CVEs más relevantes de la semana

Del 06/05/2025 al 13/05/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2024-12225

Descripción: A vulnerability was found in Quarkus in the quarkus-security-webauthn module. The Quarkus WebAuthn module publishes default REST endpoints for registering and logging users in while allowing developers to provide custom REST endpoints. When developers provide custom REST endpoints, the default endpoints remain accessible, potentially allowing attackers to obtain a login cookie that has no corre...

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-288

Tecnología: No especificado

Publicado el: 2025-05-06

CVE-2025-0855

Descripción: The PGS Core plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 5.8.0 via deserialization of untrusted input in the 'import_header' function. This makes it possible for unauthenticated attackers to inject a PHP Object. No known POP chain is present in the vulnerable software. If a POP chain is present via an additional plugin or theme installed on t...

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: 2025-05-06

CVE-2025-3844

Descripción: The PeproDev Ultimate Profile Solutions plugin for WordPress is vulnerable to Authentication Bypass in versions 1.9.1 to 7.5.2. This is due to handel_ajax_req() function not having proper restrictions on the change_user_meta functionality that makes it possible to set a OTP code and subsequently log in with that OTP code. This makes it possible for unauthenticated attackers to login as other us...

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: 2025-05-07

CVE-2025-4104

Descripción: The Frontend Dashboard plugin for WordPress is vulnerable to Privilege Escalation due to a missing capability check on the fed_wp_ajax_fed_login_form_post() function in versions 1.0 to 2.2.6. This makes it possible for unauthenticated attackers to reset the administrator's email and password, and elevate their privileges to that of an administrator.

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: 2025-05-07

CVE-2025-47548

Descripción: Server-Side Request Forgery (SSRF) vulnerability in Varun Dubey Wbcom Designs - Activity Link Preview For BuddyPress allows Server Side Request Forgery. This issue affects Wbcom Designs - Activity Link Preview For BuddyPress: from n/a through 1.4.4.

CVSS: 5.4 (MEDIUM)

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

Tipo: CWE-918

Tecnología: No especificado

Publicado el: 2025-05-07

CVE-2025-47635

Descripción: Server-Side Request Forgery (SSRF) vulnerability in WPWebinarSystem WebinarPress allows Server Side Request Forgery. This issue affects WebinarPress: from n/a through 1.33.27.

CVSS: 5.5 (MEDIUM)

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

Tipo: CWE-918

Tecnología: No especificado

Publicado el: 2025-05-07

CVE-2025-20188

Descripción: A vulnerability in the Out-of-Band Access Point (AP) Image Download feature of Cisco IOS XE Software for Wireless LAN Controllers (WLCs) could allow an unauthenticated, remote attacker to upload arbitrary files to an affected system. This vulnerability is due to the presence of a hard-coded JSON Web Token (JWT) on an affected system. An attacker could exploit this vulnerability by sending cr...

CVSS: 10.0 (CRITICAL)

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

Tipo: CWE-798

Tecnología: No especificado

Publicado el: 2025-05-07

CVE-2025-29813

Descripción: An elevation of privilege vulnerability exists when Visual Studio improperly handles pipeline job tokens. An attacker who successfully exploited this vulnerability could extend their access to a project. To exploit this vulnerability, an attacker would first have to have access to the project and swap the short-term token for a long-term one. The update addresses the vulnerability by correcting...

CVSS: 10.0 (CRITICAL)

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

Tipo: CWE-302

Tecnología: No especificado

Publicado el: 2025-05-08

CVE-2025-29827

Descripción: Improper Authorization in Azure Automation 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:L

Tipo: CWE-285

Tecnología: No especificado

Publicado el: 2025-05-08

CVE-2025-29972

Descripción: Server-Side Request Forgery (SSRF) in Azure allows an authorized attacker to perform spoofing 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-918

Tecnología: No especificado

Publicado el: 2025-05-08

CVE-2025-47733

Descripción: Server-Side Request Forgery (SSRF) in Microsoft Power Apps allows an unauthorized attacker to disclose information over a network

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-918

Tecnología: No especificado

Publicado el: 2025-05-08

CVE-2025-3810

Descripción: The WPBookit plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 1.0.2. This is due to the plugin not properly validating a user's identity prior to updating their details like password and email through the edit_profile_data() function. This makes it possible for unauthenticated attackers to change arbitrary user's email address...

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: 2025-05-09

CVE-2025-3811

Descripción: The WPBookit plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 1.0.2. This is due to the plugin not properly validating a user's identity prior to updating their details like email through the edit_newdata_customer_callback() function. This makes it possible for unauthenticated attackers to change arbitrary user's email address...

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: 2025-05-09

CVE-2024-11617

Descripción: The Envolve Plugin plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'zetra_languageUpload' and 'zetra_fontsUpload' functions in all versions up to, and including, 1.0. 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: 2025-05-09

CVE-2025-2253

Descripción: The IMITHEMES Listing plugin is vulnerable to privilege escalation via account takeover in all versions up to, and including, 3.3. This is due to the plugin not properly validating a verification code value prior to updating their password through the imic_reset_password_init() function. This makes it possible for unauthenticated attackers to change any user's passwords, including administrator...

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-620

Tecnología: No especificado

Publicado el: 2025-05-09

CVE-2025-3605

Descripción: The Frontend Login and Registration Blocks plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 1.0.7. This is due to the plugin not properly validating a user's identity prior to updating their details like email via the flr_blocks_user_settings_handle_ajax_callback() function. This makes it possible for unauthenticated attackers...

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: 2025-05-09

CVE-2025-4403

Descripción: The Drag and Drop Multiple File Upload for WooCommerce plugin for WordPress is vulnerable to arbitrary file uploads in all versions up to, and including, 1.1.6 due to accepting a user-supplied supported_type string and the uploaded filename without enforcing real extension or MIME checks within the upload() function. This makes it possible for unauthenticated attackers to upload arbitrary files...

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: 2025-05-09

CVE-2025-4555

Descripción: The web management interface of Okcat Parking Management Platform from ZONG YU has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to directly access system functions. These functions include opening gates, viewing license plates and parking records, and restarting the system.

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-306

Tecnología: No especificado

Publicado el: 2025-05-12

CVE-2025-4556

Descripción: The web management interface of Okcat Parking Management Platform from ZONG YU 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: 2025-05-12

CVE-2025-4558

Descripción: The GPM from WormHole Tech has an Unverified Password Change vulnerability, allowing unauthenticated remote attackers to change any user's password and use the modified password to log into the system.

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-620

Tecnología: No especificado

Publicado el: 2025-05-12

CVE-2023-49641

Descripción: Billing Software v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'username' parameter of the loginCheck.php resource does not validate the characters received and they are sent unfiltered to the database.

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: 2025-05-13

CVE-2025-26389

Descripción: A vulnerability has been identified in OZW672 (All versions < V8.0), OZW772 (All versions < V8.0). The web service in affected devices does not sanitize the input parameters required for the `exportDiagramPage` endpoint. This could allow an unauthenticated remote attacker to execute arbitrary code with root privileges.

CVSS: 10.0 (CRITICAL)

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

Tipo: CWE-78

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-26390

Descripción: A vulnerability has been identified in OZW672 (All versions < V6.0), OZW772 (All versions < V6.0). The web service of affected devices is vulnerable to SQL injection when checking authentication data. This could allow an unauthenticated remote attacker to bypass the check and authenticate as Administrator 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-89

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-32469

Descripción: A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.5), RUGGEDCOM ROX MX5000RE (All versions < V2.16.5), RUGGEDCOM ROX RX1400 (All versions < V2.16.5), RUGGEDCOM ROX RX1500 (All versions < V2.16.5), RUGGEDCOM ROX RX1501 (All versions < V2.16.5), RUGGEDCOM ROX RX1510 (All versions < V2.16.5), RUGGEDCOM ROX RX1511 (All versions < V2.16.5), RUGGEDCOM ROX RX1512 (All v...

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-602

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-33024

Descripción: A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.5), RUGGEDCOM ROX MX5000RE (All versions < V2.16.5), RUGGEDCOM ROX RX1400 (All versions < V2.16.5), RUGGEDCOM ROX RX1500 (All versions < V2.16.5), RUGGEDCOM ROX RX1501 (All versions < V2.16.5), RUGGEDCOM ROX RX1510 (All versions < V2.16.5), RUGGEDCOM ROX RX1511 (All versions < V2.16.5), RUGGEDCOM ROX RX1512 (All v...

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-602

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-33025

Descripción: A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.5), RUGGEDCOM ROX MX5000RE (All versions < V2.16.5), RUGGEDCOM ROX RX1400 (All versions < V2.16.5), RUGGEDCOM ROX RX1500 (All versions < V2.16.5), RUGGEDCOM ROX RX1501 (All versions < V2.16.5), RUGGEDCOM ROX RX1510 (All versions < V2.16.5), RUGGEDCOM ROX RX1511 (All versions < V2.16.5), RUGGEDCOM ROX RX1512 (All v...

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-602

Tecnología: No especificado

Publicado el: 2025-05-13

Resumen del Reporte

CVEs analizados: 26

Promedio CVSS: 9.45

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat