CVEs más relevantes de la semana

Del 05/08/2025 al 12/08/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-6994

Descripción: The Reveal Listing plugin by smartdatasoft for WordPress is vulnerable to privilege escalation in versions up to, and including, 3.3. This is due to the plugin allowing users who are registering new accounts to set their own role or by supplying 'listing_user_role' field. This makes it possible for unauthenticated attackers to gain elevated privileges by creating an account with the administrat...

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: 2025-08-06

CVE-2025-53767

Descripción: Azure OpenAI Elevation of Privilege Vulnerability

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-918

Tecnología: No especificado

Publicado el: 2025-08-07

CVE-2025-53792

Descripción: Azure Portal Elevation of Privilege Vulnerability

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-285

Tecnología: No especificado

Publicado el: 2025-08-07

CVE-2025-8730

Descripción: A vulnerability was found in Belkin F9K1009 and F9K1010 2.00.04/2.00.09 and classified as critical. Affected by this issue is some unknown functionality of the component Web Interface. The manipulation leads to hard-coded credentials. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did no...

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-259

Tecnología: No especificado

Publicado el: 2025-08-08

CVE-2025-8731

Descripción: A vulnerability was found in TRENDnet TI-G160i, TI-PG102i and TPL-430AP up to 20250724. It has been classified as critical. This affects an unknown part of the component SSH Service. The manipulation leads to use of default credentials. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosu...

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-1392

Tecnología: No especificado

Publicado el: 2025-08-08

CVE-2025-8853

Descripción: Official Document Management System developed by 2100 Technology has an Authentication Bypass vulnerability, allowing unauthenticated remote attackers to obtain any user's connection token and use it to log into the system as that user.

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-290

Tecnología: No especificado

Publicado el: 2025-08-11

CVE-2025-42950

Descripción: SAP Landscape Transformation (SLT) allows an attacker with user privileges to exploit a vulnerability in the function module exposed via RFC. This flaw enables the injection of arbitrary ABAP code into the system, bypassing essential authorization checks. This vulnerability effectively functions as a backdoor, creating the risk of full system compromise, undermining the confidentiality, integri...

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-94

Tecnología: No especificado

Publicado el: 2025-08-12

CVE-2025-42957

Descripción: SAP S/4HANA allows an attacker with user privileges to exploit a vulnerability in the function module exposed via RFC. This flaw enables the injection of arbitrary ABAP code into the system, bypassing essential authorization checks. This vulnerability effectively functions as a backdoor, creating the risk of full system compromise, undermining the confidentiality, integrity and availability of ...

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-94

Tecnología: No especificado

Publicado el: 2025-08-12

CVE-2025-8059

Descripción: The B Blocks plugin for WordPress is vulnerable to Privilege Escalation due to missing authorization and improper input validation within the rgfr_registration() function in all versions up to, and including, 2.0.6. This makes it possible for unauthenticated attackers to create a new account and assign it 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-862

Tecnología: No especificado

Publicado el: 2025-08-12

CVE-2025-40746

Descripción: A vulnerability has been identified in SIMATIC RTLS Locating Manager (All versions < V3.2). Affected products do not properly validate input for a backup script. This could allow an authenticated remote attacker with high privileges in the application to execute arbitrary code with 'NT Authority/SYSTEM' privileges.

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-20

Tecnología: No especificado

Publicado el: 2025-08-12

Resumen del Reporte

CVEs analizados: 10

Promedio CVSS: 9.70

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat