



# Multiple Path Traversal Variants in awslabs/tough

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

## Summary

<b>CVE</b>	CVE-2026-6968
<b>State</b>	PUBLISHED
<b>Assigner</b>	AMZN
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-24 20:16:29 UTC
<b>Updated</b>	2026-04-24 21:16:20 UTC
<b>Description</b>	Incomplete path traversal fixes in awslabs/tough before tough-v0.22.0 allow remote authenticated users with delegated sig

## 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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**Problem Types:** CWE-22 | CWE-22 CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

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

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/MS:C: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
-----------	--------	------	------

<a href="https://aws.amazon.com/security/security-bulletins/2026-019-aws">aws.amazon.com/security/security-bulletins/2026-019-aws</a>	ff89ba41-3aa1-4d27-914a-91399e9639e5	<a href="https://aws.amazon.com">aws.amazon.com</a>	
<a href="https://github.com/awslabs/tough/security/advisories/GHSA-v57p-gppj-p9vg">github.com/awslabs/tough/security/advisories/GHSA-v57p-gppj-p9vg</a>	ff89ba41-3aa1-4d27-914a-91399e9639e5	<a href="https://github.com">github.com</a>	
<a href="https://github.com/awslabs/tough/releases/tag/tough-v0.22.0">github.com/awslabs/tough/releases/tag/tough-v0.22.0</a>	ff89ba41-3aa1-4d27-914a-91399e9639e5	<a href="https://github.com">github.com</a>	
<a href="https://crates.io/crates/tough/0.22.0">crates.io/crates/tough/0.22.0</a>	ff89ba41-3aa1-4d27-914a-91399e9639e5	<a href="https://crates.io">crates.io</a>	
<a href="https://crates.io/crates/tuftool/0.15.0">crates.io/crates/tuftool/0.15.0</a>	ff89ba41-3aa1-4d27-914a-91399e9639e5	<a href="https://crates.io">crates.io</a>	
<a href="https://github.com/awslabs/tough/releases/tag/tuftool-v0.15.0">github.com/awslabs/tough/releases/tag/tuftool-v0.15.0</a>	ff89ba41-3aa1-4d27-914a-91399e9639e5	<a href="https://github.com">github.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canor
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canor

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](https://cve.report/api)

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