CVEs más relevantes de la semana

Del 25/11/2025 al 02/12/2025

Porque el primer paso para defender es conocer las amenazas.

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-2025-58360

Descripción: GeoServer is an open source server that allows users to share and edit geospatial data. From version 2.26.0 to before 2.26.2 and before 2.25.6, an XML External Entity (XXE) vulnerability was identified. The application accepts XML input through a specific endpoint /geoserver/wms operation GetMap. However, this input is not sufficiently sanitized or restricted, allowing an attacker to define ext...

CVSS: 8.2 (HIGH)

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

Tipo: CWE-611

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

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-2025-63531

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-2025-41742

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

Resumen del Reporte

CVEs analizados: 15

Promedio CVSS: 9.63

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat