CVEs más relevantes de la semana

Del 29/04/2025 al 06/05/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-30390

Descripción: Improper authorization in Azure 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-285

Tecnología: No especificado

Publicado el: 2025-04-30

CVE-2025-30392

Descripción: Improper authorization in Azure Bot Framework SDK 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-285

Tecnología: No especificado

Publicado el: 2025-04-30

CVE-2025-3746

Descripción: The OTP-less one tap Sign in plugin for WordPress is vulnerable to privilege escalation via account takeover in versions 2.0.14 to 2.0.59. This is due to the plugin not properly validating a user's identity prior to updating their details, like email. This makes it possible for unauthenticated attackers to change arbitrary users' email addresses, including administrators, and leverage that to r...

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: 2025-05-02

CVE-2025-3708

Descripción: Le-show medical practice management system from Le-yan has a SQL Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read, modify, and delete database contents.

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: 2025-05-02

CVE-2025-3709

Descripción: Agentflow from Flowring Technology has an Account Lockout Bypass vulnerability, allowing unauthenticated remote attackers to exploit this vulnerability to perform password brute force attack.

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-307

Tecnología: No especificado

Publicado el: 2025-05-02

CVE-2025-2812

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Mydata Informatics Ticket Sales Automation allows Blind SQL Injection.This issue affects Ticket Sales Automation: before 03.04.2025 (DD.MM.YYYY).

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: 2025-05-02

CVE-2025-3918

Descripción: The Job Listings plugin for WordPress is vulnerable to Privilege Escalation due to improper authorization within the register_action() function in versions 0.1 to 0.1.1. The plugin's registration handler reads the client-supplied $_POST['user_role'] and passes it directly to wp_insert_user() without restricting to a safe set of roles. This makes it possible for unauthenticated attackers to ele...

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-285

Tecnología: No especificado

Publicado el: 2025-05-03

CVE-2025-1909

Descripción: The BuddyBoss Platform Pro plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 2.7.01. This is due to insufficient verification on the user being supplied during the Apple OAuth authenticate request through the plugin. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have ...

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: 2025-05-05

Resumen del Reporte

CVEs analizados: 8

Promedio CVSS: 9.81

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat