CVEs más relevantes de la semana

Del 10/02/2026 al 17/02/2026

Porque el primer paso para defender es conocer las amenazas.

CVE-2026-21531

Descripción: Deserialization of untrusted data in Azure SDK allows an unauthorized attacker to execute code over a network.

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: 2026-02-10

CVE-2026-1357

Descripción: The Migration, Backup, Staging – WPvivid Backup & Migration plugin for WordPress is vulnerable to Unauthenticated Arbitrary File Upload in versions up to and including 0.9.123. This is due to improper error handling in the RSA decryption process combined with a lack of path sanitization when writing uploaded files. When the plugin fails to decrypt a session key using openssl_private_decrypt(), ...

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: 2026-02-11

CVE-2025-7659

Descripción: GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.2 before 18.6.6, 18.7 before 18.7.4, and 18.8 before 18.8.4 that could have allowed an unauthenticated user to steal tokens and access private repositories by abusing incomplete validation in the Web IDE.

CVSS: 8.0 (HIGH)

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

Tipo: CWE-346

Tecnología: No especificado

Publicado el: 2026-02-11

CVE-2025-66277

Descripción: A link following vulnerability has been reported to affect several QNAP operating system versions. The remote attackers can then exploit the vulnerability to traverse the file system to unintended locations.

We have already fixed the vulnerability in the following versions: QTS 5.2.8.3350 build 20251216 and later QuTS hero h5.3.2.3354 build 20251225 and later QuTS hero h5.2.8.3350 build 202512...

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-59

Tecnología: No especificado

Publicado el: 2026-02-11

CVE-2025-8025

Descripción: Missing Authentication for Critical Function, Improper Access Control vulnerability in Dinosoft Business Solutions Dinosoft ERP allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Dinosoft ERP: from < 3.0.1 through 11022026.

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-284

Tecnología: No especificado

Publicado el: 2026-02-11

CVE-2025-8668

Descripción: Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in E-Kalite Software Hardware Engineering Design and Internet Services Industry and Trade Ltd. Co. Turboard allows Reflected XSS.This issue affects Turboard: from 2025.07 through 11022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.

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-79

Tecnología: No especificado

Publicado el: 2026-02-11

CVE-2020-37153

Descripción: ASTPP 4.0.1 contains multiple vulnerabilities including cross-site scripting and command injection in SIP device configuration and plugin management interfaces. Attackers can exploit these flaws to inject system commands, hijack administrator sessions, and potentially execute arbitrary code with root permissions through cron task manipulation.

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-79

Tecnología: No especificado

Publicado el: 2026-02-11

CVE-2020-37176

Descripción: Torrent 3GP Converter 1.51 contains a stack overflow vulnerability that allows attackers to execute arbitrary code by overwriting Structured Exception Handler (SEH) registers. Attackers can craft a malicious payload targeting the application's registration dialog to trigger code execution and open the calculator through carefully constructed buffer overflow techniques.

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: 2026-02-11

CVE-2020-37181

Descripción: Torrent FLV Converter 1.51 Build 117 contains a stack overflow vulnerability that allows attackers to overwrite Structured Exception Handler (SEH) through a malicious registration code input. Attackers can craft a payload with specific offsets and partial SEH overwrite techniques to potentially execute arbitrary code on vulnerable Windows 32-bit systems.

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: 2026-02-11

CVE-2020-37183

Descripción: Allok RM RMVB to AVI MPEG DVD Converter 3.6.1217 contains a stack overflow vulnerability that allows attackers to execute arbitrary code by overwriting Structured Exception Handler (SEH) registers. Attackers can craft a malicious payload in the License Name input field to trigger a buffer overflow and execute system commands like calc.exe.

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: 2026-02-11

CVE-2020-37184

Descripción: Allok Video Converter 4.6.1217 contains a stack overflow vulnerability in the License Name input field that allows attackers to execute arbitrary code. Attackers can craft a specially designed payload to overwrite SEH handlers and execute system commands by injecting malicious bytecode into the input 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-121

Tecnología: No especificado

Publicado el: 2026-02-11

CVE-2020-37186

Descripción: Chevereto 3.13.4 Core contains a remote code execution vulnerability that allows attackers to inject malicious code during database configuration installation. Attackers can manipulate the database table prefix parameter to write a PHP shell file and execute arbitrary system commands through a crafted POST 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-94

Tecnología: No especificado

Publicado el: 2026-02-11

CVE-2026-26014

Descripción: Pion DTLS is a Go implementation of Datagram Transport Layer Security. Pion DTLS versions v1.0.0 through v3.0.10 and 3.1.0 use random nonce generation with AES GCM ciphers, which makes it easier for remote attackers to obtain the authentication key and spoof data by leveraging the reuse of a nonce in a session and a "forbidden attack". Upgrade to v3.0.11, v3.1.1, or later.

CVSS: 5.9 (MEDIUM)

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

Tipo: CWE-200

Tecnología: No especificado

Publicado el: 2026-02-11

CVE-2026-26021

Descripción: set-in provides the set value of nested associative structure given array of keys. A prototype pollution vulnerability exists in the the npm package set-in (>=2.0.1, < 2.0.5). Despite a previous fix that attempted to mitigate prototype pollution by checking whether user input contained a forbidden key, it is still possible to pollute Object.prototype via a crafted input using Array.prototype. T...

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-1321

Tecnología: No especificado

Publicado el: 2026-02-11

CVE-2026-20677

Descripción: A race condition was addressed with improved handling of symbolic links. This issue is fixed in macOS Tahoe 26.3, macOS Sonoma 14.8.4, iOS 18.7.5 and iPadOS 18.7.5, visionOS 26.3, iOS 26.3 and iPadOS 26.3. A shortcut may be able to bypass sandbox restrictions.

CVSS: 9.0 (CRITICAL)

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

Tipo: CWE-362

Tecnología: No especificado

Publicado el: 2026-02-11

CVE-2026-1729

Descripción: The AdForest theme for WordPress is vulnerable to authentication bypass in all versions up to, and including, 6.0.12. This is due to the plugin not properly verifying a user's identity prior to authenticating them through the 'sb_login_user_with_otp_fun' function. This makes it possible for unauthenticated attackers to log in as arbitrary users, including administrators.

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: 2026-02-12

CVE-2025-10969

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Farktor Software E-Commerce Services Inc. E-Commerce Package allows Blind SQL Injection.This issue affects E-Commerce Package: through 27112025.

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: 2026-02-12

CVE-2025-14014

Descripción: Unrestricted Upload of File with Dangerous Type vulnerability in NTN Information Processing Services Computer Software Hardware Industry and Trade Ltd. Co. Smart Panel allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Smart Panel: before 20251215.

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: 2026-02-12

CVE-2026-26216

Descripción: Crawl4AI versions prior to 0.8.0 contain a remote code execution vulnerability in the Docker API deployment. The /crawl endpoint accepts a hooks parameter containing Python code that is executed using exec(). The __import__ builtin was included in the allowed builtins, allowing unauthenticated remote attackers to import arbitrary modules and execute system commands. Successful exploitation allo...

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-94

Tecnología: No especificado

Publicado el: 2026-02-12

CVE-2026-26218

Descripción: newbee-mall includes pre-seeded administrator accounts in its database initialization script. These accounts are provisioned with a predictable default password. Deployments that initialize or reset the database using the provided schema and fail to change the default administrative credentials may allow unauthenticated attackers to log in as an administrator and gain full administrative contro...

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: 2026-02-12

CVE-2026-26219

Descripción: newbee-mall stores and verifies user passwords using an unsalted MD5 hashing algorithm. The implementation does not incorporate per-user salts or computational cost controls, enabling attackers who obtain password hashes through database exposure, backup leakage, or other compromise vectors to rapidly recover plaintext credentials via offline attacks.

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-327

Tecnología: No especificado

Publicado el: 2026-02-12

CVE-2019-25319

Descripción: Domain Quester Pro 6.02 contains a stack overflow vulnerability that allows remote attackers to execute arbitrary code by overwriting Structured Exception Handler (SEH) registers. Attackers can craft a malicious payload targeting the 'Domain Name Keywords' input field to trigger an access violation and execute a bind shell on port 9999.

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: 2026-02-12

CVE-2019-25321

Descripción: FTP Navigator 8.03 contains a stack overflow vulnerability that allows attackers to execute arbitrary code by overwriting Structured Exception Handler (SEH) registers. Attackers can craft a malicious payload that triggers a buffer overflow when pasted into the Custom Command textbox, enabling remote code execution and launching the calculator as proof of concept.

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: 2026-02-12

CVE-2019-25327

Descripción: Prime95 version 29.8 build 6 contains a buffer overflow vulnerability in the user ID input field that allows remote attackers to execute arbitrary code. Attackers can craft a malicious payload and paste it into the PrimeNet user ID and proxy host fields to trigger a bind shell on port 3110.

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: 2026-02-12

CVE-2019-25337

Descripción: OwnCloud 8.1.8 contains a username enumeration vulnerability that allows remote attackers to discover user accounts by manipulating the share.php endpoint. Attackers can send crafted GET requests to /index.php/core/ajax/share.php with a wildcard search parameter to retrieve comprehensive user 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-203

Tecnología: No especificado

Publicado el: 2026-02-12

CVE-2020-37167

Descripción: ClamAV ClamBC bytecode interpreter contains a vulnerability in function name processing that allows attackers to manipulate bytecode function names. Attackers can exploit the weak input validation in function name encoding to potentially execute malicious bytecode or cause unexpected behavior in the ClamAV engine.

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-94

Tecnología: No especificado

Publicado el: 2026-02-12

CVE-2026-1306

Descripción: The midi-Synth plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type and file extension validation in the 'export' AJAX action in all versions up to, and including, 1.1.0. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible granted the attacker can obtain a vali...

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: 2026-02-14

CVE-2025-8572

Descripción: The Truelysell Core plugin for WordPress is vulnerable to privilege escalation in versions less than, or equal to, 1.8.7. This is due to insufficient validation of the user_role parameter during user registration. This makes it possible for unauthenticated attackers to create accounts with elevated privileges, including administrator 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-269

Tecnología: No especificado

Publicado el: 2026-02-14

CVE-2026-1490

Descripción: The Spam protection, Anti-Spam, FireWall by CleanTalk plugin for WordPress is vulnerable to unauthorized Arbitrary Plugin Installation due to an authorization bypass via reverse DNS (PTR record) spoofing on the 'checkWithoutToken' function in all versions up to, and including, 6.71. This makes it possible for unauthenticated attackers to install and activate arbitrary plugins which can be lever...

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-350

Tecnología: No especificado

Publicado el: 2026-02-15

CVE-2026-26366

Descripción: eNet SMART HOME server 2.2.1 and 2.3.1 ships with default credentials (user:user, admin:admin) that remain active after installation and commissioning without enforcing a mandatory password change. Unauthenticated attackers can use these default credentials to gain administrative access to sensitive smart home configuration and control functions.

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-1392

Tecnología: No especificado

Publicado el: 2026-02-15

CVE-2026-26369

Descripción: eNet SMART HOME server 2.2.1 and 2.3.1 contains a privilege escalation vulnerability due to insufficient authorization checks in the setUserGroup JSON-RPC method. A low-privileged user (UG_USER) can send a crafted POST request to /jsonrpc/management specifying their own username to elevate their account to the UG_ADMIN group, bypassing intended access controls and gaining administrative capabil...

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: 2026-02-15

CVE-2026-2550

Descripción: A vulnerability was found in EFM iptime A6004MX 14.18.2. Affected is the function commit_vpncli_file_upload of the file /cgi/timepro.cgi. The manipulation results in unrestricted upload. The attack may be performed from remote. The exploit has been made public and could 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-284

Tecnología: No especificado

Publicado el: 2026-02-16

Resumen del Reporte

CVEs analizados: 32

Promedio CVSS: 9.57

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat ▯