CVEs más relevantes de la semana

Del 03/02/2026 al 10/02/2026

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-69971

Descripción: FUXA v1.2.7 contains a hard-coded credential vulnerability in server/api/jwt-helper.js. The application uses a hard-coded secret key to sign and verify JWT Tokens. This allows remote attackers to forge valid admin tokens and bypass authentication to gain full administrative access.

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: 2026-02-03

CVE-2025-69981

Descripción: FUXA v1.2.7 contains an Unrestricted File Upload vulnerability in the `/api/upload` API endpoint. The endpoint lacks authentication mechanisms, allowing unauthenticated remote attackers to upload arbitrary files. This can be exploited to overwrite critical system files (such as the SQLite user database) to gain administrative access, or to upload malicious scripts to execute arbitrary 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-434

Tecnología: No especificado

Publicado el: 2026-02-03

CVE-2025-69983

Descripción: FUXA v1.2.7 allows Remote Code Execution (RCE) via the project import functionality. The application does not properly sanitize or sandbox user-supplied scripts within imported project files. An attacker can upload a malicious project containing system commands, leading to full system compromise.

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: NVD-CWE-noinfo

Tecnología: No especificado

Publicado el: 2026-02-03

CVE-2026-25233

Descripción: PEAR is a framework and distribution system for reusable PHP components. Prior to version 1.33.0, logic bug in the roadmap role check allows non-lead maintainers to create, update, or delete roadmaps. This issue has been patched in version 1.33.0.

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-783

Tecnología: No especificado

Publicado el: 2026-02-03

CVE-2026-25234

Descripción: PEAR is a framework and distribution system for reusable PHP components. Prior to version 1.33.0, a SQL injection vulnerability in category deletion can allow an attacker with access to the category manager workflow to inject SQL via a category id. This issue has been patched in version 1.33.0.

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: 2026-02-03

CVE-2026-25236

Descripción: PEAR is a framework and distribution system for reusable PHP components. Prior to version 1.33.0, a SQL injection risk exists in karma queries due to unsafe literal substitution for an IN (...) list. This issue has been patched in version 1.33.0.

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: 2026-02-03

CVE-2026-25237

Descripción: PEAR is a framework and distribution system for reusable PHP components. Prior to version 1.33.0, use of preg_replace() with the /e modifier in bug update email handling can enable PHP code execution if attacker-controlled content reaches the evaluated replacement. This issue has been patched in version 1.33.0.

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-624

Tecnología: No especificado

Publicado el: 2026-02-03

CVE-2026-25238

Descripción: PEAR is a framework and distribution system for reusable PHP components. Prior to version 1.33.0, a SQL injection vulnerability in bug subscription deletion may allow attackers to inject SQL via a crafted email value. This issue has been patched in version 1.33.0.

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: 2026-02-03

CVE-2026-25240

Descripción: PEAR is a framework and distribution system for reusable PHP components. Prior to version 1.33.0, a SQL injection vulnerability can occur in user::maintains() when role filters are provided as an array and interpolated into an IN (...) clause. This issue has been patched in version 1.33.0.

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: 2026-02-03

CVE-2026-25241

Descripción: PEAR is a framework and distribution system for reusable PHP components. Prior to version 1.33.0, an unauthenticated SQL injection in the /get/<package>/<version> endpoint allows remote attackers to execute arbitrary SQL via a crafted package version. This issue has been patched in version 1.33.0.

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: 2026-02-03

CVE-2020-37065

Descripción: StreamRipper32 version 2.6 contains a buffer overflow vulnerability in the Station/Song Section that allows attackers to overwrite memory by manipulating the SongPattern input. Attackers can craft a malicious payload exceeding 256 bytes to potentially execute arbitrary code and compromise 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-120

Tecnología: No especificado

Publicado el: 2026-02-03

CVE-2020-37066

Descripción: GoldWave 5.70 contains a buffer overflow vulnerability that allows attackers to execute arbitrary code by crafting malicious input in the File Open URL dialog. Attackers can generate a specially crafted text file with Unicode-encoded shellcode to trigger a stack-based overflow and execute commands when the file is opened.

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: 2026-02-03

CVE-2020-37067

Descripción: Filetto 1.0 FTP server contains a denial of service vulnerability in the FEAT command processing that allows attackers to crash the service. Attackers can send an oversized FEAT command with 11,008 bytes of repeated characters to trigger a buffer overflow and terminate the FTP service.

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-770

Tecnología: No especificado

Publicado el: 2026-02-03

CVE-2020-37068

Descripción: Konica Minolta FTP Utility 1.0 contains a buffer overflow vulnerability in the LIST command that allows attackers to overwrite system registers. Attackers can send an oversized buffer of 1500 'A' characters to crash the FTP server and potentially 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-120

Tecnología: No especificado

Publicado el: 2026-02-03

CVE-2020-37069

Descripción: Konica Minolta FTP Utility 1.0 contains a buffer overflow vulnerability in the NLST command that allows attackers to overwrite system registers. Attackers can send an oversized buffer of 1500 'A' characters to crash the FTP server and potentially 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-120

Tecnología: No especificado

Publicado el: 2026-02-03

CVE-2020-37070

Descripción: CloudMe 1.11.2 contains a buffer overflow vulnerability that allows remote attackers to execute arbitrary code through crafted network packets. Attackers can exploit the vulnerability by sending a specially crafted payload to the CloudMe service running on port 8888, enabling remote code execution.

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: 2026-02-03

CVE-2020-37071

Descripción: CraftCMS 3 vCard Plugin 1.0.0 contains a deserialization vulnerability that allows unauthenticated attackers to execute arbitrary PHP code through a crafted payload. Attackers can generate a malicious serialized payload that triggers remote code execution by exploiting the plugin's vCard download functionality with a specially crafted request.

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: 2026-02-03

CVE-2020-37074

Descripción: Remote Desktop Audit 2.3.0.157 contains a buffer overflow vulnerability that allows attackers to execute arbitrary code during the Add Computers Wizard file import process. Attackers can craft a malicious payload file to trigger a structured exception handler (SEH) bypass and execute shellcode when importing computer lists.

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: 2026-02-03

CVE-2020-37075

Descripción: LanSend 3.2 contains a buffer overflow vulnerability in the Add Computers Wizard file import functionality that allows remote attackers to execute arbitrary code. Attackers can craft a malicious payload file to trigger a structured exception handler (SEH) overwrite and execute shellcode when importing computers from a file.

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: 2026-02-03

CVE-2020-37080

Descripción: webTareas 2.0.p8 contains a file deletion vulnerability in the print_layout.php administration component that allows authenticated attackers to delete arbitrary files. Attackers can exploit the vulnerability by manipulating the 'atttmp1' parameter to specify and delete files on the server through an unauthenticated file deletion 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-73

Tecnología: No especificado

Publicado el: 2026-02-03

CVE-2020-37082

Descripción: webERP 4.15.1 contains an unauthenticated file access vulnerability that allows remote attackers to download database backup files without authentication. Attackers can directly access generated backup files in the companies/weberp/ directory by requesting the Backup_[timestamp].sql.gz file.

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-552

Tecnología: No especificado

Publicado el: 2026-02-03

CVE-2020-37089

Descripción: School ERP Pro 1.0 contains a SQL injection vulnerability in the 'es_messagesid' parameter that allows attackers to manipulate database queries through GET requests. Attackers can exploit the vulnerable parameter by injecting crafted SQL statements to potentially extract, modify, or delete database information.

CVSS: 8.2 (HIGH)

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

Tipo: CWE-89

Tecnología: No especificado

Publicado el: 2026-02-03

CVE-2020-37090

Descripción: School ERP Pro 1.0 contains a file upload vulnerability that allows students to upload arbitrary PHP files to the messaging system. Attackers can upload malicious PHP scripts through the message attachment feature, enabling remote 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: 2026-02-03

CVE-2020-37094

Descripción: EspoCRM 5.8.5 contains an authentication vulnerability that allows attackers to access other user accounts by manipulating authorization headers. Attackers can decode and modify Basic Authorization and Espo-Authorization tokens to gain unauthorized access to administrative user information and 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-639

Tecnología: No especificado

Publicado el: 2026-02-03

CVE-2025-5329

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Martcode Software Inc. Delta Course Automation allows SQL Injection.This issue affects Delta Course Automation: through 04022026.

NOTE: 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-89

Tecnología: No especificado

Publicado el: 2026-02-04

CVE-2026-25049

Descripción: n8n is an open source workflow automation platform. Prior to versions 1.123.17 and 2.5.2, an authenticated user with permission to create or modify workflows could abuse crafted expressions in workflow parameters to trigger unintended system command execution on the host running n8n. This issue has been patched in versions 1.123.17 and 2.5.2.

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-913

Tecnología: No especificado

Publicado el: 2026-02-04

CVE-2026-25052

Descripción: n8n is an open source workflow automation platform. Prior to versions 1.123.18 and 2.5.0, a vulnerability in the file access controls allows authenticated users with permission to create or modify workflows to read sensitive files from the n8n host system. This can be exploited to obtain critical configuration data and user credentials, leading to complete account takeover of any user on the in...

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-367

Tecnología: No especificado

Publicado el: 2026-02-04

CVE-2026-25053

Descripción: n8n is an open source workflow automation platform. Prior to versions 1.123.10 and 2.5.0, vulnerabilities in the Git node allowed authenticated users with permission to create or modify workflows to execute arbitrary system commands or read arbitrary files on the n8n host. This issue has been patched in versions 1.123.10 and 2.5.0.

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-78

Tecnología: No especificado

Publicado el: 2026-02-04

CVE-2026-25115

Descripción: n8n is an open source workflow automation platform. Prior to version 2.4.8, a vulnerability in the Python Code node allows authenticated users to break out of the Python sandbox environment and execute code outside the intended security boundary. This issue has been patched in version 2.4.8.

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-693

Tecnología: No especificado

Publicado el: 2026-02-04

CVE-2026-22247

Descripción: GLPI is a free asset and IT management software package. From version 11.0.0 to before 11.0.5, a GLPI administrator can perform SSRF request through the Webhook feature. This issue has been patched in version 11.0.5.

CVSS: 4.1 (MEDIUM)

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

Tipo: CWE-918

Tecnología: No especificado

Publicado el: 2026-02-04

CVE-2025-13375

Descripción: IBM Common Cryptographic Architecture (CCA) 7.5.52 and 8.4.82 could allow an unauthenticated user to execute arbitrary commands with elevated privileges on the 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-250

Tecnología: No especificado

Publicado el: 2026-02-04

CVE-2020-37119

Descripción: Nsauditor 3.0.28 and 3.2.1.0 contains a buffer overflow vulnerability in the DNS Lookup tool that allows attackers to execute arbitrary code by overwriting memory. Attackers can craft a malicious DNS query payload to trigger a three-byte overwrite, bypass ASLR, and execute shellcode through a carefully constructed exploit.

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: 2026-02-05

CVE-2020-37120

Descripción: Rubo DICOM Viewer 2.0 contains a buffer overflow vulnerability in the DICOM server name input field that allows attackers to overwrite Structured Exception Handler (SEH). Attackers can craft a malicious text file with carefully constructed payload to execute arbitrary code by overwriting SEH and triggering remote code execution.

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: 2026-02-05

CVE-2020-37123

Descripción: Pinger 1.0 contains a remote code execution vulnerability that allows attackers to inject shell commands through the ping and socket parameters. Attackers can exploit the unsanitized input in ping.php to write arbitrary PHP files and execute system commands by appending shell metacharacters.

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: 2026-02-05

CVE-2020-37124

Descripción: B64dec 1.1.2 contains a buffer overflow vulnerability that allows attackers to execute arbitrary code by overwriting Structured Exception Handler (SEH) with crafted input. Attackers can leverage an egg hunter technique and carefully constructed payload to inject and execute malicious code during base64 decoding process.

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: 2026-02-05

CVE-2020-37125

Descripción: Edimax EW-7438RPn-v3 Mini 1.27 contains a remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary commands through the /goform/mp endpoint. Attackers can exploit the vulnerability by sending crafted POST requests with command injection payloads to download and execute malicious scripts on the device.

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: 2026-02-05

CVE-2020-37126

Descripción: Free Desktop Clock 3.0 contains a stack overflow vulnerability in the Time Zones display name input that allows attackers to overwrite Structured Exception Handler (SEH) registers. Attackers can exploit the vulnerability by crafting a malicious Unicode input that triggers an access violation and potentially execute arbitrary 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-121

Tecnología: No especificado

Publicado el: 2026-02-05

CVE-2020-37129

Descripción: Memu Play 7.1.3 contains an insecure folder permissions vulnerability that allows low-privileged users to modify the MemuService.exe executable. Attackers can replace the service executable with a malicious file during system restart to gain SYSTEM-level privileges by exploiting unrestricted file modification permissions.

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-276

Tecnología: No especificado

Publicado el: 2026-02-05

CVE-2020-37137

Descripción: PHP-Fusion 9.03.50 contains a remote code execution vulnerability in the 'add_panel_form()' function that allows attackers to execute arbitrary code through an eval() function with unsanitized POST data. Attackers can exploit the vulnerability by sending crafted panel_content POST parameters to the panels.php administration endpoint to execute malicious code.

CVSS: 6.1 (MEDIUM)

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

Tipo: CWE-95

Tecnología: No especificado

Publicado el: 2026-02-05

CVE-2020-37138

Descripción: 10-Strike Network Inventory Explorer 9.03 contains a buffer overflow vulnerability in the file import functionality that allows remote attackers to execute arbitrary code. Attackers can craft a malicious text file with carefully constructed payload to trigger a stack-based buffer overflow and bypass data execution prevention through a ROP chain.

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: 2026-02-05

CVE-2025-68723

Descripción: Axigen Mail Server before 10.5.57 contains multiple stored Cross-Site Scripting (XSS) vulnerabilities in the WebAdmin interface. Three instances exist: (1) the log file name parameter in the Local Services Log page, (2) certificate file content in the SSL Certificates View Usage feature, and (3) the Certificate File name parameter in the WebMail Listeners SSL settings. Attackers can inject mali...

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-79

Tecnología: No especificado

Publicado el: 2026-02-05

CVE-2025-68121

Descripción: During session resumption in crypto/tls, if the underlying Config has its ClientCAs or RootCAs fields mutated between the initial handshake and the resumed handshake, the resumed handshake may succeed when it should have failed. This may happen when a user calls Config.Clone and mutates the returned Config, or uses Config.GetConfigForClient. This can cause a client to resume a session with a se...

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-295

Tecnología: No especificado

Publicado el: 2026-02-05

CVE-2026-24300

Descripción: Azure Front Door Elevation of Privilege Vulnerability

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-284

Tecnología: No especificado

Publicado el: 2026-02-05

CVE-2026-1499

Descripción: The WP Duplicate plugin for WordPress is vulnerable to Missing Authorization leading to Arbitrary File Upload in all versions up to and including 1.1.8. This is due to a missing capability check on the `process_add_site()` AJAX action combined with path traversal in the file upload functionality. This makes it possible for authenticated (subscriber-level) attackers to set the internal `prod_key...

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-862

Tecnología: No especificado

Publicado el: 2026-02-06

CVE-2026-2017

Descripción: A vulnerability was detected in IP-COM W30AP up to 1.0.0.11(1340). Affected by this issue is the function R7WebsSecurityHandler of the file /goform/wx3auth of the component POST Request Handler. The manipulation of the argument data results in stack-based buffer overflow. The attack may be performed from remote. The exploit is now public and may be used. The vendor was contacted early about thi...

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: 2026-02-06

CVE-2026-25722

Descripción: Claude Code is an agentic coding tool. Prior to version 2.0.57, Claude Code failed to properly validate directory changes when combined with write operations to protected folders. By using the cd command to navigate into sensitive directories like .claude, it was possible to bypass write protection and create or modify files without user confirmation. Reliably exploiting this required the abili...

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-20

Tecnología: No especificado

Publicado el: 2026-02-06

CVE-2026-25725

Descripción: Claude Code is an agentic coding tool. Prior to version 2.1.2, Claude Code's bubblewrap sandboxing mechanism failed to properly protect the .claude/settings.json configuration file when it did not exist at startup. While the parent directory was mounted as writable and .claude/settings.local.json was explicitly protected with read-only constraints, settings.json was not protected if it was miss...

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-501

Tecnología: No especificado

Publicado el: 2026-02-06

CVE-2026-25752

Descripción: FUXA is a web-based Process Visualization (SCADA/HMI/Dashboard) software. An authorization bypass vulnerability in FUXA allows an unauthenticated, remote attacker to modify device tags via WebSockets. Exploitation allows an unauthenticated, remote attacker to bypass role-based access controls and overwrite arbitrary device tags or disable communication drivers, exposing connected ICS/SCADA envi...

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: 2026-02-06

CVE-2020-37095

Descripción: Cyberoam Authentication Client 2.1.2.7 contains a buffer overflow vulnerability that allows remote attackers to execute arbitrary code by overwriting Structured Exception Handler (SEH) memory. Attackers can craft a malicious input in the 'Cyberoam Server Address' field to trigger a bind TCP shell on port 1337 with system-level access.

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: 2026-02-07

CVE-2020-37159

Descripción: Parallaxis Cuckoo Clock 5.0 contains a buffer overflow vulnerability that allows attackers to execute arbitrary code by overwriting memory registers in the alarm scheduling feature. Attackers can craft a malicious payload exceeding 260 bytes to overwrite EIP and EBP, enabling shellcode execution with potential remote code execution.

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: 2026-02-07

CVE-2020-37161

Descripción: Wedding Slideshow Studio 1.36 contains a buffer overflow vulnerability that allows attackers to execute arbitrary code by overwriting the registration name field with malicious payload. Attackers can craft a specially designed payload to trigger remote code execution, demonstrating the ability to run system commands like launching the calculator.

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: 2026-02-07

CVE-2020-37162

Descripción: Wedding Slideshow Studio 1.36 contains a buffer overflow vulnerability in the registration key input that allows attackers to execute arbitrary code by overwriting memory. Attackers can craft a malicious payload of 1608 bytes to trigger a stack-based buffer overflow and execute commands through the registration key field.

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-122

Tecnología: No especificado

Publicado el: 2026-02-07

CVE-2026-2087

Descripción: A flaw has been found in SourceCodester Online Class Record System 1.0. Affected by this issue is some unknown functionality of the file /admin/login.php. This manipulation of the argument user_email causes sql injection. The attack may be initiated remotely. The exploit has been published 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: 2026-02-07

CVE-2026-2088

Descripción: A vulnerability has been found in PHPGurukul Beauty Parlour Management System 1.1. This affects an unknown part of the file /admin/accepted-appointment.php. Such manipulation of the argument delid 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: 2026-02-07

CVE-2026-2089

Descripción: A vulnerability was found in SourceCodester Online Class Record System 1.0. This vulnerability affects unknown code of the file /admin/subject/controller.php. Performing a manipulation of the argument ID results in sql injection. Remote exploitation of the attack is possible. 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: 2026-02-07

CVE-2026-2090

Descripción: A vulnerability was determined in SourceCodester Online Class Record System 1.0. This issue affects some unknown processing of the file /admin/message/search.php. Executing a manipulation of the argument term 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: 2026-02-07

CVE-2026-2114

Descripción: A vulnerability was detected in itsourcecode Society Management System 1.0. This vulnerability affects unknown code of the file /admin/edit_admin.php. The manipulation of the argument admin_id results in sql injection. The attack may be performed from remote. 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: 2026-02-07

CVE-2026-2115

Descripción: A flaw has been found in itsourcecode Society Management System 1.0. This issue affects some unknown processing of the file /admin/delete_expenses.php. This manipulation of the argument expenses_id causes sql injection. It is possible to initiate the attack remotely. The exploit has been published 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: 2026-02-07

CVE-2026-2116

Descripción: A vulnerability has been found in itsourcecode Society Management System 1.0. Impacted is an unknown function of the file /admin/edit_expenses.php. Such manipulation of the argument expenses_id 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: 2026-02-08

CVE-2026-2117

Descripción: A vulnerability was found in itsourcecode Society Management System 1.0. The affected element is an unknown function of the file /admin/edit_activity.php. Performing a manipulation of the argument activity_id results in sql injection. The attack can be initiated 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: 2026-02-08

CVE-2025-15027

Descripción: The JAY Login & Register plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 2.6.03. This is due to the plugin allowing a user to update arbitrary user meta through the 'jay_login_register_ajax_create_final_user' function. This makes it possible for unauthenticated attackers to elevate their privileges to that of an administrator.

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: 2026-02-08

CVE-2026-2132

Descripción: A security flaw has been discovered in code-projects Online Music Site 1.0. This issue affects some unknown processing of the file /Administrator/PHP/AdminUpdateCategory.php. The manipulation of the argument txtcat 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: 2026-02-08

CVE-2026-2133

Descripción: A weakness has been identified in code-projects Online Music Site 1.0. Impacted is an unknown function of the file /Administrator/PHP/AdminUpdateCategory.php. This manipulation of the argument txtimage causes unrestricted upload. The attack is possible to be carried out remotely. The exploit has been made available to the public and could 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-284

Tecnología: No especificado

Publicado el: 2026-02-08

CVE-2026-2161

Descripción: A vulnerability was found in itsourcecode Directory Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/forget-password.php. The manipulation of the argument email 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: 2026-02-08

CVE-2026-2166

Descripción: A security vulnerability has been detected in code-projects Online Reviewer System 1.0. The affected element is an unknown function of the file /login/index.php of the component Login. The manipulation of the argument username/password leads to sql injection. The attack is possible to be carried out 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: 2026-02-08

CVE-2026-2171

Descripción: A vulnerability was found in code-projects Online Student Management System 1.0. Affected is an unknown function of the file accounts.php of the component Login. Performing a manipulation of the argument username/password results in sql injection. The attack can be initiated 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: 2026-02-08

CVE-2026-2189

Descripción: A vulnerability was identified in itsourcecode School Management System 1.0. This affects an unknown function of the file /ramonsys/report/index.php. The manipulation of the argument ay 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: 2026-02-08

CVE-2026-2190

Descripción: A security flaw has been discovered in itsourcecode School Management System 1.0. This impacts an unknown function of the file /ramonsys/user/controller.php. The manipulation of the argument ID results in sql injection. The attack can 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: 2026-02-08

CVE-2026-2195

Descripción: A vulnerability has been found in code-projects Online Reviewer System 1.0. This vulnerability affects unknown code of the file /system/system/admins/assessments/pretest/questions-view.php. The manipulation of the argument ID leads to sql injection. The attack is possible to be carried out 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: 2026-02-09

CVE-2026-2196

Descripción: A vulnerability was found in code-projects Online Reviewer System 1.0. This issue affects some unknown processing of the file /system/system/admins/assessments/pretest/exam-update.php. The manipulation of the argument test_id results in sql injection. The attack may be performed from remote. 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: 2026-02-09

CVE-2026-2197

Descripción: A vulnerability was determined in code-projects Online Reviewer System 1.0. Impacted is an unknown function of the file /system/system/admins/assessments/pretest/exam-delete.php. This manipulation of the argument test_id causes sql injection. It is possible to initiate 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: 2026-02-09

CVE-2026-2198

Descripción: A vulnerability was identified in code-projects Online Reviewer System 1.0. The affected element is an unknown function of the file /system/system/admins/assessments/pretest/loaddata.php. Such manipulation of the argument difficulty_id leads to sql injection. It is possible to launch the attack 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: 2026-02-09

CVE-2026-2199

Descripción: A security flaw has been discovered in code-projects Online Reviewer System 1.0. The impacted element is an unknown function of the file /reviewer/system/system/admins/manage/users/user-delete.php. Performing a manipulation of the argument ID results in sql injection. The attack can be initiated 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: 2026-02-09

CVE-2026-2211

Descripción: A vulnerability was determined in code-projects Online Music Site 1.0. Affected is an unknown function of the file /Administrator/PHP/AdminDeleteCategory.php. Executing a manipulation of the argument ID 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: 2026-02-09

CVE-2026-2212

Descripción: A vulnerability was identified in code-projects Online Music Site 1.0. Affected by this vulnerability is an unknown functionality of the file /Administrator/PHP/AdminEditCategory.php. The manipulation of the argument ID leads to sql injection. The attack is possible to be carried out 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: 2026-02-09

CVE-2026-2217

Descripción: A vulnerability was found in itsourcecode Event Management System 1.0. The impacted element is an unknown function of the file /admin/manage_user.php. The manipulation of the argument ID results in sql injection. The attack may 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: 2026-02-09

CVE-2026-2220

Descripción: A vulnerability was identified in code-projects Online Reviewer System 1.0. This impacts an unknown function of the file /system/system/admins/assessments/pretest/btn_functions.php. Such manipulation of the argument difficulty_id leads to sql injection. The attack can be executed 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: 2026-02-09

CVE-2026-2221

Descripción: A security flaw has been discovered in code-projects Online Reviewer System 1.0. Affected is an unknown function of the file /login/index.php of the component Login. Performing a manipulation of the argument Username results in sql injection. The attack is possible to be carried out 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: 2026-02-09

CVE-2026-22903

Descripción: An unauthenticated remote attacker can send a crafted HTTP request containing an overly long SESSIONID cookie. This can trigger a stack buffer overflow in the modified lighttpd server, causing it to crash and potentially enabling remote code execution due to missing stack protections.

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: 2026-02-09

CVE-2026-22904

Descripción: Improper length handling when parsing multiple cookie fields (including TRACKID) allows an unauthenticated remote attacker to send oversized cookie values and trigger a stack buffer overflow, resulting in a denial-of-service condition and possible remote code execution.

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: 2026-02-09

CVE-2026-22906

Descripción: User credentials are stored using AES-ECB encryption with a hardcoded key. An unauthenticated remote attacker obtaining the configuration file can decrypt and recover plaintext usernames and passwords, especially when combined with the authentication bypass.

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-321

Tecnología: No especificado

Publicado el: 2026-02-09

CVE-2026-2223

Descripción: A security vulnerability has been detected in code-projects Online Reviewer System 1.0. Affected by this issue is some unknown functionality of the file /system/system/students/assessments/pretest/take/index.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack 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: 2026-02-09

CVE-2026-2234

Descripción: C&Cm@il developed by HGiga has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to read and modify any user's mail content.

CVSS: 9.1 (CRITICAL)

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

Tipo: CWE-306

Tecnología: No especificado

Publicado el: 2026-02-09

CVE-2025-6830

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Xpoda Türkiye Information Technology Inc. Xpoda Studio allows SQL Injection.This issue affects Xpoda Studio: through 09022026. NOTE: 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-89

Tecnología: No especificado

Publicado el: 2026-02-09

CVE-2026-24677

Descripción: FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.22.0, ecam_encoder_compress_h264 trusts server-controlled dimensions and does not validate the source buffer size, leading to an out-of-bounds read in sws_scale. This vulnerability is fixed in 3.22.0.

CVSS: 9.1 (CRITICAL)

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

Tipo: CWE-416

Tecnología: No especificado

Publicado el: 2026-02-09

CVE-2026-24679

Descripción: FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.22.0, The URBDRC client uses server-supplied interface numbers as array indices without bounds checks, causing an out-of-bounds read in libusb_udev_select_interface. This vulnerability is fixed in 3.22.0.

CVSS: 9.1 (CRITICAL)

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

Tipo: CWE-122

Tecnología: No especificado

Publicado el: 2026-02-09

CVE-2026-0488

Descripción: An authenticated attacker in SAP CRM and SAP S/4HANA (Scripting Editor) could exploit a flaw in a generic function module call and execute unauthorized critical functionalities, which includes the ability to execute an arbitrary SQL statement. This leads to a full database compromise with high impact on confidentiality, integrity, and availability.

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-862

Tecnología: No especificado

Publicado el: 2026-02-10

CVE-2026-0509

Descripción: SAP NetWeaver Application Server ABAP and ABAP Platform allows an authenticated, low-privileged user to perform background Remote Function Calls without the required S_RFC authorization in certain cases. This can result in a high impact on integrity and availability, and no impact on the confidentiality of the application.

CVSS: 9.6 (CRITICAL)

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

Tipo: CWE-862

Tecnología: No especificado

Publicado el: 2026-02-10

CVE-2026-2095

Descripción: Agentflow developed by Flowring has an Authentication Bypass vulnerability, allowing unauthenticated remote attackers to exploit a specific functionality to obtain arbitrary user authentication token and log into the system as any 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-288

Tecnología: No especificado

Publicado el: 2026-02-10

CVE-2026-2096

Descripción: Agentflow developed by Flowring 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-288

Tecnología: No especificado

Publicado el: 2026-02-10

CVE-2025-11242

Descripción: Server-Side Request Forgery (SSRF) vulnerability in Teknolist Computer Systems Software Publishing Industry and Trade Inc. Okulistik allows Server Side Request Forgery.This issue affects Okulistik: through 21102025.

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-918

Tecnología: No especificado

Publicado el: 2026-02-10

Resumen del Reporte

CVEs analizados: 91

Promedio CVSS: 8.92

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat