CVEs más relevantes de la semana

Del 23/09/2025 al 30/09/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-41715

Descripción: The database for the web application is exposed without authentication, allowing an unauthenticated remote attacker to gain unauthorized access and potentially compromise it.

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: 2025-09-24

CVE-2025-9054

Descripción: The MultiLoca - WooCommerce Multi Locations Inventory Management plugin for WordPress is vulnerable to unauthorized modification of data that can lead to privilege escalation due to a missing capability check on the 'wcmlim_settings_ajax_handler' function in all versions up to, and including, 4.2.8. This makes it possible for unauthenticated attackers to update arbitrary options on the WordPres...

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: 2025-09-24

CVE-2025-21483

Descripción: Memory corruption when the UE receives an RTP packet from the network, during the reassembly of NALUs.

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-119

Tecnología: No especificado

Publicado el: 2025-09-24

CVE-2025-27034

Descripción: Memory corruption while selecting the PLMN from SOR failed list.

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-129

Tecnología: No especificado

Publicado el: 2025-09-24

CVE-2025-10585

Descripción: Type confusion in V8 in Google Chrome prior to 140.0.7339.185 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)

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-843

Tecnología: No especificado

Publicado el: 2025-09-24

CVE-2025-20363

Descripción: A vulnerability in the web services of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software, Cisco Secure Firewall Threat Defense (FTD) Software, Cisco IOS Software, Cisco IOS XE Software, and Cisco IOS XR Software could allow an unauthenticated, remote attacker (Cisco ASA and FTD Software) or authenticated, remote attacker (Cisco IOS, IOS XE, and IOS XR Software) with low user priv...

CVSS: 9.0 (CRITICAL)

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

Tipo: CWE-122

Tecnología: No especificado

Publicado el: 2025-09-25

CVE-2025-9642

Descripción: An issue has been discovered in GitLab CE/EE affecting all versions from 14.10 before 18.2.7, 18.3 before 18.3.3, and 18.4 before 18.4.1 that could allow an attacker to inject malicious content that may lead to account takeover.

CVSS: 8.7 (HIGH)

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

Tipo: CWE-79

Tecnología: No especificado

Publicado el: 2025-09-26

CVE-2025-11126

Descripción: A security flaw has been discovered in Apeman ID71 218.53.203.117. This vulnerability affects unknown code of the file /system/www/system.ini. The manipulation results in hard-coded credentials. The attack may be performed from remote. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.

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: 2025-09-29

CVE-2024-13150

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Fayton Software and Consulting Services fayton.Pro ERP allows SQL Injection.This issue affects fayton.Pro ERP: through 20250929.

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: 2025-09-29

CVE-2025-8625

Descripción: The Copypress Rest API plugin for WordPress is vulnerable to Remote Code Execution via copyreap_handle_image() Function in versions 1.1 to 1.2. The plugin falls back to a hard-coded JWT signing key when no secret is defined and does not restrict which file types can be fetched and saved as attachments. As a result, unauthenticated attackers can forge a valid token to gain elevated privileges an...

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-321

Tecnología: No especificado

Publicado el: 2025-09-30

CVE-2025-9762

Descripción: The Post By Email plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the save_attachments function in all versions up to, and including, 1.0.4b. 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-78

Tecnología: No especificado

Publicado el: 2025-09-30

CVE-2025-7493

Descripción: A privilege escalation flaw from host to domain administrator was found in FreeIPA. This vulnerability is similar to CVE-2025-4404, where it fails to validate the uniqueness of the krbCanonicalName. While the previously released version added validations for the admin@REALM credential, FreeIPA still does not validate the root@REALM canonical name, which can also be used as the realm administrat...

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-1220

Tecnología: No especificado

Publicado el: 2025-09-30

Resumen del Reporte

CVEs analizados: 12

Promedio CVSS: 9.58

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat □