CVEs más relevantes de la semana

Del 26/08/2025 al 02/09/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-9523

Descripción: A vulnerability was detected in Tenda AC1206 15.03.06.23. Affected is the function GetParentControlInfo of the file /goform/GetParentControlInfo. The manipulation of the argument mac results in stack-based buffer overflow. It is possible to launch the attack remotely. The exploit is now public and may be used.

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: 2025-08-27

CVE-2025-7955

Descripción: The RingCentral Communications plugin for WordPress is vulnerable to Authentication Bypass due to improper validation within the ringcentral_admin_login_2fa_verify() function in versions 1.5 to 1.6.8. This makes it possible for unauthenticated attackers to log in as any user simply by supplying identical bogus codes.

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-287

Tecnología: No especificado

Publicado el: 2025-08-28

CVE-2025-57819

Descripción: FreePBX is an open-source web-based graphical user interface. FreePBX 15, 16, and 17 endpoints are vulnerable due to insufficiently sanitized user-supplied data allowing unauthenticated access to FreePBX Administrator leading to arbitrary database manipulation and remote code execution. This issue has been patched in endpoint versions 15.0.66, 16.0.89, and 17.0.3.

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: 2025-08-28

CVE-2025-8857

Descripción: Clinic Image System developed by Changing contains hard-coded Credentials, allowing unauthenticated remote attackers to log into the system using administrator credentials embedded in the source code.

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-798

Tecnología: No especificado

Publicado el: 2025-08-29

CVE-2025-8861

Descripción: TSA developed by Changing has a Missing Authentication vulnerability, allowing unauthenticated remote attackers 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-306

Tecnología: No especificado

Publicado el: 2025-08-29

CVE-2025-9643

Descripción: A vulnerability was found in itsourcecode Apartment Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /setting/utility_bill_setup.php. Performing manipulation of the argument txtGasBill results in sql injection. It is possible to initiate the attack remotely. The exploit has been made public and could be used.

CVSS: 7.3 (HIGH)

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

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-08-29

CVE-2025-9644

Descripción: A vulnerability was determined in itsourcecode Apartment Management System 1.0. Affected by this issue is some unknown functionality of the file /setting/bill_setup.php. Executing manipulation of the argument txtBillType can lead to sql injection. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized.

CVSS: 7.3 (HIGH)

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

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-08-29

CVE-2025-9645

Descripción: A vulnerability was identified in itsourcecode Apartment Management System 1.0. This affects an unknown part of the file /t_dashboard/r_all_info.php. The manipulation of the argument mid leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might be used.

CVSS: 7.3 (HIGH)

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

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-08-29

CVE-2024-28988

Descripción: SolarWinds Web Help Desk was found to be susceptible to a Java Deserialization Remote Code Execution vulnerability that, if exploited, would allow an attacker to run commands on the host machine. This vulnerability was found by the ZDI team after researching a previous vulnerability and providing this report. The ZDI team was able to discover an unauthenticated attack during their research.

...

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: 2025-09-01

Resumen del Reporte

CVEs analizados: 9

Promedio CVSS: 8.97

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat