Axios has a NO_PROXY Hostname Normalization Bypass Leads to SSRF

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-62718
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-09 15:16:08 UTC
Updated	2026-04-09 17:16:24 UTC
Description	Axios is a promise based HTTP client for the browser and Node.js. Prior to 1.15.0, Axios does not correctly handle hostnam

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from security-advisories@github.com

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

Problem Types: CWE-441 | CWE-918 | CWE-441 CWE-441: Unintended Proxy or Intermediary ('Confused Deputy') | CWE-918 CWE-918: Server-Side Request Forgery (SSRF)

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:L/SC:H/
4.0	CNA	DECLARED	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:L/SC:H/

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

Low

Availability

Low

Sub Conf.

High

Sub Integrity

Low

Sub Availability

Low

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:L/SC:H/SI:L/SA:L/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/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	Axios	Axios	affected < 1.15.0	Not specified

References

Reference	Source	Link
datatracker.ietf.org/doc/html/rfc3986	security-advisories@github.com	datatracker.ietf.c
github.com/axios/axios/releases/tag/v1.15.0	security-advisories@github.com	github.com
github.com/axios/axios/pull/10661	security-advisories@github.com	github.com
datatracker.ietf.org/doc/html/rfc1034	security-advisories@github.com	datatracker.ietf.c
github.com/axios/axios/commit/fb3befb6daac6cad26b2e54094d0f2d9e47f24df	security-advisories@github.com	github.com
github.com/axios/axios/security/advisories/GHSA-3p68-rc4w-qgx5	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**