CVEs más relevantes de la semana

Del 01/11/2025 al 08/11/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-12602

Descripción: /etc/avahi/services/z9.service can be Arbitrarily Written.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.

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-787

Tecnología: No especificado

Publicado el: 2025-11-01

CVE-2025-12603

Descripción: /etc/timezone can be Arbitrarily Written.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.

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-787

Tecnología: No especificado

Publicado el: 2025-11-01

CVE-2025-12595

Descripción: A weakness has been identified in Tenda AC23 16.03.07.52. This impacts the function formSetVirtualSer of the file /goform/SetVirtualServerCfg. This manipulation of the argument list causes buffer overflow. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be exploited.

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: 2025-11-02

CVE-2025-12596

Descripción: A security vulnerability has been detected in Tenda AC23 16.03.07.52. Affected is the function saveParentControlInfo of the file /goform/saveParentControlInfo. Such manipulation of the argument Time leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.

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: 2025-11-02

CVE-2025-12597

Descripción: A vulnerability was detected in SourceCodester Best House Rental Management System 1.0. Affected by this vulnerability is the function save_category of the file /admin_class.php. Performing manipulation of the argument Name results in sql injection. The attack can be initiated remotely. The exploit is now public 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-74

Tecnología: No especificado

Publicado el: 2025-11-02

CVE-2025-12598

Descripción: A flaw has been found in SourceCodester Best House Rental Management System 1.0. Affected by this issue is the function save_tenant of the file /admin_class.php. Executing manipulation of the argument firstname can lead to sql injection. The attack can be launched remotely. The exploit has been published and may be used. Other parameters might be affected as well.

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: 2025-11-02

CVE-2025-12604

Descripción: A vulnerability has been found in itsourcecode Online Loan Management System 1.0. This affects an unknown part of the file /load_fields.php. The manipulation of the argument loan_id leads to sql injection. The attack may be initiated 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: 2025-11-02

CVE-2025-12605

Descripción: A vulnerability was found in itsourcecode Online Loan Management System 1.0. This vulnerability affects unknown code of the file /manage_loan.php. The manipulation of the argument ID results in sql injection. The attack may be launched 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: 2025-11-02

CVE-2025-12606

Descripción: A vulnerability was determined in itsourcecode Online Loan Management System 1.0. This issue affects some unknown processing of the file /manage_borrower.php. This manipulation of the argument ID causes sql injection. Remote exploitation of the attack is possible. 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: 2025-11-03

CVE-2025-12607

Descripción: A vulnerability was identified in itsourcecode Online Loan Management System 1.0. Impacted is an unknown function of the file /manage_payment.php. Such manipulation of the argument ID leads to sql injection. The attack can be executed 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: 2025-11-03

CVE-2025-12608

Descripción: A security flaw has been discovered in itsourcecode Online Loan Management System 1.0. The affected element is an unknown function of the file /manage_user.php. Performing manipulation of the argument ID 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: 2025-11-03

CVE-2025-12611

Descripción: A vulnerability was identified in Tenda AC21 16.03.08.16. This vulnerability affects the function formSetPPTPServer of the file /goform/SetPptpServerCfg. The manipulation of the argument startIp leads to buffer overflow. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.

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: 2025-11-03

CVE-2025-12612

Descripción: A security flaw has been discovered in Campcodes School Fees Payment Management System 1.0. This issue affects some unknown processing of the file /ajax.php. The manipulation results in sql injection. The attack can be executed 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: 2025-11-03

CVE-2025-12614

Descripción: A weakness has been identified in SourceCodester Best House Rental Management System 1.0. Impacted is the function delete_payment of the file /admin_class.php. This manipulation of the argument ID causes sql injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be exploited.

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: 2025-11-03

CVE-2025-12617

Descripción: A flaw has been found in itsourcecode Billing System 1.0. This affects an unknown function of the file /admin/app/login_crud.php. Executing manipulation of the argument Password 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: 2025-11-03

CVE-2025-12618

Descripción: A vulnerability has been found in Tenda AC8 16.03.34.06. This impacts an unknown function of the file /goform/DatabaseIniSet. The manipulation of the argument Time leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.

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: 2025-11-03

CVE-2025-12619

Descripción: A vulnerability was found in Tenda A15 15.13.07.13. Affected is the function fromSetWirelessRepeat of the file /goform/openNetworkGateway. The manipulation of the argument wpapsk_crypto2_4g results in buffer overflow. The attack can be launched remotely. The exploit has been made public and could be used.

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: 2025-11-03

CVE-2025-12622

Descripción: A vulnerability was determined in Tenda AC10 16.03.10.13. Affected by this vulnerability is the function formSysRunCmd of the file /goform/SysRunCmd. This manipulation of the argument getui causes buffer overflow. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.

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: 2025-11-03

CVE-2025-0987

Descripción: Authorization Bypass Through User-Controlled Key vulnerability in CB Project Ltd. Co. CVLand allows Parameter Injection.This issue affects CVLand: from 2.1.0 through 20251103.

CVSS: 9.9 (CRITICAL)

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

Tipo: CWE-639

Tecnología: No especificado

Publicado el: 2025-11-03

CVE-2025-8900

Descripción: The Doccure Core plugin for WordPress is vulnerable to privilege escalation in versions up to, and excluding, 1.5.4. This is due to the plugin allowing users who are registering new accounts to set their own role or by supplying 'user_type' field. This makes it possible for unauthenticated attackers to gain elevated privileges by creating an account with the administrator role.

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: 2025-11-03

CVE-2025-12531

Descripción: IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources.

CVSS: 7.1 (HIGH)

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

Tipo: CWE-611

Tecnología: No especificado

Publicado el: 2025-11-03

CVE-2025-11007

Descripción: The CE21 Suite plugin for WordPress is vulnerable to unauthorized plugin settings update due to a missing capability check on the wp_ajax_nopriv_ce21_single_sign_on_save_api_settings AJAX action in versions 2.2.1 to 2.3.1. This makes it possible for unauthenticated attackers to update the plugin's API settings including a secret key used for authentication. This allows unauthenticated attackers...

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: 2025-11-04

CVE-2025-11008

Descripción: The CE21 Suite plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.3.1 via the log file. This makes it possible for unauthenticated attackers to extract sensitive data including authentication credentials, which can be used to log in as other users as long as they have used the plugin's custom authentication feature before. This may inclu...

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-532

Tecnología: No especificado

Publicado el: 2025-11-04

CVE-2025-12158

Descripción: The Simple User Capabilities plugin for WordPress is vulnerable to Privilege Escalation due to a missing capability check on the suc_submit_capabilities() function in all versions up to, and including, 1.0. This makes it possible for unauthenticated attackers to elevate the role of any user account to administrator.

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: 2025-11-04

CVE-2025-12493

Descripción: The ShopLentor – WooCommerce Builder for Elementor & Gutenberg +21 Modules – All in One Solution (formerly WooLentor) plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 3.2.5 via the 'load_template' function. This makes it possible for unauthenticated attackers to include and execute arbitrary .php files on the server, allowing the execution of any ...

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: 2025-11-04

CVE-2025-12682

Descripción: The Easy Upload Files During Checkout plugin for WordPress is vulnerable to arbitrary JavaScript file uploads due to missing file type validation in the 'file_during_checkout' function in all versions up to, and including, 2.9.8. This makes it possible for unauthenticated attackers to upload arbitrary JavaScript 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: 2025-11-04

CVE-2025-11749

Descripción: The AI Engine plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.1.3 via the /mcp/v1/ REST API endpoint that exposes the 'Bearer Token' value when 'No-Auth URL' is enabled. This makes it possible for unauthenticated attackers to extract the bearer token, which can be used to gain access to a valid session and perform many actions like cr...

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: 2025-11-05

CVE-2025-12674

Descripción: The KiotViet Sync plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the create_media() 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: 2025-11-05

CVE-2025-47151

Descripción: A type confusion vulnerability exists in the lasso_node_impl_init_from_xml functionality of Entr'ouvert Lasso 2.5.1 and 2.8.2. A specially crafted SAML response can lead to an arbitrary code execution. An attacker can send a malformed SAML response to trigger this 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-843

Tecnología: No especificado

Publicado el: 2025-11-05

CVE-2025-20354

Descripción: A vulnerability in the Java Remote Method Invocation (RMI) process of Cisco Unified CCX could allow an unauthenticated, remote attacker to upload arbitrary files and execute arbitrary commands with root permissions on an affected system. This vulnerability is due to improper authentication mechanisms that are associated to specific Cisco Unified CCX features. An attacker could exploit this v...

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: 2025-11-05

CVE-2025-20358

Descripción: A vulnerability in the Contact Center Express (CCX) Editor application of Cisco Unified CCX could allow an unauthenticated, remote attacker to bypass authentication and obtain administrative permissions pertaining to script creation and execution. This vulnerability is due to improper authentication mechanisms in the communication between the CCX Editor and an affected Unified CCX server. An...

CVSS: 9.4 (CRITICAL)

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

Tipo: CWE-306

Tecnología: No especificado

Publicado el: 2025-11-05

CVE-2025-45378

Descripción: Dell CloudLink, versions 8.0 through 8.1.2, contain vulnerability on restricted shell. A Privileged user with known password can break into command shell of CloudLink server and gain access of shell and escalate privilege, gain unauthorized access of system.

If ssh is enabled with web credentials of server, attack is possible through network with known privileged user/password.

CVSS: 9.1 (CRITICAL)

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

Tipo: CWE-78

Tecnología: No especificado

Publicado el: 2025-11-05

CVE-2025-64163

Descripción: DataEase is an open source data visualization analysis tool. In versions 2.10.14 and below, the vendor added a blacklist to filter ldap:// and ldaps://. However, omission of protection for the dns:// protocol results in an SSRF vulnerability. This issue is fixed in version 2.10.15.

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: 2025-11-06

CVE-2025-64164

Descripción: Dataease is an open source data visualization analysis tool. In versions 2.10.14 and below, DataEase did not properly filter when establishing JDBC connections to Oracle, resulting in a risk of JNDI injection (Java Naming and Directory Interface injection). This issue is fixed in version 2.10.15.

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: 2025-11-06

CVE-2025-27918

Descripción: An issue was discovered in AnyDesk before 9.0.0. It has an integer overflow and resultant heap-based buffer overflow via a UDP packet during processing of an Identity user image within the Discovery feature, or when establishing a connection between any two clients.

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-190

Tecnología: No especificado

Publicado el: 2025-11-06

CVE-2025-12352

Descripción: The Gravity Forms plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the copy_post_image() function in all versions up to, and including, 2.9.20. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. This only impacts sites that have allow_url_fo...

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: 2025-11-07

CVE-2025-10230

Descripción: A flaw was found in Samba, in the front-end WINS hook handling: NetBIOS names from registration packets are passed to a shell without proper validation or escaping. Unsanitized NetBIOS name data from WINS registration packets are inserted into a shell command and executed by the Samba Active Directory Domain Controller's wins hook, allowing an unauthenticated network attacker to achieve remote ...

CVSS: 10.0 (CRITICAL)

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

Tipo: CWE-78

Tecnología: No especificado

Publicado el: 2025-11-07

Resumen del Reporte

CVEs analizados: 37

Promedio CVSS: 8.63

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat