CVEs más relevantes de la semana

Del 18/10/2025 al 25/10/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-11948

Descripción: Document Management System developed by Excellent Infotek 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: 2025-10-20

CVE-2025-55086

Descripción: In NetXDuo version before 6.4.4, a networking support module for Eclipse Foundation ThreadX, in the DHCPV6 client there was an unchecked index extracting the server DUID from the server reply. With a crafted packet, an attacker could cause an out of memory read.

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-125

Tecnología: No especificado

Publicado el: 2025-10-20

CVE-2025-6542

Descripción: An arbitrary OS command may be executed on the product by a remote unauthenticated attacker.

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-78

Tecnología: No especificado

Publicado el: 2025-10-21

CVE-2025-7851

Descripción: An attacker may obtain the root shell on the underlying OS system with the restricted conditions on Omada gateways.

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: 2025-10-21

CVE-2025-41723

Descripción: The importFile SOAP method is vulnerable to a directory traversal attack. An unauthenticated remote attacker bypass the path restriction and upload files to arbitrary locations.

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-35

Tecnología: No especificado

Publicado el: 2025-10-22

CVE-2025-57870

Descripción: A SQL Injection vulnerability exists in Esri ArcGIS Server versions 11.3, 11.4 and 11.5 on Windows, Linux and Kubernetes. This vulnerability allows a remote, unauthenticated attacker to execute arbitrary SQL commands via a specific ArcGIS Feature Service operation. Successful exploitation can potentially result in unauthorized access, modification, or deletion of data from the underlying Enterp...

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-89

Tecnología: No especificado

Publicado el: 2025-10-22

CVE-2025-11023

Descripción: Inclusion of Functionality from Untrusted Control Sphere, Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ArkSigner Software and Hardware Inc. AcBakImzala allows PHP Local File Inclusion.This issue affects AcBakImzala: before v5.1.4.

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-98

Tecnología: No especificado

Publicado el: 2025-10-23

CVE-2025-59503

Descripción: Server-side request forgery (ssrf) in Azure Compute Gallery 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-918

Tecnología: No especificado

Publicado el: 2025-10-23

CVE-2025-6440

Descripción: The WooCommerce Designer Pro plugin for WordPress, used by the Pricom - Printing Company & Design Services WordPress theme, is vulnerable to arbitrary file uploads due to missing file type validation in the 'wcdp_save_canvas_design_ajax' function in all versions up to, and including, 1.9.26. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's se...

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: 2025-10-24

CVE-2025-11253

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Aksis Technology Inc. Netty ERP allows SQL Injection.This issue affects Netty ERP: before V.1.1000.

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: 2025-10-24

Resumen del Reporte

CVEs analizados: 10

Promedio CVSS: 9.83

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat □