CVEs más relevantes de la semana

Del 11/10/2025 al 18/10/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-11656

Descripción: A weakness has been identified in ProjectsAndPrograms School Management System up to 6b6fae5426044f89c08d0dd101c7fa71f9042a59. This affects an unknown function of the file /assets/editNotes.php. Executing manipulation of the argument File can lead to unrestricted upload. The attack can be launched remotely. The exploit has been made available to the public and could be exploited. This product d...

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-284

Tecnología: No especificado

Publicado el: 2025-10-13

CVE-2025-11657

Descripción: A security vulnerability has been detected in ProjectsAndPrograms School Management System up to 6b6fae5426044f89c08d0dd101c7fa71f9042a59. This impacts an unknown function of the file /assets/createNotice.php. The manipulation of the argument File leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used. This product uses a roll...

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-284

Tecnología: No especificado

Publicado el: 2025-10-13

CVE-2025-11658

Descripción: A vulnerability was detected in ProjectsAndPrograms School Management System up to 6b6fae5426044f89c08d0dd101c7fa71f9042a59. Affected is an unknown function of the file /assets/changeSllyabus.php. The manipulation of the argument File results in unrestricted upload. The attack may be launched remotely. The exploit is now public and may be used. This product operates on a rolling release basis, ...

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-284

Tecnología: No especificado

Publicado el: 2025-10-13

CVE-2025-11659

Descripción: A flaw has been found in ProjectsAndPrograms School Management System up to 6b6fae5426044f89c08d0dd101c7fa71f9042a59. Affected by this vulnerability is an unknown functionality of the file /assets/uploadNotes.php. This manipulation of the argument File causes unrestricted upload. Remote exploitation of the attack is possible. The exploit has been published and may be used. This product follows ...

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-284

Tecnología: No especificado

Publicado el: 2025-10-13

CVE-2025-11661

Descripción: A vulnerability was found in ProjectsAndPrograms School Management System up to 6b6fae5426044f89c08d0dd101c7fa71f9042a59. This affects an unknown part. Performing manipulation results in missing authentication. The attack is possible to be carried out remotely. The exploit has been made public and could be used. This product adopts a rolling release strategy to maintain continuous delivery

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-287

Tecnología: No especificado

Publicado el: 2025-10-13

CVE-2025-11662

Descripción: A security flaw has been discovered in SourceCodester Best Salon Management System 1.0. Impacted is an unknown function of the file /booking.php. The manipulation of the argument serv_id 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: 2025-10-13

CVE-2025-11664

Descripción: A security vulnerability has been detected in Campcodes Online Beauty Parlor Management System 1.0. The impacted element is an unknown function of the file /admin/search-appointment.php. Such manipulation of the argument searchdata leads to sql injection. 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-74

Tecnología: No especificado

Publicado el: 2025-10-13

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

CVE-2025-11717

Descripción: When switching between Android apps using the card carousel Firefox shows a black screen as its card image when a password-related screen was the last one being used. Prior to Firefox 144 the password edit screen was visible. This vulnerability affects Firefox < 144.

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-200

Tecnología: No especificado

Publicado el: 2025-10-14

CVE-2025-11719

Descripción: Starting in Firefox 143, the use of the native messaging API by web extensions on Windows could lead to crashes caused by use-after-free memory corruption. This vulnerability affects Firefox < 144 and Thunderbird < 144.

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-416

Tecnología: No especificado

Publicado el: 2025-10-14

CVE-2025-11721

Descripción: Memory safety bug present in Firefox 143 and Thunderbird 143. This bug showed evidence of memory corruption and we presume that with enough effort this could have been exploited to run arbitrary code. This vulnerability affects Firefox < 144 and Thunderbird < 144.

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: 2025-10-14

CVE-2024-33507

Descripción: An insufficient session expiration vulnerability [CWE-613] and an incorrect authorization vulnerability [CWE-863] in FortiIsolator 2.4.0 through 2.4.4, 2.3 all versions, 2.2.0, 2.1 all versions, 2.0 all versions authentication mechanism may allow remote unauthenticated attacker to deauthenticate logged in admins via crafted cookie and remote authenticated read-only attacker to gain write privil...

CVSS: 7.4 (HIGH)

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

Tipo: CWE-613

Tecnología: No especificado

Publicado el: 2025-10-14

CVE-2025-49201

Descripción: A weak authentication in Fortinet FortiPAM 1.5.0, 1.4.0 through 1.4.2, 1.3.0 through 1.3.1, 1.2.0, 1.1.0 through 1.1.2, 1.0.0 through 1.0.3, FortiSwitchManager 7.2.0 through 7.2.4 allows attacker to execute unauthorized code or commands via specially crafted http requests

CVSS: 8.1 (HIGH)

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

Tipo: CWE-1390

Tecnología: No especificado

Publicado el: 2025-10-14

CVE-2025-49708

Descripción: Use after free in Microsoft Graphics Component allows an authorized attacker to elevate privileges over a network.

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: 2025-10-14

CVE-2025-55315

Descripción: Inconsistent interpretation of http requests ('http request/response smuggling') in ASP.NET Core allows an authorized attacker to bypass a security feature over a network.

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-444

Tecnología: No especificado

Publicado el: 2025-10-14

CVE-2025-59287

Descripción: Deserialization of untrusted data in Windows Server Update Service allows an unauthorized attacker to execute code over a network.

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: 2025-10-14

CVE-2025-11736

Descripción: A flaw has been found in itsourcecode Online Examination System 1.0. Affected by this issue is some unknown functionality of the file /index.php. This manipulation of the argument Username 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: 2025-10-14

CVE-2025-49553

Descripción: Adobe Connect versions 12.9 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be exploited by an attacker to execute malicious scripts in a victim's browser. Exploitation of this issue requires user interaction in that a victim must navigate to a crafted web page. A successful attacker can abuse this to achieve session takeover, increasing the confident...

CVSS: 9.3 (CRITICAL)

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

Tipo: CWE-79

Tecnología: No especificado

Publicado el: 2025-10-14

CVE-2025-10041

Descripción: The Flex QR Code Generator plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in thesave_qr_code_to_db() function in all versions up to, and including, 1.2.5. 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: 2025-10-15

CVE-2025-10294

Descripción: The OwnID Passwordless Login plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 1.3.4. This is due to the plugin not properly checking if the ownid_shared_secret value is empty prior to authenticating a user via JWT. This makes it possible for unauthenticated attackers to log in as other users, including administrators, on instances where the plugi...

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: 2025-10-15

CVE-2025-9967

Descripción: The Orion SMS OTP Verification plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 1.1.7. This is due to the plugin not properly validating a user's identity prior to updating their password. This makes it possible for unauthenticated attackers to change arbitrary user's password to a one-time password if the attacker knows the u...

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: 2025-10-15

CVE-2025-10742

Descripción: The Truelysell Core plugin for WordPress is vulnerable to Arbitrary User Password Change in versions up to, and including, 1.8.6. 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. Not...

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: 2025-10-16

CVE-2025-10850

Descripción: The Felan Framework plugin for WordPress is vulnerable to improper authentication in versions up to, and including, 1.1.4. This is due to the hardcoded password in the 'fb_ajax_login_or_register' function and in the 'google_ajax_login_or_register' function. This makes it possible for unauthenticated attackers to log in as any existing user on the site, if they registered with facebook or google...

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-798

Tecnología: No especificado

Publicado el: 2025-10-16

CVE-2025-11900

Descripción: The iSherlock developed by HGiga has an OS Command Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary OS commands and execute them on the server.

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: 2025-10-17

CVE-2017-20206

Descripción: The Appointments plugin for WordPress is vulnerable to PHP Object Injection in versions up to, and including, 2.2.1 via deserialization of untrusted input from the `wpmudev_appointments` cookie. This allows unauthenticated attackers to inject a PHP Object. Attackers were actively exploiting this vulnerability with the WP_Theme() class to create backdoors.

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: 2025-10-18

CVE-2017-20207

Descripción: The Flickr Gallery plugin for WordPress is vulnerable to PHP Object Injection in versions up to, and including, 1.5.2 via deserialization of untrusted input from the `pager ` parameter. This allows unauthenticated attackers to inject a PHP Object. Attackers were actively exploiting this vulnerability with the WP_Theme() class to create backdoors.

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: 2025-10-18

CVE-2017-20208

Descripción: The RegistrationMagic – Custom Registration Forms, User Registration, Payment, and User Login plugin for WordPress is vulnerable to PHP Object Injection in all versions up to 3.7.9.3 (exclusive) via deserialization of untrusted input from the is_expired_by_date() function. This makes it possible for unauthenticated attackers to inject a PHP Object. The additional presence of a POP chain allows ...

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: 2025-10-18

CVE-2025-11391

Descripción: The PPOM – Product Addons & Custom Fields for WooCommerce plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the image cropper functionality in all versions up to, and including, 33.0.15. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. Whil...

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: 2025-10-18

Resumen del Reporte

CVEs analizados: 32

Promedio CVSS: 8.91

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat ▯