CVEs más relevantes de la semana

Del 03/01/2026 al 10/01/2026

Porque el primer paso para defender es conocer las amenazas.

CVE-2026-0575

Descripción: A security vulnerability has been detected in code-projects Online Product Reservation System 1.0. This impacts an unknown function of the file /handgunner-administrator/adminlogin.php of the component Administrator Login. Such manipulation of the argument emailadd/pass leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly 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: 2026-01-04

CVE-2026-0576

Descripción: A vulnerability was detected in code-projects Online Product Reservation System 1.0. Affected is an unknown function of the file /handgunner-administrator/prod.php of the component Parameter Handler. Performing manipulation of the argument cat/price/name/model/serial results in sql injection. It is possible to initiate the attack remotely. The exploit is now 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: 2026-01-04

CVE-2026-0577

Descripción: A flaw has been found in code-projects Online Product Reservation System 1.0. Affected by this vulnerability is an unknown functionality of the file /handgunner-administrator/prod.php. Executing manipulation can lead to unrestricted upload. It is possible to launch the attack remotely. The exploit has been published 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: 2026-01-04

CVE-2026-0578

Descripción: A vulnerability has been found in code-projects Online Product Reservation System 1.0. Affected by this issue is some unknown functionality of the file /handgunner-administrator/delete.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: 2026-01-04

CVE-2026-0579

Descripción: A vulnerability was found in code-projects Online Product Reservation System 1.0. This affects an unknown part of the file /handgunner-administrator/edit.php of the component POST Parameter Handler. The manipulation of the argument prod_id/name/price/model/serial results in sql injection. The attack can be launched 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: 2026-01-04

CVE-2026-0583

Descripción: A security flaw has been discovered in code-projects Online Product Reservation System 1.0. This vulnerability affects unknown code of the file app/user/login.php of the component User Login. The manipulation of the argument emailadd results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.

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: 2026-01-05

CVE-2026-0584

Descripción: A weakness has been identified in code-projects Online Product Reservation System 1.0. This issue affects some unknown processing of the file app/products/left_cart.php. This manipulation of the argument ID causes sql injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks.

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: 2026-01-05

CVE-2026-0585

Descripción: A security vulnerability has been detected in code-projects Online Product Reservation System 1.0. Impacted is an unknown function of the file /order_view.php of the component GET Parameter Handler. Such manipulation of the argument transaction_id leads to sql injection. The attack can be executed remotely. The exploit has been disclosed publicly 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: 2026-01-05

CVE-2026-0590

Descripción: A vulnerability was determined in code-projects Online Product Reservation System 1.0. The affected element is an unknown function of the file /app/checkout/delete.php of the component POST Parameter Handler. This manipulation of the argument ID causes sql injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.

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: 2026-01-05

CVE-2026-0591

Descripción: A vulnerability was identified in code-projects Online Product Reservation System 1.0. The impacted element is an unknown function of the file /app/checkout/update.php of the component Cart Update Handler. Such manipulation of the argument id/qty leads to sql injection. It is possible to launch the attack remotely. The exploit is publicly available and might 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: 2026-01-05

CVE-2026-0592

Descripción: A security flaw has been discovered in code-projects Online Product Reservation System 1.0. This affects an unknown function of the file /handgunner-administrator/register_code.php of the component User Registration Handler. Performing a manipulation of the argument fname/lname/address/city/province/country/zip/tel_no/email/username results in sql injection. The attack can be initiated remotely...

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: 2026-01-05

CVE-2025-14996

Descripción: The AS Password Field In Default Registration Form 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 properly validating a user's identity prior to updating their password. This makes it possible for unauthenticated attackers to change arbitrary user's passwords, including administrators, 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-639

Tecnología: No especificado

Publicado el: 2026-01-06

CVE-2025-15001

Descripción: The FS Registration Password plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 1.0.1. This is due to the plugin not properly validating a user's identity prior to updating their password. This makes it possible for unauthenticated attackers to change arbitrary user's passwords, including administrators, and leverage that to gai...

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: 2026-01-06

CVE-2020-36912

Descripción: Plexus anblick Digital Signage Management 3.1.13 contains an open redirect vulnerability in the 'PantallaLogin' script that allows attackers to manipulate the 'pagina' GET parameter. Attackers can craft malicious links that redirect users to arbitrary websites by exploiting improper input validation in the parameter.

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-601

Tecnología: No especificado

Publicado el: 2026-01-06

CVE-2020-36925

Descripción: Arteco Web Client DVR/NVR contains a session hijacking vulnerability with insufficient session ID complexity that allows remote attackers to bypass authentication. Attackers can brute force session IDs within a specific numeric range to obtain valid sessions and access live camera streams without authorization.

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-331

Tecnología: No especificado

Publicado el: 2026-01-06

CVE-2025-15471

Descripción: A vulnerability was detected in TRENDnet TEW-713RE 1.02. The impacted element is an unknown function of the file /goformX/formFSrvX. The manipulation of the argument SZCMD results in os command injection. It is possible to launch the attack remotely. The exploit is now public and may be used. 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-77

Tecnología: No especificado

Publicado el: 2026-01-07

CVE-2025-15018

Descripción: The Optional Email plugin for WordPress is vulnerable to Privilege Escalation via Account Takeover in all versions up to, and including, 1.3.11. This is due to the plugin not restricting its 'random_password' filter to registration contexts, allowing the filter to affect password reset key generation. This makes it possible for unauthenticated attackers to set a known password reset key when in...

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: 2026-01-07

CVE-2026-21679

Descripción: iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of ICC color management profiles. Prior to version 2.3.1.2, iccDEV is vulnerable to heap-buffer-overflow in CIccLocalizedUnicode::GetText(). This issue has been patched in version 2.3.1.2.

CVSS: 8.8 (HIGH)

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

Tipo: CWE-20

Tecnología: No especificado

Publicado el: 2026-01-07

CVE-2019-25268

Descripción: NREL BEopt 2.8.0.0 contains a DLL hijacking vulnerability that allows attackers to load arbitrary libraries by tricking users into opening application files from remote shares. Attackers can exploit insecure library loading of sdl2.dll and libegl.dll by placing malicious libraries on WebDAV or SMB shares to execute unauthorized 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-427

Tecnología: No especificado

Publicado el: 2026-01-08

CVE-2019-25282

Descripción: V-SOL GPON/EPON OLT Platform v2.03 contains an open redirect vulnerability in the script that allows attackers to manipulate the 'parent' GET parameter. Attackers can craft malicious links that redirect logged-in users to arbitrary websites by exploiting improper input validation in the redirect mechanism.

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-601

Tecnología: No especificado

Publicado el: 2026-01-08

CVE-2025-14736

Descripción: The Frontend Admin by DynamiApps plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 3.28.25. This is due to insufficient validation of user-supplied role values in the 'validate_value', 'pre_update_value', and 'get_fields_display' functions. This makes it possible for unauthenticated attackers to register as administrators and gain complete control ...

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: 2026-01-09

CVE-2025-14741

Descripción: The Frontend Admin by DynamiApps plugin for WordPress is vulnerable to missing authorization to unauthorized data modification and deletion due to a missing capability check on the 'delete_object' function in all versions up to, and including, 3.28.25. This makes it possible for unauthenticated attackers to delete arbitrary posts, pages, products, taxonomy terms, and user accounts.

CVSS: 9.1 (CRITICAL)

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

Tipo: CWE-862

Tecnología: No especificado

Publicado el: 2026-01-09

CVE-2025-15500

Descripción: A vulnerability was found in Sangfor Operation and Maintenance Management System up to 3.0.8. This issue affects some unknown processing of the file /isomp-protocol/protocol/getHis of the component HTTP POST Request Handler. The manipulation of the argument sessionPath results in os command injection. The attack may be launched remotely. The exploit has been made public and could be used. The v...

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-77

Tecnología: No especificado

Publicado el: 2026-01-09

CVE-2025-15501

Descripción: A vulnerability was determined in Sangfor Operation and Maintenance Management System up to 3.0.8. Impacted is the function WriterHandle.getCmd of the file /isomp-protocol/protocol/getCmd. This manipulation of the argument sessionPath causes os command injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized. The vendor was contacted ...

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-77

Tecnología: No especificado

Publicado el: 2026-01-09

Resumen del Reporte

CVEs analizados: 24

Promedio CVSS: 8.42

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat ▯