CVEs más relevantes de la semana

Del 22/11/2025 al 29/11/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-13556

Descripción: A flaw has been found in Campcodes Online Polling System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/checklogin.php. Executing manipulation of the argument myusername can lead to sql injection. The attack can be launched 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: 2025-11-23

CVE-2025-13557

Descripción: A vulnerability has been found in Campcodes Online Polling System 1.0. Affected by this issue is some unknown functionality of the file /registeracc.php. The manipulation of the argument email 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: 2025-11-23

CVE-2025-13560

Descripción: A vulnerability was found in SourceCodester Company Website CMS 1.0. This affects an unknown part of the file /admin/reset-password.php. The manipulation of the argument email 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: 2025-11-23

CVE-2025-13561

Descripción: A vulnerability was determined in SourceCodester Company Website CMS 1.0. This vulnerability affects unknown code of the file /admin/index.php. This manipulation of the argument Username 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: 2025-11-23

CVE-2025-13562

Descripción: A vulnerability was identified in D-Link DIR-852 1.00. This issue affects some unknown processing of the file /gena.cgi. Such manipulation of the argument service leads to command injection. The attack can be executed remotely. The exploit is publicly available and might be used. This vulnerability only affects products that are no longer supported by the maintainer.

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: 2025-11-23

CVE-2025-13565

Descripción: A weakness has been identified in SourceCodester Inventory Management System 1.0. The affected element is an unknown function of the file /model/user/resetPassword.php. Executing manipulation can lead to weak password recovery. The attack may be performed from remote. The exploit has been made available to the public and could be exploited.

CVSS: 5.3 (MEDIUM)

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

Tipo: CWE-640

Tecnología: No especificado

Publicado el: 2025-11-23

CVE-2025-13578

Descripción: A vulnerability has been found in code-projects Library System 1.0. This affects an unknown function of the file /index.php of the component Login. The manipulation of the argument Username leads to sql injection. The attack can 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: 2025-11-24

CVE-2025-6389

Descripción: The Sneeit Framework plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 8.3 via the sneeit_articles_pagination_callback() function. This is due to the function accepting user input and then passing that through call_user_func(). This makes it possible for unauthenticated attackers to execute code on the server which can be leveraged to inject backd...

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: 2025-11-25

CVE-2025-13559

Descripción: The EduKart Pro plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.0.3. This is due to the 'edukart_pro_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: 2025-11-25

CVE-2025-65084

Descripción: An Out-of-Bounds Write vulnerability is present in Ashlar-Vellum Cobalt, Xenon, Argon, Lithium, and Cobalt Share versions 12.6.1204.207 and prior that could allow an attacker to disclose information or execute arbitrary code.

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: 2025-11-25

CVE-2025-65085

Descripción: A Heap-based Buffer Overflow vulnerability is present in Ashlar-Vellum Cobalt, Xenon, Argon, Lithium, and Cobalt Share versions 12.6.1204.207 and prior that could allow an attacker to disclose information or execute arbitrary code.

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: 2025-11-25

CVE-2025-13595

Descripción: The CIBELES AI plugin for WordPress is vulnerable to arbitrary file uploads due to missing capability check in the 'actualizador_git.php' file in all versions up to, and including, 1.10.8. This makes it possible for unauthenticated attackers to download arbitrary GitHub repositories and overwrite plugin 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: 2025-11-25

CVE-2025-13597

Descripción: The AI Feeds plugin for WordPress is vulnerable to arbitrary file uploads due to missing capability check in the 'actualizador_git.php' file in all versions up to, and including, 1.0.11. This makes it possible for unauthenticated attackers to download arbitrary GitHub repositories and overwrite plugin 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: 2025-11-25

CVE-2025-64656

Descripción: Out-of-bounds read in Application Gateway allows an unauthorized attacker to elevate privileges over a network.

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-125

Tecnología: No especificado

Publicado el: 2025-11-26

CVE-2025-64657

Descripción: Stack-based buffer overflow in Azure Application Gateway allows an unauthorized attacker to elevate privileges 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-121

Tecnología: No especificado

Publicado el: 2025-11-26

CVE-2025-13538

Descripción: The FindAll Listing plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.0.5. This is due to the 'findall_listing_user_registration_additional_params' 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 ac...

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: 2025-11-27

CVE-2025-13539

Descripción: The FindAll Membership plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 1.0.4. This is due to the plugin not properly logging in a user with the data that was previously verified through the 'findall_membership_check_facebook_user' and the 'findall_membership_check_google_user' functions. This makes it possible for unauthenticated attackers to lo...

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: 2025-11-27

CVE-2025-13540

Descripción: The Tiare Membership plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.2. This is due to the 'tiare_membership_init_rest_api_register' 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 s...

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: 2025-11-27

CVE-2025-13675

Descripción: The Tiger theme for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 101.2.1. This is due to the 'paypal-submit.php' file 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: 2025-11-27

Resumen del Reporte

CVEs analizados: 19

Promedio CVSS: 8.75

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat