



# oma-topic: name Field in Topic Manifests (topic.json) May Allow CRLF Injection

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

## Summary

<b>CVE</b>	CVE-2026-39958
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-09 17:16:30 UTC
<b>Updated</b>	2026-04-09 17:16:30 UTC
<b>Description</b>	oma is a package manager for AOSC OS. Prior to 1.25.2, oma-topics is responsible for fetching metadata for testing reposi

## Risk And Classification

**Primary CVSS:** v4.0 5.2 MEDIUM from security-advisories@github.com

CVSS:4.0/AV:N/AC:H/AT:P/PR:H/UI:P/VC:N/VI:N/VA:N/SC:H/SI:H/SA:H/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	security-advisories@github.com	Secondary	5.2	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:P/PR:H/UI:P/VC:N/VI:N/VA:N/SC:H/
4.0	CNA	DECLARED	5.2	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:P/PR:H/UI:P/VC:N/VI:N/VA:N/SC:H/

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

Present

Privileges Required

High

User Interaction

Passive

Confidentiality

None

Integrity

None

Availability

None

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:N/AC:H/AT:P/PR:H/UI:P/VC:N/VI:N/VA:N/SC:H/SI:H/SA:H/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	AOSC-Dev	Oma	affected < 1.25.1	Not specified

### References

Reference	Source	Link	Tags
github.com/AOSC-Dev/oma/security/advisories/GHSA-86jc-7r6q-cr3f	security-advisories@github.com	github.com	
github.com/AOSC-Dev/oma/pull/733	security-advisories@github.com	github.com	
github.com/AOSC-Dev/oma/releases/tag/v1.25.2	security-advisories@github.com	github.com	
github.com/AOSC-Dev/oma/commit/b361c0f219bbf91a684610c76210f71f093dbc18	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

No vendor comments have been submitted for this CVE.

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](https://cve.report/api)

