



Decompression Bomb in cow_spdy:inflate/2 Allows Memory Exhaustion via Crafted SPDY Frame

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-43970
State	PUBLISHED
Assigner	EEF
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-13 19:17:25 UTC
Updated	2026-05-14 17:07:07 UTC
Description	Improper Handling of Highly Compressed Data (Data Amplification) vulnerability in ninenines cowlib allows unauthenticated

Risk And Classification

Primary CVSS: v4.0 8.2 HIGH from 6b3ad84c-e1a6-4bf7-a703-f496b71e49db

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.001390000 probability, percentile 0.336040000 (date 2026-05-15)

Problem Types: CWE-409 | CWE-409 CWE-409 Improper Handling of Highly Compressed Data (Data Amplification)

Version	Source	Type	Score	Severity	Vector
4.0	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	Secondary	8.2	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	CVSS	8.2	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality	None
Integrity	None
Availability	High
Sub Conf.	None
Sub Integrity	None
Sub Availability	None

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Ninenines	Cowlib	affected 0.1.0 2.16.1 semver
CNA	Ninenines	Cowlib	affected fad5c0049df278cc498b6cdb519b09e845a070a8 16aad3fb9f81f5cda4d1706ff0c54237c619c282 git

References

Reference	Source	Link
github.com/ninenines/cowlib/commit/16aad3fb9f81f5cda4d1706ff0c54237c619c282	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
cna.erlef.org/cves/CVE-2026-43970.html	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	cna.erlef.org
osv.dev/vulnerability/EEF-CVE-2026-43970	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	osv.dev
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Peter Ullrich (en)

CNA: Loïc Hoguein (en)

Additional Advisory Data

Solutions

CNA: Upgrade to cowlib 2.16.1 or later, in which the cow_spdy module has been removed entirely. No patched version of cow_spdy will be provided. Migrate away from SPDY, which

has been deprecated since 2015 in favour of HTTP/2.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)