CVEs más relevantes de la semana

Del 20/01/2026 al 27/01/2026

Porque el primer paso para defender es conocer las amenazas.

CVE-2026-21969

Descripción: Vulnerability in the Oracle Agile Product Lifecycle Management for Process product of Oracle Supply Chain (component: Supplier Portal). The supported version that is affected is 6.2.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Agile Product Lifecycle Management for Process. Successful attacks of this vulnerability can r...

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: N/A

Tecnología: No especificado

Publicado el: 2026-01-20

CVE-2025-15521

Descripción: The Academy LMS – WordPress LMS Plugin for Complete eLearning Solution plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 3.5.0. This is due to the plugin not properly validating a user's identity prior to updating their password and relying solely on a publicly-exposed nonce for authorization. This makes it possible for unauthe...

CVSS: 9.8 (CRITICAL)

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

Tipo: CWE-639

Tecnología: No especificado

Publicado el: 2026-01-21

CVE-2026-20045

Descripción: A vulnerability in Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P), Cisco Unity Connection, and Cisco Webex Calling Dedicated Instance could allow an unauthenticated, remote attacker to execute arbitrary commands on the un...

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-94

Tecnología: No especificado

Publicado el: 2026-01-21

CVE-2021-47748

Descripción: Hasura GraphQL 1.3.3 contains a remote code execution vulnerability that allows attackers to execute arbitrary shell commands through SQL query manipulation. Attackers can inject commands into the run_sql endpoint by crafting malicious GraphQL queries that execute system commands through PostgreSQL's COPY FROM PROGRAM 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-78

Tecnología: No especificado

Publicado el: 2026-01-21

CVE-2021-47851

Descripción: Mini Mouse 9.2.0 contains a remote code execution vulnerability that allows attackers to execute arbitrary commands through an unauthenticated HTTP endpoint. Attackers can leverage the /op=command endpoint to download and execute payloads by sending crafted JSON requests with malicious script commands.

CVSS: 9.8 (CRITICAL)

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

Tipo: CWE-78

Tecnología: No especificado

Publicado el: 2026-01-21

CVE-2021-47854

Descripción: DD-WRT version 45723 contains a buffer overflow vulnerability in the UPNP network discovery service that allows remote attackers to potentially execute arbitrary code. Attackers can send crafted M-SEARCH packets with oversized UUID payloads to trigger buffer overflow conditions on the target 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-120

Tecnología: No especificado

Publicado el: 2026-01-21

CVE-2021-47875

Descripción: GeoGebra CAS Calculator 6.0.631.0 contains a denial of service vulnerability that allows attackers to crash the application by generating a large buffer overflow. Attackers can create a payload with 8000 repeated characters and paste it into the calculator's input field to trigger an application crash.

CVSS: 9.8 (CRITICAL)

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

Tipo: CWE-770

Tecnología: No especificado

Publicado el: 2026-01-21

CVE-2026-0920

Descripción: The LA-Studio Element Kit for Elementor plugin for WordPress is vulnerable to Administrative User Creation in all versions up to, and including, 1.5.6.3. This is due to the 'ajax_register_handle' function not restricting what user roles a user can register with. This makes it possible for unauthenticated attackers to supply the 'lakit_bkrole' parameter during registration and gain 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: 2026-01-22

CVE-2026-1331

Descripción: MeetingHub developed by HAMASTAR Technology has an Arbitrary File Upload vulnerability, allowing unauthenticated remote attackers to upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.

CVSS: 9.8 (CRITICAL)

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

Tipo: CWE-434

Tecnología: No especificado

Publicado el: 2026-01-22

CVE-2026-23760

Descripción: SmarterTools SmarterMail versions prior to build 9511 contain an authentication bypass vulnerability in the password reset API. The force-reset-password endpoint permits anonymous requests and fails to verify the existing password or a reset token when resetting system administrator accounts. An unauthenticated attacker can supply a target administrator username and a new password to reset 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-288

Tecnología: No especificado

Publicado el: 2026-01-22

CVE-2026-21264

Descripción: Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Account allows an unauthorized attacker to perform spoofing over a network.

CVSS: 9.3 (CRITICAL)

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

Tipo: CWE-79

Tecnología: No especificado

Publicado el: 2026-01-22

CVE-2026-24305

Descripción: Azure Entra ID Elevation of Privilege Vulnerability

CVSS: 9.3 (CRITICAL)

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

Tipo: CWE-285

Tecnología: No especificado

Publicado el: 2026-01-22

CVE-2026-24306

Descripción: Improper access control in Azure Front Door (AFD) allows an unauthorized attacker to elevate privileges 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-284

Tecnología: No especificado

Publicado el: 2026-01-22

CVE-2026-24307

Descripción: Improper validation of specified type of input in M365 Copilot allows an unauthorized attacker to disclose information over a network.

CVSS: 9.3 (CRITICAL)

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

Tipo: CWE-1287

Tecnología: No especificado

Publicado el: 2026-01-22

CVE-2026-24304

Descripción: Improper access control in Azure Resource Manager allows an authorized attacker to elevate privileges over a network.

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-284

Tecnología: No especificado

Publicado el: 2026-01-23

CVE-2026-1363

Descripción: IAQS and I6 developed by JNC has a Client-Side Enforcement of Server-Side Security vulnerability, allowing unauthenticated remote attackers to gain administrator privileges by manipulating the web front-end.

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-603

Tecnología: No especificado

Publicado el: 2026-01-23

CVE-2026-1364

Descripción: IAQS and I6 developed by JNC has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to directly operate system administrative functionalities.

CVSS: 9.8 (CRITICAL)

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

Tipo: CWE-306

Tecnología: No especificado

Publicado el: 2026-01-23

CVE-2025-4319

Descripción: Improper Restriction of Excessive Authentication Attempts, Weak Password Recovery Mechanism for Forgotten Password vulnerability in Birebirsoft Software and Technology Solutions Sufirmam allows Brute Force, Password Recovery Exploitation.This issue affects Sufirmam: through 23012026. 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:H/I:L/A:H

Tipo: CWE-307

Tecnología: No especificado

Publicado el: 2026-01-23

CVE-2025-4320

Descripción: Authentication Bypass by Primary Weakness, Weak Password Recovery Mechanism for Forgotten Password vulnerability in Birebirsoft Software and Technology Solutions Sufirmam allows Authentication Bypass, Password Recovery Exploitation.This issue affects Sufirmam: through 23012026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.

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-305

Tecnología: No especificado

Publicado el: 2026-01-23

CVE-2021-47891

Descripción: Unified Remote 3.9.0.2463 contains a remote code execution vulnerability that allows attackers to send crafted network packets to execute arbitrary commands. Attackers can exploit the service by connecting to port 9512 and sending specially crafted packets to open a command prompt and download and execute malicious payloads.

CVSS: 9.8 (CRITICAL)

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

Tipo: CWE-306

Tecnología: No especificado

Publicado el: 2026-01-23

CVE-2025-13374

Descripción: The Kalrav AI Agent plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the kalrav_upload_file AJAX action in all versions up to, and including, 2.3.3. 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: 2026-01-24

CVE-2020-36940

Descripción: Easy CD & DVD Cover Creator 4.13 contains a buffer overflow vulnerability in the serial number input field that allows attackers to crash the application. Attackers can generate a 6000-byte payload and paste it into the serial number field to trigger an application crash.

CVSS: 9.8 (CRITICAL)

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

Tipo: CWE-120

Tecnología: No especificado

Publicado el: 2026-01-27

CVE-2020-36941

Descripción: Knockpy 4.1.1 contains a CSV injection vulnerability that allows attackers to inject malicious formulas into CSV reports through unfiltered server headers. Attackers can manipulate server response headers to include spreadsheet formulas that will execute when the CSV is opened in spreadsheet applications.

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-1236

Tecnología: No especificado

Publicado el: 2026-01-27

CVE-2020-36948

Descripción: VestaCP 0.9.8-26 contains a session token vulnerability in the LoginAs module that allows remote attackers to manipulate authentication tokens. Attackers can exploit insufficient token validation to access user accounts and perform unauthorized login requests without proper administrative 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-863

Tecnología: No especificado

Publicado el: 2026-01-27

CVE-2021-47900

Descripción: Gila CMS versions prior to 2.0.0 contain a remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary system commands through manipulated HTTP headers. Attackers can inject PHP code in the User-Agent header with shell_exec() to run system commands by sending crafted requests to the admin endpoint.

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: 2026-01-27

CVE-2021-47901

Descripción: Dirsearch 0.4.1 contains a CSV injection vulnerability when using the --csv-report flag that allows attackers to inject formulas through redirected endpoints. Attackers can craft malicious server redirects with comma-separated paths containing Excel formulas to manipulate the generated CSV report.

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-1236

Tecnología: No especificado

Publicado el: 2026-01-27

Resumen del Reporte

CVEs analizados: 26

Promedio CVSS: 9.68

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat