of

ObjectPlanet Opinio 7.26 rev12562 on

Web-based platforms allows an attacker to force the server to perform HTTP GET requests via crafted import requests

to an arbitrary destination.

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-918

Tecnología: No especificado

Publicado el: 2025-12-02

CVE-2025-41742

Descripción: Sprecher Automations SPRECON-E-C, SPRECON-E-P, SPRECON-E-T3 is vulnerable to attack by an unauthorized remote attacker via default cryptographic keys. The use of these keys allows the attacker to read, modify, and write projects and data, or to access any device via remote maintenance.

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-1394

Tecnología: No especificado

Publicado el: 2025-12-02

CVE-2025-41744

Descripción: Sprecher Automations SPRECON-E series uses default cryptographic keys that allow an unprivileged remote attacker to access all encrypted communications, thereby compromising confidentiality and integrity.

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-1394

Tecnología: No especificado

Publicado el: 2025-12-02

CVE-2025-11778

Descripción: Stack-based buffer overflow in Circutor SGE-PLC1000/SGE-PLC50 v0.9.2. This vulnerability allows an attacker to remotely exploit memory corruption through the 'read_packet()' function of the TACACSPLUS implementation.

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-122

Tecnología: No especificado

Publicado el: 2025-12-02

CVE-2025-11779

Descripción: Stack-based buffer overflow vulnerability in CircutorSGE-PLC1000/SGE-PLC50 v9.0.2. The 'SetLan' function is invoked when a new configuration is applied. This new configuration function is activated by a management web request, which can be invoked by a user when making changes to the 'index.cgi' web application. The parameters are not being sanitised, which could lead to command injection.

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: 2025-12-02

CVE-2025-11780

Descripción: Stack-based buffer overflow vulnerability in Circutor SGE-PLC1000/SGE-PLC50 v9.0.2. In the 'showMeterReport()' function, there is an unlimited user input that is copied to a fixed-size buffer via 'sprintf()'. The 'GetParameter(meter)' function retrieves the user input, which is directly incorporated into a buffer without size validation. An attacker can provide an excessively large input for 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-120

Tecnología: No especificado

Publicado el: 2025-12-02

CVE-2025-11782

Descripción: Stack-based buffer overflow vulnerability in Circutor SGE-PLC1000/SGE-PLC50 v9.0.2. The 'ShowDownload()' function uses “sprintf()” to format a string that includes the user-controlled input of 'GetParameter(meter)' in the fixed-size buffer 'acStack_4c' (64 bytes) without checking the length. An attacker can provide an excessively long value for the 'meter' parameter that exceeds the 64-byte buf...

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: 2025-12-02

CVE-2025-11783

Descripción: Stack-based buffer overflow vulnerability in Circutor SGE-PLC1000/SGE-PLC50 v9.0.2. The vulnerability is found in the 'AddEvent()' function when copying the user-controlled username input to a fixed-size buffer (48 bytes) without boundary checking. This can lead to memory corruption, resulting in possible remote code execution.

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: 2025-12-02

CVE-2025-11784

Descripción: Stack-based buffer overflow vulnerability in Circutor SGE-PLC1000/SGE-PLC50 v9.0.2. In the 'ShowMeterDatabase()' function, there is an unlimited user input that is copied to a fixed-size buffer via 'sprintf()'. The 'GetParameter(meter)' function retrieves the user input, which is directly incorporated into a buffer without size validation. An attacker can provide an excessively large input for ...

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: 2025-12-02

CVE-2025-11785

Descripción: Stack-based buffer overflow vulnerability in Circutor SGE-PLC1000/SGE-PLC50 v9.0.2. In the 'ShowMeterPasswords()' function, there is an unlimited user input that is copied to a fixed-size buffer via 'sprintf()'. The 'GetParameter(meter)' function retrieves the user input, which is directly incorporated into a buffer without size validation. An attacker can provide an excessively large input for...

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: 2025-12-02

CVE-2025-11786

Descripción: Stack-based buffer overflow vulnerability in Circutor SGE-PLC1000/SGE-PLC50 v9.0.2. In the 'SetUserPassword()' function, the 'newPassword' parameter is directly embedded in a shell command string using 'sprintf()' without any sanitisation or validation, and then executed using 'system()'. This allows an attacker to inject arbitrary shell commands that will be executed with the same privileges a...

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: 2025-12-02

CVE-2025-11788

Descripción: Heap-based buffer overflow vulnerability in Circutor SGE-PLC1000/SGE-PLC50 v9.0.2. In the 'ShowSupervisorParameters()' function, there is an unlimited user input that is copied to a fixed-size buffer via 'sprintf()'. The 'GetParameter(meter)' function retrieves the user input, which is directly incorporated into a buffer without size validation. An attacker can provide an excessively large inpu...

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-122

Tecnología: No especificado

Publicado el: 2025-12-02

CVE-2025-41013

Descripción: SQL injection vulnerability in TCMAN GIM v11 in version 20250304. This vulnerability allows an attacker to retrieve, create, update, and delete databases by sending a GET request using the 'idmant' parameter in '/PC/frmEPIS.aspx'.

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: 2025-12-02

CVE-2025-13542

Descripción: The DesignThemes LMS plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.0.4. This is due to the 'dtlms_register_user_front_end' 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: 2025-12-02

CVE-2025-13486

Descripción: The Advanced Custom Fields: Extended plugin for WordPress is vulnerable to Remote Code Execution in versions 0.9.0.5 through 0.9.1.1 via the prepare_form() function. This is due to the function accepting user input and then passing that through call_user_func_array(). This makes it possible for unauthenticated attackers to execute arbitrary code on the server, which can be leveraged to inject b...

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-94

Tecnología: No especificado

Publicado el: 2025-12-03

CVE-2025-13342

Descripción: The Frontend Admin by DynamiApps plugin for WordPress is vulnerable to unauthorized modification of arbitrary WordPress options in all versions up to, and including, 3.28.20. This is due to insufficient capability checks and input validation in the ActionOptions::run() save handler. This makes it possible for unauthenticated attackers to modify critical WordPress options such as users_can_regis...

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: 2025-12-03

CVE-2025-66032

Descripción: Claude Code is an agentic coding tool. Prior to 1.0.93, Due to errors in parsing shell commands related to $IFS and short CLI flags, it was possible to bypass the Claude Code read-only validation and trigger arbitrary code execution. Reliably exploiting this requires the ability to add untrusted content into a Claude Code context window. This vulnerability is fixed in 1.0.93.

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: 2025-12-03

CVE-2025-66222

Descripción: DeepChat is a smart assistant uses artificial intelligence. In 0.5.0 and earlier, there is a Stored Cross-Site Scripting (XSS) vulnerability in the Mermaid diagram renderer allows an attacker to execute arbitrary JavaScript within the application context. By leveraging the exposed Electron IPC bridge, this XSS can be escalated to Remote Code Execution (RCE) by registering and starting a malicio...

CVSS: 9.6 (CRITICAL)

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

Tipo: CWE-94

Tecnología: No especificado

Publicado el: 2025-12-03

CVE-2024-45538

Descripción: Cross-Site Request Forgery (CSRF) vulnerability in WebAPI Framework in Synology DiskStation Manager (DSM) before 7.2.1-69057-2 and 7.2.2-72806 and Synology Unified Controller (DSMUC) before 3.1.4-23079 allows remote attackers to execute arbitrary code via unspecified vectors.

CVSS: 9.6 (CRITICAL)

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

Tipo: CWE-352

Tecnología: No especificado

Publicado el: 2025-12-04

CVE-2025-13313

Descripción: The CRM Memberships plugin for WordPress is vulnerable to privilege escalation via password reset in all versions up to, and including, 2.5. This is due to missing authorization and authentication checks on the `ntzcrm_changepassword` AJAX action. This makes it possible for unauthenticated attackers to reset arbitrary user passwords and gain unauthorized access to user accounts via the `ntzcrm_...

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: 2025-12-05

CVE-2025-12374

Descripción: The Email Verification, Email OTP, Block Spam Email, Passwordless login, Hide Login, Magic Login – User Verification plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 2.0.39. This is due to the plugin not properly validating that an OTP was generated before comparing it to user input in the "user_verification_form_wrap_process_otpLogin" function. ...

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-287

Tecnología: No especificado

Publicado el: 2025-12-05

CVE-2025-12673

Descripción: The Flex QR Code Generator plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the update_qr_code() function in all versions up to, and including, 1.2.6. 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: 2025-12-06

CVE-2025-13377

Descripción: The 10Web Booster – Website speed optimization, Cache & Page Speed optimizer plugin for WordPress is vulnerable to arbitrary folder deletion due to insufficient file path validation in the get_cache_dir_for_page_from_url() function in all versions up to, and including, 2.32.7. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary folders...

CVSS: 9.6 (CRITICAL)

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

Tipo: CWE-22

Tecnología: No especificado

Publicado el: 2025-12-06

Resumen del Reporte

CVEs analizados: 31

Promedio CVSS: 9.23

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat ▯