



# Axios has Unrestricted Cloud Metadata Exfiltration via Header Injection Chain

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

## Summary

<b>CVE</b>	CVE-2026-40175
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-10 20:16:22 UTC
<b>Updated</b>	2026-04-16 19:16:34 UTC
<b>Description</b>	Axios is a promise based HTTP client for the browser and Node.js. Prior to 1.15.0 and 0.3.1, the Axios library is vulnerable

## Risk And Classification

**Primary CVSS:** v3.1 4.8 MEDIUM from security-advisories@github.com

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

**EPSS:** 0.005300000 probability, percentile 0.672790000 (date 2026-04-16)

**Problem Types:** CWE-113 | CWE-444 | CWE-918 | CWE-113 CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting') | CWE-444 CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') | CWE-918 CWE-918: Server-Side Request Forgery (SSRF)

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	4.8	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N
3.1	CNA	DECLARED	4.8	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

None

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Axios</a>	<a href="#">Axios</a>	affected >= 1.0.0, < 1.15.0	Not specified
CNA	<a href="#">Axios</a>	<a href="#">Axios</a>	affected < 0.31.0	Not specified

### References

Reference	Source	Link
<a href="https://github.com/axios/axios/commit/363185461b90b1b78845dc8a99a1f103d9b122a1">github.com/axios/axios/commit/363185461b90b1b78845dc8a99a1f103d9b122a1</a>	security-advisories@github.com	<a href="#">github.com</a>
<a href="https://github.com/axios/axios/releases/tag/v1.15.0">github.com/axios/axios/releases/tag/v1.15.0</a>	security-advisories@github.com	<a href="#">github.com</a>
<a href="https://github.com/axios/axios/pull/10660">github.com/axios/axios/pull/10660</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="#">github.com</a>
<a href="https://github.com/axios/axios/security/advisories/GHSA-fvcv-3m26-pcqx">github.com/axios/axios/security/advisories/GHSA-fvcv-3m26-pcqx</a>	security-advisories@github.com	<a href="#">github.com</a>
<a href="https://github.com/axios/axios/commit/03cdfc99e8db32a390e12128208b6778492cee9c">github.com/axios/axios/commit/03cdfc99e8db32a390e12128208b6778492cee9c</a>	security-advisories@github.com	<a href="#">github.com</a>
<a href="https://github.com/axios/axios/releases/tag/v0.31.0">github.com/axios/axios/releases/tag/v0.31.0</a>	security-advisories@github.com	<a href="#">github.com</a>
<a href="https://github.com/axios/axios/pull/10660">github.com/axios/axios/pull/10660</a>	security-advisories@github.com	<a href="#">github.com</a>
<a href="https://github.com/axios/axios/pull/10688">github.com/axios/axios/pull/10688</a>	security-advisories@github.com	<a href="#">github.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

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)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)