CVEs más relevantes de la semana

Del 14/10/2025 al 21/10/2025

Porque el primer paso para defender es conocer las amenazas.

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-2025-11736

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-2025-41018

Descripción: SQL injection in Sergestec's Exito v8.0. This vulnerability allows an attacker to retrieve, create, update, and delete databases through the 'cat' parameter in '/public.php'.

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: 2025-10-16

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

CVE-2025-11948

Descripción: Document Management System developed by Excellent Infotek has an Arbitrary File Upload vulnerability, allowing unauthenticated remote attackers to upload and execute web shell backdoors, thereby enabling arbitrary code execution 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-434

Tecnología: No especificado

Publicado el: 2025-10-20

Resumen del Reporte

CVEs analizados: 16

Promedio CVSS: 9.62

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat