



# Cookie Request Header Injection via Unvalidated Encoder in cow\_cookie:cookie/1

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

## Summary

<b>CVE</b>	CVE-2026-43969
<b>State</b>	PUBLISHED
<b>Assigner</b>	EEF
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-11 19:16:25 UTC
<b>Updated</b>	2026-05-11 19:16:25 UTC
<b>Description</b>	Improper Neutralization of CRLF Sequences ('CRLF Injection') vulnerability in ninenines cowlib allows HTTP request splittin

## Risk And Classification

**Primary CVSS:** v4.0 2.1 LOW from 6b3ad84c-e1a6-4bf7-a703-f496b71e49db

CVSS:4.0/AV:L/AC:L/AT:P/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:L/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

**Problem Types:** CWE-93 | CWE-93 CWE-93 Improper Neutralization of CRLF Sequences ('CRLF Injection')

Version	Source	Type	Score	Severity	Vector
4.0	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	Secondary	2.1	LOW	CVSS:4.0/AV:L/AC:L/AT:P/PR:N/UI:N/VC:N/VI:L/VA:N
4.0	CNA	CVSS	2.1	LOW	CVSS:4.0/AV:L/AC:L/AT:P/PR:N/UI:N/VC:N/VI:L/VA:N

## CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

None

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:P/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:L/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	Platforms
CNA	Ninenines	Cowlib	affected 2.9.0 semver	Not specified
CNA	Ninenines	Cowlib	affected f017f8a0ecbfd5033d9ab49bf180186f7a523a7 git	Not specified

### References

Reference	Source	Link
cna.erlef.org/cves/CVE-2026-43969.html	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	<a href="https://cna.erlef.org/cves/CVE-2026-43969.html">cna.erlef.org</a>
github.com/erlef/cowlib/commit/177953dd51540da11090666c1f007214127a1144	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	<a href="https://github.com/erlef/cowlib/commit/177953dd51540da11090666c1f007214127a1144">github.com</a>
osv.dev/vulnerability/EEF-CVE-2026-43969	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	<a href="https://osv.dev/vulnerability/EEF-CVE-2026-43969">osv.dev</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

### Vendor Comments And Credit

Discovery Credit

**CNA:** Peter Ullrich (en)

### Additional Advisory Data

Workarounds

**CNA:** Validate inputs into cow\_cookie:cookie/1 to only include valid cookie name and value characters as defined in RFC 6265 Section 4.1.1 before passing them to the function.

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](#)