CVEs más relevantes de la semana

Del 06/01/2026 al 13/01/2026

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-14942

Descripción: wolfSSH's key exchange state machine can be manipulated to leak the client's password in the clear, trick the client to send a bogus signature, or trick the client into skipping user authentication. This affects client applications with wolfSSH version 1.4.21 and earlier. Users of wolfSSH must update or apply the fix patch and it's recommended to update credentials used. This fix is also recomm...

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: 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-2026-22189

Descripción: Panda3D versions up to and including 1.10.16 egg-mkfont contains a stack-based buffer overflow vulnerability due to use of an unbounded sprintf() call with attacker-controlled input. When constructing glyph filenames, egg-mkfont formats a user-supplied glyph pattern (-gp) into a fixed-size stack buffer without length validation. Supplying an excessively long glyph pattern string can overflow th...

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-121

Tecnología: No especificado

Publicado el: 2026-01-07

CVE-2025-69264

Descripción: pnpm is a package manager. Versions 10.0.0 through 10.25 allow git-hosted dependencies to execute arbitrary code during pnpm install, circumventing the v10 security feature "Dependency lifecycle scripts execution disabled by default". While pnpm v10 blocks postinstall scripts via the onlyBuiltDependencies mechanism, git dependencies can still execute prepare, prepublish, and prepack scripts dur...

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-693

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-2026-0700

Descripción: A vulnerability was determined in code-projects Intern Membership Management System 1.0. Affected is an unknown function of the file /intern/admin/check_admin.php. Executing a manipulation of the argument Username can lead to sql injection. The attack can be executed 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: 2026-01-08

CVE-2026-21891

Descripción: ZimaOS is a fork of CasaOS, an operating system for Zima devices and x86-64 systems with UEFI. In versions up to and including 1.5.0, the application checks the validity of the username but appears to skip, misinterpret, or incorrectly validate the password when the provided username matches a known system service account. The application's login function fails to properly handle the password v...

CVSS: 9.4 (CRITICAL)

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

Tipo: CWE-287

Tecnología: No especificado

Publicado el: 2026-01-08

CVE-2025-55125

Descripción: This vulnerability allows a Backup or Tape Operator to perform remote code execution (RCE) as root by creating a malicious backup configuration file.

CVSS: 7.8 (HIGH)

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

Tipo: CWE-77

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

CVE-2026-0491

Descripción: SAP Landscape Transformation allows an attacker with admin privileges to exploit a vulnerability in the function module exposed via RFC. This flaw enables the injection of arbitrary ABAP code/OS commands into the system, bypassing essential authorization checks. This vulnerability effectively functions as a backdoor, creating the risk of full system compromise, undermining the confidentiality, ...

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-94

Tecnología: No especificado

Publicado el: 2026-01-13

CVE-2026-0498

Descripción: SAP S/4HANA (Private Cloud and On-Premise) allows an attacker with admin privileges to exploit a vulnerability in the function module exposed via RFC. This flaw enables the injection of arbitrary ABAP code/OS commands into the system, bypassing essential authorization checks. This vulnerability effectively functions as a backdoor, creating the risk of full system compromise, undermining the con...

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-94

Tecnología: No especificado

Publicado el: 2026-01-13

CVE-2026-0500

Descripción: Due to the usage of vulnerable third party component in SAP Wily Introscope Enterprise Manager (WorkStation), an unauthenticated attacker could create a malicious JNLP (Java Network Launch Protocol) file accessible by a public facing URL. When a victim clicks on the URL the accessed Wily Introscope Server could execute OS commands on the victim's machine. This could completely compromising conf...

CVSS: 9.6 (CRITICAL)

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

Tipo: CWE-94

Tecnología: No especificado

Publicado el: 2026-01-13

CVE-2026-0501

Descripción: Due to insufficient input validation in SAP S/4HANA Private Cloud and On-Premise (Financials General Ledger), an authenticated user could execute crafted SQL queries to read, modify, and delete backend database data. This leads to a high impact on the confidentiality, integrity, and availability of the application.

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-89

Tecnología: No especificado

Publicado el: 2026-01-13

CVE-2025-40805

Descripción: Affected devices do not properly enforce user authentication on specific API endpoints. This could facilitate an unauthenticated remote attacker to circumvent authentication and impersonate a legitimate user. Successful exploitation requires that the attacker has learned the identity of a legitimate user.

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-639

Tecnología: No especificado

Publicado el: 2026-01-13

CVE-2025-12548

Descripción: A flaw was found in Eclipse Che che-machine-exec. This vulnerability allows unauthenticated remote arbitrary command execution and secret exfiltration (SSH keys, tokens, etc.) from other users' Developer Workspace containers, via an unauthenticated JSON-RPC / websocket API exposed on TCP port 3333.

CVSS: 9.0 (CRITICAL)

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

Tipo: CWE-306

Tecnología: No especificado

Publicado el: 2026-01-13

Resumen del Reporte

CVEs analizados: 21

Promedio CVSS: 9.34

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat