Missing Delegated Metadata Validation in awslabs/tough

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

Summary

CVE	CVE-2026-6967
State	PUBLISHED
Assigner	AMZN
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-24 20:16:29 UTC
Updated	2026-04-24 21:16:19 UTC
Description	Missing expiration, hash, and length enforcement in delegated metadata validation in awslabs/tough before tough-v0.22.0 a

Risk And Classification

Primary CVSS: v4.0 7.1 HIGH from ff89ba41-3aa1-4d27-914a-91399e9639e5

CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:N/VI:H/VA:N/SC:N/SI:H/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-345 | CWE-345 CWE-345: Insufficient Verification of Data Authenticity

Version	Source	Type	Score	Severity	Vector
4.0	ff89ba41-3aa1-4d27-914a-91399e9639e5	Secondary	7.1	HIGH	CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:N/VI:H/VA:
4.0	CNA	CVSS	7.1	HIGH	CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:N/VI:H/VA:
3.1	ff89ba41-3aa1-4d27-914a-91399e9639e5	Secondary	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:L
3.1	CNA	CVSS	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:L

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

Present

Privileges Required

Low

User Interaction

None

None

Confidentiality

None

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

High

Sub Availability

Low

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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	AWS	Tough	unaffected 0.22.0	Not specified
CNA	AWS	Tuftool	unaffected 0.15.0	Not specified

References

Reference	Source	Link	Tags

github.com/awslabs/tough/security/advisories/GHSA-4v58-8p28-2rq3	ff89ba41-3aa1-4d27-914a-91399e9639e5	github.com	
aws.amazon.com/security/security-bulletins/2026-019-aws	ff89ba41-3aa1-4d27-914a-91399e9639e5	aws.amazon.com	
github.com/awslabs/tough/releases/tag/tough-v0.22.0	ff89ba41-3aa1-4d27-914a-91399e9639e5	github.com	
crates.io/crates/tough/0.22.0	ff89ba41-3aa1-4d27-914a-91399e9639e5	crates.io	
crates.io/crates/tuftool/0.15.0	ff89ba41-3aa1-4d27-914a-91399e9639e5	crates.io	
github.com/awslabs/tough/releases/tag/tuftool-v0.15.0	ff89ba41-3aa1-4d27-914a-91399e9639e5	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.