CVEs más relevantes de la semana

Del 14/02/2026 al 21/02/2026

Porque el primer paso para defender es conocer las amenazas.

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-2026-2521

Descripción: A weakness has been identified in Open5GS up to 2.7.6. This issue affects the function sgwc_s5c_handle_create_session_response of the component SGW-C. Executing a manipulation can lead to memory corruption. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue repor...

CVSS: 5.3 (MEDIUM)

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

Tipo: CWE-119

Tecnología: No especificado

Publicado el: 2026-02-15

CVE-2026-2522

Descripción: A security vulnerability has been detected in Open5GS up to 2.7.6. Impacted is an unknown function of the file /src/mme/esm-build.c of the component MME. The manipulation leads to memory corruption. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.

CVSS: 5.3 (MEDIUM)

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

Tipo: CWE-119

Tecnología: No especificado

Publicado el: 2026-02-16

CVE-2026-2527

Descripción: A vulnerability was determined in Wavlink WL-WN579A3 up to 20210219. Affected is an unknown function of the file /cgi-bin/login.cgi. Executing a manipulation of the argument key can lead to command injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.

CVSS: 6.3 (MEDIUM)

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

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2026-02-16

CVE-2026-2528

Descripción: A vulnerability was identified in Wavlink WL-WN579A3 up to 20210219. Affected by this vulnerability is the function Delete_Mac_list of the file /cgi-bin/wireless.cgi. The manipulation of the argument delete_list leads to command injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but ...

CVSS: 6.3 (MEDIUM)

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

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2026-02-16

CVE-2026-2529

Descripción: A security flaw has been discovered in Wavlink WL-WN579A3 up to 20210219. Affected by this issue is the function DeleteMac of the file /cgi-bin/wireless.cgi. The manipulation of the argument delete_list results in command injection. The attack can be executed remotely. The vendor was contacted early about this disclosure but did not respond in any way.

CVSS: 6.3 (MEDIUM)

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

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2026-02-16

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

CVE-2026-22208

Descripción: OpenS100 (the reference implementation S-100 viewer) prior to commit 753cf29 contain a remote code execution vulnerability via an unrestricted Lua interpreter. The Portrayal Engine initializes Lua using luaL_openlibs() without sandboxing or capability restrictions, exposing standard libraries such as 'os' and 'io' to untrusted portrayal catalogues. An attacker can provide a malicious S-100 port...

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-749

Tecnología: No especificado

Publicado el: 2026-02-17

CVE-2026-2616

Descripción: A vulnerability has been found in Beetel 777VR1 up to 01.00.09. The impacted element is an unknown function of the component Web Management Interface. The manipulation leads to hard-coded credentials. The attack needs to be initiated within the local network. The exploit has been disclosed to the public and may be used. It is advisable to modify the configuration settings. The vendor was contac...

CVSS: 8.8 (HIGH)

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

Tipo: CWE-259

Tecnología: No especificado

Publicado el: 2026-02-17

CVE-2026-23647

Descripción: Glory RBG-100 recycler systems using the ISPK-08 software component contain hard-coded operating system credentials that allow remote authentication to the underlying Linux system. Multiple local user accounts, including accounts with administrative privileges, were found to have fixed, embedded passwords. An attacker with network access to exposed services such as SSH may authenticate using th...

CVSS: 9.8 (CRITICAL)

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

Tipo: CWE-798

Tecnología: No especificado

Publicado el: 2026-02-17

CVE-2025-33089

Descripción: IBM Concert 1.0.0 through 2.1.0 could allow a remote attacker to obtain sensitive information or perform unauthorized actions due to the use of hard coded user credentials.

CVSS: 6.5 (MEDIUM)

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

Tipo: CWE-798

Tecnología: No especificado

Publicado el: 2026-02-17

CVE-2026-22769

Descripción: Dell RecoverPoint for Virtual Machines, versions prior to 6.0.3.1 HF1, contain a hardcoded credential vulnerability. This is considered critical as an unauthenticated remote attacker with knowledge of the hardcoded credential could potentially exploit this vulnerability leading to unauthorized access to the underlying operating system and root-level persistence. Dell recommends that customers u...

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-798

Tecnología: No especificado

Publicado el: 2026-02-17

CVE-2026-1937

Descripción: The YayMail – WooCommerce Email Customizer plugin for WordPress is vulnerable to unauthorized modification of data that can lead to privilege escalation due to a missing capability check on the `yaymail_import_state` AJAX action in all versions up to, and including, 4.3.2. This makes it possible for authenticated attackers, with Shop Manager-level access and above, to update arbitrary options o...

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: 2026-02-18

CVE-2026-1435

Descripción: Not properly invalidated session vulnerability in Graylog Web Interface, version 2.2.3, due to incorrect management of session invalidation after new logins. The application generates a new 'sessionId' each time a user authenticates, but does not invalidate previously issued session identifiers, which remain valid even after multiple consecutive logins by the same user. As a result, a stolen or...

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-613

Tecnología: No especificado

Publicado el: 2026-02-18

CVE-2026-2654

Descripción: A weakness has been identified in huggingface smolagents 1.24.0. Impacted is the function requests.get/requests.post of the component LocalPythonExecutor. Executing a manipulation can lead to server-side request forgery. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclos...

CVSS: 6.3 (MEDIUM)

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

Tipo: CWE-918

Tecnología: No especificado

Publicado el: 2026-02-18

CVE-2026-2329

Descripción: An unauthenticated stack-based buffer overflow vulnerability exists in the HTTP API endpoint /cgi-bin/api.values.get. A remote attacker can leverage this vulnerability to achieve unauthenticated remote code execution (RCE) with root privileges on a target device. The vulnerability affects all six device models in the series: GXP1610, GXP1615, GXP1620, GXP1625, GXP1628, and GXP1630.

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: 2026-02-18

CVE-2026-0573

Descripción: An URL redirection vulnerability was identified in GitHub Enterprise Server that allowed attacker-controlled redirects to leak sensitive authorization tokens. The repository_pages API insecurely followed HTTP redirects when fetching artifact URLs, preserving the authorization header containing a privileged JWT. An authenticated user could redirect these requests to an attacker-controlled domain...

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-601

Tecnología: No especificado

Publicado el: 2026-02-18

CVE-2019-25360

Descripción: Aida64 Engineer 6.10.5200 contains a buffer overflow vulnerability in the CSV logging configuration that allows attackers to execute malicious code by crafting a specially designed payload. Attackers can exploit the vulnerability by creating a malformed log file with carefully constructed SEH (Structured Exception Handler) overwrite techniques to achieve 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: 2026-02-18

CVE-2019-25361

Descripción: Ayukov NFTP client 1.71 contains a buffer overflow vulnerability in the SYST command handling that allows remote attackers to execute arbitrary code. Attackers can send a specially crafted SYST command with oversized payload to trigger a buffer overflow and execute a bind shell on port 5150.

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: 2026-02-18

CVE-2019-25362

Descripción: WMV to AVI MPEG DVD WMV Convertor 4.6.1217 contains a buffer overflow vulnerability that allows attackers to execute arbitrary code by overwriting the license name and license code fields. Attackers can craft a malicious payload of 6000 bytes to trigger a bind shell on port 4444 by exploiting a stack-based buffer overflow in the application's input handling.

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: 2026-02-18

CVE-2019-25364

Descripción: MailCarrier 2.51 contains a buffer overflow vulnerability in the POP3 USER command that allows remote attackers to execute arbitrary code. Attackers can send a crafted oversized buffer to the POP3 service, overwriting memory and potentially gaining remote system 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: 2026-02-18

CVE-2019-25365

Descripción: ChaosPro 2.0 contains a buffer overflow vulnerability in the configuration file path handling that allows attackers to execute arbitrary code by overwriting the Structured Exception Handler. Attackers can craft a malicious configuration file with carefully constructed payload to overwrite memory and gain remote code execution on vulnerable Windows XP 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: 2026-02-18

CVE-2026-27174

Descripción: MajorDoMo (aka Major Domestic Module) allows unauthenticated remote code execution via the admin panel's PHP console feature. An include order bug in modules/panel.class.php causes execution to continue past a redirect() call that lacks an exit statement, allowing unauthenticated requests to reach the ajax handler in inc_panel_ajax.php. The console handler within that file passes user-supplied ...

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: 2026-02-18

CVE-2026-27175

Descripción: MajorDoMo (aka Major Domestic Module) is vulnerable to unauthenticated OS command injection via rc/index.php. The $param variable from user input is interpolated into a command string within double quotes without sanitization via escapeshellarg(). The command is inserted into a database queue by safe_exec(), which performs no sanitization. The cycle_execs.php script, which is web-accessible wit...

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: 2026-02-18

CVE-2026-27179

Descripción: MajorDoMo (aka Major Domestic Module) contains an unauthenticated SQL injection vulnerability in the commands module. The commands_search.inc.php file directly interpolates the $_GET['parent'] parameter into multiple SQL queries without sanitization or parameterized queries. The commands module is loadable without authentication via the /objects/?module=commands endpoint, which includes arbitra...

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: 2026-02-18

CVE-2026-27180

Descripción: MajorDoMo (aka Major Domestic Module) is vulnerable to unauthenticated remote code execution through supply chain compromise via update URL poisoning. The saverestore module exposes its admin() method through the /objects/?module=saverestore endpoint without authentication because it uses gr('mode') (which reads directly from $_REQUEST) instead of the framework's $this->mode. An attacker can po...

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-494

Tecnología: No especificado

Publicado el: 2026-02-18

CVE-2026-24126

Descripción: Weblate is a web based localization tool. Prior to 5.16.0, the SSH management console did not validate the passed input while adding the SSH host key, which could lead to an argument injection to `ssh-add`. Version 5.16.0 fixes the issue. As a workaround, properly limit access to the management console.

CVSS: 6.6 (MEDIUM)

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

Tipo: CWE-88

Tecnología: No especificado

Publicado el: 2026-02-19

CVE-2026-2686

Descripción: A security vulnerability has been detected in SECCN Dingcheng G10 3.1.0.181203. This impacts the function qq of the file /cgi-bin/session_login.cgi. The manipulation of the argument User leads to os command injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.

CVSS: 9.8 (CRITICAL)

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

Tipo: CWE-77

Tecnología: No especificado

Publicado el: 2026-02-19

CVE-2025-12882

Descripción: The Clasifico Listing plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 2.0. This is due to the plugin allowing users who are registering new accounts to set their own role by supplying the 'listing_user_role' parameter. This makes it possible for unauthenticated attackers to gain elevated privileges by registering an account with the administrator role.

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: 2026-02-19

CVE-2025-13563

Descripción: The Lizza LMS Pro plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.0.3. This is due to the 'lizza_lms_pro_register_user_front_end' function not restricting what user roles a user can register with. This makes it possible for unauthenticated attackers to supply the 'administrator' role during registration and gain administrator access to the site.

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: 2026-02-19

CVE-2025-13851

Descripción: The Buyent Classified plugin for WordPress (bundled with Buyent theme) is vulnerable to privilege escalation via user registration in all versions up to, and including, 1.0.7. This is due to the plugin not validating or restricting the user role during registration via the REST API endpoint. This makes it possible for unauthenticated attackers to register accounts with arbitrary roles, includin...

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: 2026-02-19

CVE-2026-0926

Descripción: The Prodigy Commerce plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 3.2.9 via the 'parameters[template_name]' parameter. This makes it possible for unauthenticated attackers to include and read arbitrary files or execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access 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-98

Tecnología: No especificado

Publicado el: 2026-02-19

CVE-2026-1405

Descripción: The Slider Future plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'slider_future_handle_image_upload' function in all versions up to, and including, 1.0.5. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.

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: 2026-02-19

CVE-2026-1994

Descripción: The s2Member plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 260127. This is due to the plugin not properly validating a user's identity prior to updating their password. This makes it possible for unauthenticated attackers to change arbitrary user's passwords, including administrators, and leverage that to gain access to the...

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: 2026-02-19

CVE-2026-25242

Descripción: Gogs is an open source self-hosted Git service. Versions 0.13.4 and below expose unauthenticated file upload endpoints by default. When the global RequireSigninView setting is disabled (default), any remote user can upload arbitrary files to the server via /releases/attachments and /issues/attachments. This enables the instance to be abused as a public file host, potentially leading to disk exh...

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: 2026-02-19

CVE-2025-8350

Descripción: Execution After Redirect (EAR), Missing Authentication for Critical Function vulnerability in Inrove Software and Internet Services BiEticaret CMS allows Authentication Bypass, HTTP Response Splitting.This issue affects BiEticaret CMS: from 2.1.13 through 19022026.

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-306

Tecnología: No especificado

Publicado el: 2026-02-19

CVE-2025-9953

Descripción: Authorization Bypass Through User-Controlled SQL Primary Key vulnerability in DATABASE Software Training Consulting Ltd. Databank Accreditation Software allows SQL Injection.This issue affects Databank Accreditation Software: through 19022026.

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-566

Tecnología: No especificado

Publicado el: 2026-02-19

CVE-2025-71243

Descripción: The 'Saisies pour formulaire' (Saisies) plugin for SPIP versions 5.4.0 through 5.11.0 contains a critical Remote Code Execution (RCE) vulnerability. An attacker can exploit this vulnerability to execute arbitrary code on the server. Users should immediately update to version 5.11.1 or later.

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: 2026-02-19

CVE-2026-27476

Descripción: RustFly 2.0.0 contains a command injection vulnerability in its remote UI control mechanism that accepts hex-encoded instructions over UDP port 5005 without proper sanitization. Attackers can send crafted hex-encoded payloads containing system commands to execute arbitrary operations on the target system, including reverse shell establishment and command 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-78

Tecnología: No especificado

Publicado el: 2026-02-19

CVE-2026-27002

Descripción: OpenClaw is a personal AI assistant. Prior to version 2026.2.15, a configuration injection issue in the Docker tool sandbox could allow dangerous Docker options (bind mounts, host networking, unconfined profiles) to be applied, enabling container escape or host data access. OpenClaw 2026.2.15 blocks dangerous sandbox Docker settings and includes runtime enforcement when building `docker create`...

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: 2026-02-20

CVE-2026-26988

Descripción: LibreNMS is an auto-discovering PHP/MySQL/SNMP based network monitoring tool. Versions 25.12.0 and below contain an SQL Injection vulnerability in the ajax_table.php endpoint. The application fails to properly sanitize or parameterize user input when processing IPv6 address searches. Specifically, the address parameter is split into an address and a prefix, and the prefix portion is directly co...

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-89

Tecnología: No especificado

Publicado el: 2026-02-20

CVE-2025-10970

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Kolay Software Inc. Talentics allows Blind SQL Injection.This issue affects Talentics: through 20022026.

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: 2026-02-20

CVE-2026-2848

Descripción: A flaw has been found in SourceCodester Simple Responsive Tourism Website 1.0. Affected by this vulnerability is an unknown functionality of the file /classes/Master.php?f=register of the component Registration. This manipulation of the argument Username 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: 2026-02-20

CVE-2019-25441

Descripción: thesystem 1.0 contains a command injection vulnerability that allows unauthenticated attackers to execute arbitrary system commands by submitting malicious input to the run_command endpoint. Attackers can send POST requests with shell commands in the command parameter to execute arbitrary code on the server 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: 2026-02-20

Resumen del Reporte

CVEs analizados: 46

Promedio CVSS: 9.02

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat