CVEs más relevantes de la semana

Del 31/01/2026 al 07/02/2026

Porque el primer paso para defender es conocer las amenazas.

CVE-2022-50981

Descripción: An unauthenticated remote attacker can gain full access on the affected devices as they are shipped without a password by default and setting one is not enforced.

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: 2026-02-02

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-2020-37090

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-2020-37138

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-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-2026-1709

Descripción: A flaw was found in Keylime. The Keylime registrar, since version 7.12.0, does not enforce client-side Transport Layer Security (TLS) authentication. This authentication bypass vulnerability allows unauthenticated clients with network access to perform administrative operations, including listing agents, retrieving public Trusted Platform Module (TPM) data, and deleting agents, by connecting wi...

CVSS: 9.4 (CRITICAL)

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

Tipo: CWE-322

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

Resumen del Reporte

CVEs analizados: 44

Promedio CVSS: 9.65

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat ▯