CVEs más relevantes de la semana

Del 26/07/2025 al 02/08/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-8226

Descripción: A vulnerability was found in yanyutao0402 ChanCMS up to 3.1.2. It has been classified as problematic. Affected is an unknown function of the file /sysApp/find. The manipulation of the argument accessKey/secretKey leads to information disclosure. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.1.3 is able to addre...

CVSS: 4.3 (MEDIUM)

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

Tipo: CWE-200

Tecnología: No especificado

Publicado el: 2025-07-27

CVE-2025-8227

Descripción: A vulnerability was found in yanyutao0402 ChanCMS up to 3.1.2. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /collect/getArticle. The manipulation of the argument taskUrl leads to deserialization. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.1.3 is able to addr...

CVSS: 6.3 (MEDIUM)

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

Tipo: CWE-20

Tecnología: No especificado

Publicado el: 2025-07-27

CVE-2025-8244

Descripción: A vulnerability was found in TOTOLINK X15 1.0.0-B20230714.1105. It has been classified as critical. Affected is an unknown function of the file /boafrm/formMapDelDevice of the component HTTP POST Request Handler. The manipulation of the argument macstr leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.

CVSS: 8.8 (HIGH)

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

Tipo: CWE-119

Tecnología: No especificado

Publicado el: 2025-07-27

CVE-2025-8249

Descripción: A vulnerability, which was classified as critical, has been found in code-projects Exam Form Submission 1.0. This issue affects some unknown processing of the file /admin/update_s3.php. The manipulation of the argument credits leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may 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: 2025-07-28

CVE-2025-8250

Descripción: A vulnerability, which was classified as critical, was found in code-projects Exam Form Submission 1.0. Affected is an unknown function of the file /admin/update_s4.php. The manipulation of the argument credits leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may 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: 2025-07-28

CVE-2025-8251

Descripción: A vulnerability has been found in code-projects Exam Form Submission 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/delete_s4.php. The manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may 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: 2025-07-28

CVE-2025-8252

Descripción: A vulnerability was found in code-projects Exam Form Submission 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/delete_s5.php. The manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may 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: 2025-07-28

CVE-2025-8253

Descripción: A vulnerability was found in code-projects Exam Form Submission 1.0. It has been classified as critical. This affects an unknown part of the file /admin/delete_s6.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may 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: 2025-07-28

CVE-2025-8254

Descripción: A vulnerability was found in Campcodes Courier Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /view_parcel.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.

CVSS: 6.3 (MEDIUM)

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

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-07-28

CVE-2025-8255

Descripción: A vulnerability was found in code-projects Exam Form Submission 1.0. It has been rated as critical. This issue affects some unknown processing of the file /register.php. The manipulation of the argument image leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may 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-284

Tecnología: No especificado

Publicado el: 2025-07-28

CVE-2025-8256

Descripción: A vulnerability classified as critical has been found in code-projects Online Ordering System 1.0. Affected is an unknown function of the file /admin/product.php. The manipulation of the argument image leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.

CVSS: 6.3 (MEDIUM)

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

Tipo: CWE-284

Tecnología: No especificado

Publicado el: 2025-07-28

CVE-2025-8259

Descripción: A vulnerability, which was classified as critical, was found in Vaelsys 4.1.0. This affects the function execute_DataObjectProc of the file /grid/vgrid_server.php. The manipulation of the argument xajaxargs leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclos...

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-77

Tecnología: No especificado

Publicado el: 2025-07-28

CVE-2025-8261

Descripción: A vulnerability was found in Vaelsys 4.1.0 and classified as critical. This issue affects some unknown processing of the file /grid/vgrid_server.php of the component User Creation Handler. The manipulation leads to improper authorization. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but d...

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-266

Tecnología: No especificado

Publicado el: 2025-07-28

CVE-2025-8269

Descripción: A vulnerability was found in code-projects Exam Form Submission 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/delete_s1.php. The manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may 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: 2025-07-28

CVE-2025-8270

Descripción: A vulnerability was found in code-projects Exam Form Submission 1.0. It has been classified as critical. This affects an unknown part of the file /admin/delete_s2.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may 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: 2025-07-28

CVE-2025-8271

Descripción: A vulnerability was found in code-projects Exam Form Submission 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/delete_s3.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may 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: 2025-07-28

CVE-2025-6918

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Ncvav Virtual PBX Software allows SQL Injection.This issue affects Virtual PBX Software: before 09.07.2025.

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: 2025-07-28

CVE-2025-8272

Descripción: A vulnerability was found in code-projects Exam Form Submission 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/update_fst.php. The manipulation of the argument credits leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may 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: 2025-07-28

CVE-2025-8273

Descripción: A vulnerability classified as critical has been found in code-projects Exam Form Submission 1.0. Affected is an unknown function of the file /admin/update_s8.php. The manipulation of the argument credits leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may 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: 2025-07-28

CVE-2025-26469

Descripción: An incorrect default permissions vulnerability exists in the CServerSettings::SetRegistryValues functionality of MedDream PACS Premium 7.3.3.840. A specially crafted application can decrypt credentials stored in a configuration-related registry key. An attacker can execute a malicious script or application to exploit this vulnerability.

CVSS: 9.3 (CRITICAL)

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

Tipo: CWE-732

Tecnología: No especificado

Publicado el: 2025-07-28

CVE-2025-27724

Descripción: A privilege escalation vulnerability exists in the login.php functionality of meddream MedDream PACS Premium 7.3.3.840. A specially crafted .php file can lead to elevated capabilities. An attacker can upload a malicious file to trigger this vulnerability.

CVSS: 9.3 (CRITICAL)

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

Tipo: CWE-284

Tecnología: No especificado

Publicado el: 2025-07-28

CVE-2025-54530

Descripción: In JetBrains TeamCity before 2025.07 privilege escalation was possible due to incorrect directory permissions

CVSS: 7.5 (HIGH)

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

Tipo: CWE-276

Tecnología: No especificado

Publicado el: 2025-07-28

CVE-2025-54531

Descripción: In JetBrains TeamCity before 2025.07 path traversal was possible via plugin unpacking on Windows

CVSS: 7.7 (HIGH)

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

Tipo: CWE-23

Tecnología: No especificado

Publicado el: 2025-07-28

CVE-2025-5954

Descripción: The Service Finder SMS System plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 2.0.0. This is due to the plugin not restricting user role selection at the time of registration through the aonesms_fn_savedata_after_signup() function. This makes it possible for unauthenticated attackers to register as an 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-269

Tecnología: No especificado

Publicado el: 2025-08-01

CVE-2025-5947

Descripción: The Service Finder Bookings plugin for WordPress is vulnerable to privilege escalation via authentication bypass in all versions up to, and including, 6.0. This is due to the plugin not properly validating a user's cookie value prior to logging them in through the service_finder_switch_back() function. This makes it possible for unauthenticated attackers to login as any user including admins.

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: 2025-08-01

Resumen del Reporte

CVEs analizados: 25

Promedio CVSS: 7.60

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat □