



Signature Threshold Bypass in awslabs/tough Delegated Roles

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

Summary

CVE	CVE-2026-6966
State	PUBLISHED
Assigner	AMZN
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-24 20:16:28 UTC
Updated	2026-04-24 21:16:19 UTC
Description	Improper verification of cryptographic signature uniqueness in delegated role validation in awslabs/tough before tough-v0.2

Risk And Classification

Primary CVSS: v4.0 7 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: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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-347 | CWE-347 CWE-347: Improper Verification of Cryptographic Signature

Version	Source	Type	Score	Severity	Vector
4.0	ff89ba41-3aa1-4d27-914a-91399e9639e5	Secondary	7	HIGH	CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:N/VI:H/VA:
4.0	CNA	CVSS	7	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	5.3	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:N
3.1	CNA	CVSS	5.3	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

Present

Privileges Required

Low

User Interaction

None

Confidentiality

None

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

High

Sub Availability

None

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

None

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

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	Tag
github.com/aws-labs/tough/security/advisories/GHSA-8m7c-8m39-rv4x	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/aws-labs/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/aws-labs/tough/releases/tag/tuftool-v0.15.0	ff89ba41-3aa1-4d27-914a-91399e9639e5	github.com	
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

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