CVEs más relevantes de la semana

Del 27/01/2026 al 03/02/2026

Porque el primer paso para defender es conocer las amenazas.

CVE-2026-22262

Descripción: Suricata is a network IDS, IPS and NSM engine. While saving a dataset a stack buffer is used to prepare the data. Prior to versions 8.0.3 and 7.0.14, if the data in the dataset is too large, this can result in a stack overflow. Versions 8.0.3 and 7.0.14 contain a patch. As a workaround, do not use rules with datasets `save` nor `state` options.

CVSS: 5.9 (MEDIUM)

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

Tipo: CWE-121

Tecnología: No especificado

Publicado el: 2026-01-27

CVE-2026-22264

Descripción: Suricata is a network IDS, IPS and NSM engine. Prior to version 8.0.3 and 7.0.14, an unsigned integer overflow can lead to a heap use-after-free condition when generating excessive amounts of alerts for a single packet. Versions 8.0.3 and 7.0.14 contain a patch. As a workaround, do not run untrusted rulesets or run with less than 65536 signatures that can match on the same packet.

CVSS: 7.4 (HIGH)

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

Tipo: CWE-416

Tecnología: No especificado

Publicado el: 2026-01-27

CVE-2025-21589

Descripción: An Authentication Bypass Using an Alternate Path or Channel vulnerability in Juniper Networks Session Smart Router may allows a network-based attacker to bypass authentication and take administrative control of the device.

This issue affects Session Smart Router:

* from 5.6.7 before 5.6.17,   * from 6.0 before 6.0.8
(affected from 6.0.8),

* from 6.1 before 6.1.12-lts,   * from 6...

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: 2026-01-27

CVE-2025-40551

Descripción: SolarWinds Web Help Desk was found to be susceptible to an untrusted data deserialization vulnerability that could lead to remote code execution, which would allow an attacker to run commands on the host machine. This could be exploited 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-502

Tecnología: No especificado

Publicado el: 2026-01-28

CVE-2025-40552

Descripción: SolarWinds Web Help Desk was found to be susceptible to an authentication bypass vulnerability that if exploited, would allow a malicious actor to execute actions and methods that should be protected by 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-1390

Tecnología: No especificado

Publicado el: 2026-01-28

CVE-2025-40553

Descripción: SolarWinds Web Help Desk was found to be susceptible to an untrusted data deserialization vulnerability that could lead to remote code execution, which would allow an attacker to run commands on the host machine. This could be exploited 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-502

Tecnología: No especificado

Publicado el: 2026-01-28

CVE-2025-40554

Descripción: SolarWinds Web Help Desk was found to be susceptible to an authentication bypass vulnerability that, if exploited, could allow an attacker to invoke specific actions within Web Help Desk.

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-1390

Tecnología: No especificado

Publicado el: 2026-01-28

CVE-2026-1056

Descripción: The Snow Monkey Forms plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the 'generate_user_dirpath' function in all versions up to, and including, 12.0.3. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-co...

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-22

Tecnología: No especificado

Publicado el: 2026-01-28

CVE-2020-36961

Descripción: 10-Strike Network Inventory Explorer 8.65 contains a buffer overflow vulnerability in exception handling that allows remote attackers to execute arbitrary code. Attackers can craft a malicious file with 209 bytes of padding and a specially constructed Structured Exception Handler to trigger 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: 2026-01-28

CVE-2025-68662

Descripción: Discourse is an open source discussion platform. In versions prior to 3.5.4, 2025.11.2, 2025.12.1, and 2026.1.0, a hostname validation issue in FinalDestination could allow bypassing SSRF protections under certain conditions. This issue is patched in versions 3.5.4, 2025.11.2, 2025.12.1, and 2026.1.0. No known workarounds are available.

CVSS: 7.6 (HIGH)

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

Tipo: CWE-918

Tecnología: No especificado

Publicado el: 2026-01-28

CVE-2026-1534

Descripción: A weakness has been identified in code-projects Online Music Site 1.0. This affects an unknown function of the file /Administrator/PHP/AdminEditUser.php. This manipulation of the argument ID causes sql injection. It is possible to initiate the attack 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-74

Tecnología: No especificado

Publicado el: 2026-01-28

CVE-2026-1535

Descripción: A security vulnerability has been detected in code-projects Online Music Site 1.0. This impacts an unknown function of the file /Administrator/PHP/AdminReply.php. Such manipulation of the argument ID leads to sql injection. It is possible to launch 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: 2026-01-28

CVE-2026-1545

Descripción: A weakness has been identified in itsourcecode School Management System 1.0. The affected element is an unknown function of the file /course/index.php. Executing a manipulation of the argument ID can lead to sql injection. The attack may be performed from remote. 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-74

Tecnología: No especificado

Publicado el: 2026-01-28

CVE-2020-36997

Descripción: BacklinkSpeed 2.4 contains a buffer overflow vulnerability that allows attackers to corrupt the Structured Exception Handler (SEH) chain through malicious file import. Attackers can craft a specially designed payload file to overwrite SEH addresses, potentially executing arbitrary code and gaining control of 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-121

Tecnología: No especificado

Publicado el: 2026-01-29

CVE-2020-37000

Descripción: Free MP3 CD Ripper 2.8 contains a stack buffer overflow vulnerability that allows remote attackers to execute arbitrary code by crafting a malicious WAV file with oversized payload. Attackers can leverage a specially crafted exploit file with shellcode, SEH bypass, and egghunter technique to achieve remote code execution on vulnerable Windows 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: 2026-01-29

CVE-2020-37002

Descripción: Ajenti 2.1.36 contains an authentication bypass vulnerability that allows remote attackers to execute arbitrary commands after successful login. Attackers can leverage the /api/terminal/create endpoint to send a netcat reverse shell payload targeting a specified IP and port.

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: 2026-01-29

CVE-2026-1589

Descripción: A vulnerability was determined in itsourcecode School Management System 1.0. This affects an unknown function of the file /ramonsys/inquiry/index.php. This manipulation of the argument txtsearch causes sql injection. The attack can be initiated 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: 2026-01-29

CVE-2026-1590

Descripción: A vulnerability was identified in itsourcecode School Management System 1.0. This impacts an unknown function of the file /ramonsys/faculty/index.php. Such manipulation of the argument ID leads to sql injection. The attack can be launched 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: 2026-01-29

CVE-2026-1593

Descripción: A weakness has been identified in itsourcecode Society Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/edit_expenses_query.php. Executing a manipulation of the argument detail can lead to sql injection. The attack may be launched 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-74

Tecnología: No especificado

Publicado el: 2026-01-29

CVE-2026-1594

Descripción: A security vulnerability has been detected in itsourcecode Society Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/add_expenses.php. The manipulation of the argument detail leads to sql injection. Remote exploitation of the attack is possible. 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: 2026-01-29

CVE-2026-1595

Descripción: A vulnerability was detected in itsourcecode Society Management System 1.0. This affects an unknown part of the file /admin/edit_student_query.php. The manipulation of the argument student_id results in sql injection. The attack can be executed remotely. 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: 2026-01-29

CVE-2019-25232

Descripción: NetPCLinker 1.0.0.0 contains a buffer overflow vulnerability in the Clients Control Panel DNS/IP field that allows attackers to execute arbitrary shellcode. Attackers can craft a malicious payload in the DNS/IP input to overwrite SEH handlers and execute shellcode when adding a new client.

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: 2026-01-30

CVE-2020-37027

Descripción: Sickbeard alpha contains a remote command injection vulnerability that allows unauthenticated attackers to execute arbitrary commands through the extra scripts configuration. Attackers can set malicious commands in the extra scripts field and trigger processing to execute remote code on the vulnerable Sickbeard installation.

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: 2026-01-30

CVE-2020-37043

Descripción: 10-Strike Bandwidth Monitor 3.9 contains a buffer overflow vulnerability that allows attackers to bypass SafeSEH, ASLR, and DEP protections through carefully crafted input. Attackers can exploit the vulnerability by sending a malicious payload to the application's registration key input, enabling remote code execution and launching arbitrary system 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-120

Tecnología: No especificado

Publicado el: 2026-01-30

CVE-2020-37050

Descripción: Quick Player 1.3 contains a buffer overflow vulnerability that allows attackers to execute arbitrary code by crafting a malicious .m3l file with carefully constructed payload. Attackers can trigger the vulnerability by loading a specially crafted file through the application's file loading mechanism, potentially 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: 2026-01-30

CVE-2020-37052

Descripción: AirControl 1.4.2 contains a pre-authentication remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary system commands through malicious Java expression injection. Attackers can exploit the /.seam endpoint by crafting a specially constructed URL with embedded Java expressions to run commands with the application's system 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-94

Tecnología: No especificado

Publicado el: 2026-01-30

CVE-2020-37056

Descripción: Crystal Shard http-protection 0.2.0 contains an IP spoofing vulnerability that allows attackers to bypass protection middleware by manipulating request headers. Attackers can hardcode consistent IP values across X-Forwarded-For, X-Client-IP, and X-Real-IP headers to circumvent security checks and gain unauthorized 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-290

Tecnología: No especificado

Publicado el: 2026-01-30

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-2025-5319

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Emit Information and Communication Technologies Industry and Trade Ltd. Co. Efficiency Management System allows SQL Injection.This issue affects Efficiency Management System: through 03022026.

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: 2026-02-03

Resumen del Reporte

CVEs analizados: 29

Promedio CVSS: 8.82

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat ▯