Istio HTTP debug endpoints on port 15014 to enforce namespace-based authorization, preventing cross-namespace proxy data access.

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

Summary

CVE	CVE-2026-31838
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-10 22:16:21 UTC
Updated	2026-04-07 03:16:07 UTC
Description	Istio is an open platform to connect, manage, and secure microservices. Prior to 1.29.1, 1.28.5, and 1.27.8, a vulnerability i

Risk And Classification

Primary CVSS: v4.0 6.9 MEDIUM from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-863 | CWE-863 CWE-863: Incorrect Authorization

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/S
4.0	CNA	DECLARED	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/S
3.1	nvd@nist.gov	Primary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

None

Confidentiality

Low

Integrity

None

Availability

None

Sub Conf.

Low

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Istio	Istio	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Istio	Istio	affected >= 1.29.0-alpha.0, < 1.29.1	Not specified

CNA	Istio	Istio	affected >= 1.28.0-alpha.0, < 1.28.5	Not specified
CNA	Istio	Istio	affected < 1.27.8	Not specified

References

Reference	Source	Link	Tags
github.com/istio/istio/commit/004fd6921314a8e2293fd195d91645dcbbff0aa1	security-advisories@github.com	github.com	
github.com/istio/istio/security/advisories/GHSA-974c-2wxh-g4ww	security-advisories@github.com	github.com	Vendor Advi
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

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