CVEs más relevantes de la semana

Del 10/01/2026 al 17/01/2026

Porque el primer paso para defender es conocer las amenazas.

CVE-2026-0821

Descripción: A vulnerability was determined in quickjs-ng quickjs up to 0.11.0. This vulnerability affects the function js_typed_array_constructor of the file quickjs.c. Executing a manipulation can lead to heap-based buffer overflow. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized. This patch is called c5d80831e51e48a83eab16ea867be87f091783c5. A patch should...

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-119

Tecnología: No especificado

Publicado el: 2026-01-10

CVE-2026-0851

Descripción: A vulnerability was identified in code-projects Online Music Site 1.0. The affected element is an unknown function of the file /Administrator/PHP/AdminAddUser.php. The manipulation of the argument txtusername leads to sql injection. Remote exploitation of the attack is possible. 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: 2026-01-12

CVE-2026-0852

Descripción: A security flaw has been discovered in code-projects Online Music Site 1.0. The impacted element is an unknown function of the file /Administrator/PHP/AdminUpdateUser.php. The manipulation of the argument ID results in sql injection. The attack can be executed 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: 2026-01-12

CVE-2025-69269

Descripción: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Broadcom DX NetOps Spectrum on Windows, Linux allows OS Command Injection.This issue affects DX NetOps Spectrum: 23.3.6 and earlier.

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: 2026-01-12

CVE-2025-69270

Descripción: Information Exposure Through Query Strings in GET Request vulnerability in Broadcom DX NetOps Spectrum on Windows, Linux allows Session Hijacking.This issue affects DX NetOps Spectrum: 24.3.8 and earlier.

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-598

Tecnología: No especificado

Publicado el: 2026-01-12

CVE-2026-22252

Descripción: LibreChat is a ChatGPT clone with additional features. Prior to v0.8.2-rc2, LibreChat's MCP stdio transport accepts arbitrary commands without validation, allowing any authenticated user to execute shell commands as root inside the container through a single API request. This vulnerability is fixed in v0.8.2-rc2.

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-285

Tecnología: No especificado

Publicado el: 2026-01-12

CVE-2026-22781

Descripción: TinyWeb is a web server (HTTP, HTTPS) written in Delphi for Win32. TinyWeb HTTP Server before version 1.98 is vulnerable to OS command injection via CGI ISINDEX-style query parameters. The query parameters are passed as command-line arguments to the CGI executable via Windows CreateProcess(). An unauthenticated remote attacker can execute arbitrary commands on the server by injecting Windows sh...

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: 2026-01-12

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

CVE-2025-25249

Descripción: A heap-based buffer overflow vulnerability in Fortinet FortiOS 7.6.0 through 7.6.3, FortiOS 7.4.0 through 7.4.8, FortiOS 7.2.0 through 7.2.11, FortiOS 7.0.0 through 7.0.17, FortiOS 6.4.0 through 6.4.16, FortiSwitchManager 7.2.0 through 7.2.6, FortiSwitchManager 7.0.0 through 7.0.5 allows attacker to execute unauthorized code or commands via specially crafted packets

CVSS: 8.1 (HIGH)

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

Tipo: CWE-122

Tecnología: No especificado

Publicado el: 2026-01-13

CVE-2022-50893

Descripción: VIAVIWEB Wallpaper Admin 1.0 contains an unauthenticated remote code execution vulnerability in the image upload functionality. Attackers can upload a malicious PHP file through the add_gallery_image.php endpoint to execute arbitrary code on the server.

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-434

Tecnología: No especificado

Publicado el: 2026-01-13

CVE-2022-50894

Descripción: VIAVIWEB Wallpaper Admin 1.0 contains an SQL injection vulnerability that allows authenticated attackers to manipulate database queries by injecting SQL code through the img_id parameter. Attackers can send GET requests to edit_gallery_image.php with malicious img_id values to extract database information.

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: 2026-01-13

CVE-2022-50912

Descripción: ImpressCMS 1.4.4 contains a file upload vulnerability with weak extension sanitization that allows attackers to upload potentially malicious files. Attackers can bypass file upload restrictions by using alternative file extensions .php2.php6.php7.phps.pht to execute arbitrary PHP code on the server.

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-434

Tecnología: No especificado

Publicado el: 2026-01-13

CVE-2022-50919

Descripción: Tdarr 2.00.15 contains an unauthenticated remote code execution vulnerability in its Help terminal that allows attackers to inject and chain arbitrary commands. Attackers can exploit the lack of input filtering by chaining commands like `--help; curl .py | python` to execute remote code without authentication.

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: 2026-01-13

CVE-2022-50922

Descripción: Audio Conversion Wizard v2.01 contains a buffer overflow vulnerability that allows attackers to execute arbitrary code by overwriting memory with a specially crafted registration code. Attackers can generate a payload that overwrites the application's memory stack, potentially enabling remote code execution through a carefully constructed input buffer.

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-120

Tecnología: No especificado

Publicado el: 2026-01-13

CVE-2022-50926

Descripción: WAGO 750-8212 PFC200 G2 2ETH RS firmware contains a privilege escalation vulnerability that allows attackers to manipulate user session cookies. Attackers can modify the cookie's 'name' and 'roles' parameters to elevate from ordinary user to administrative privileges without authentication.

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-565

Tecnología: No especificado

Publicado el: 2026-01-13

CVE-2022-50935

Descripción: Flame II HSPA USB Modem contains an unquoted service path vulnerability in its Windows service configuration. Attackers can exploit the unquoted path in 'C:\Program Files (x86)\Internet Telcel\ApplicationController.exe' to execute arbitrary code with elevated system privileges.

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-428

Tecnología: No especificado

Publicado el: 2026-01-13

CVE-2025-14301

Descripción: The Integration Opvius AI for WooCommerce plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.3.0. This is due to the `process_table_bulk_actions()` function processing user-supplied file paths without authentication checks, nonce verification, or path validation. This makes it possible for unauthenticated attackers to delete or download arbitrary files ...

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-22

Tecnología: No especificado

Publicado el: 2026-01-14

CVE-2021-47760

Descripción: TestLink versions 1.16 through 1.19 contain an unauthenticated file download vulnerability in the attachmentdownload.php endpoint. Attackers can download arbitrary files by iterating file IDs through the 'id' parameter with 'skipCheck=1' to bypass access controls.

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: 2026-01-15

CVE-2021-47774

Descripción: Kingdia CD Extractor 3.0.2 contains a buffer overflow vulnerability in the registration name field that allows attackers to execute arbitrary code. Attackers can craft a malicious payload exceeding 256 bytes to overwrite Structured Exception Handler and gain remote code execution through a bind shell.

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-787

Tecnología: No especificado

Publicado el: 2026-01-15

CVE-2021-47781

Descripción: Cmder Console Emulator 1.3.18 contains a buffer overflow vulnerability that allows attackers to trigger a denial of service condition through a maliciously crafted .cmd file. Attackers can create a specially constructed .cmd file with repeated characters to overwhelm the console emulator's buffer and crash the application.

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-787

Tecnología: No especificado

Publicado el: 2026-01-15

CVE-2021-47819

Descripción: ProjeQtOr Project Management 9.1.4 contains a file upload vulnerability that allows guest users to upload malicious PHP files with arbitrary code execution capabilities. Attackers can upload a PHP script through the profile attachment section and execute system commands by accessing the uploaded file with a specially crafted request 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-434

Tecnología: No especificado

Publicado el: 2026-01-15

CVE-2021-47796

Descripción: Denver SHC-150 Smart Wifi Camera contains a hardcoded telnet credential vulnerability that allows unauthenticated attackers to access a Linux shell. Attackers can connect to port 23 using the default credential to execute arbitrary commands on the camera's operating system.

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: 2026-01-16

CVE-2021-47798

Descripción: NoteBurner 2.35 contains a buffer overflow vulnerability in the license code input field that allows attackers to crash the application. Attackers can generate a 6000-byte payload and paste it into the 'Name' and 'Code' fields to trigger an application crash.

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-120

Tecnología: No especificado

Publicado el: 2026-01-16

CVE-2026-1019

Descripción: Police Statistics Database System developed by Gotac has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to read, modify, and delete database contents by using a specific functionality.

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: 2026-01-16

CVE-2026-1021

Descripción: Police Statistics Database System developed by Gotac has an Arbitrary File Upload vulnerability, allowing unauthenticated remote attacker to upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.

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-434

Tecnología: No especificado

Publicado el: 2026-01-16

CVE-2025-15403

Descripción: The RegistrationMagic plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 6.0.7.1. This is due to the 'add_menu' function is accessible via the 'rm_user_exists' AJAX action and allows arbitrary updates to the 'admin_order' setting. This makes it possible for unauthenticated attackers to injecting an empty slug into the order parameter, and manipulate...

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: 2026-01-17

CVE-2025-10484

Descripción: The Registration & Login with Mobile Phone Number for WooCommerce plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 1.3.1. This is due to the plugin not properly verifying a users identity prior to authenticating them via the fma_lwp_set_session_php_fun() function. This makes it possible for unauthenticated attackers to authenticate as any user on...

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-288

Tecnología: No especificado

Publicado el: 2026-01-17

Resumen del Reporte

CVEs analizados: 32

Promedio CVSS: 9.43

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat