Multiple Path Traversal Variants in awslabs/tough

Moderate **rpkelly** published **GHSA-v57p-gppj-p9vg** 43 minutes ago

Package

tough

Affected versions	Patched versions
0.9.0	0.22.0

tuftool

<0.15.0	0.15.0

Description

Summary

Incomplete path traversal fixes in awslabs/tough before tough-v0.22.0 allow remote authenticated users with delegated signing authority to write files outside intended output directories via absolute target names in copy_target/link_target, symlinked parent directories in save_target, or symlinked metadata filenames in SignedRole::write, because write paths trust the joined destination path without post-resolution containment verification.

Impact

The tough library, prior to 0.22.0, does not properly validate the output directory of files it writes to disk. This could allow for a remote repository to be configured in such a way as to enable a call to output files in unexpected locations on the callers filesystem.

Impacted versions: tough 0.9.0 through 0.21.x, tuftool through 0.14.x

Patches

This issue has been addressed in tough version 0.22.0 and tuftool version 0.15.0. We recommend upgrading to the latest version and ensuring any forked or derivative code is patched to incorporate the new fixes.

Workarounds

No workarounds to this issue are known.

References

CVE-2026-6968

If you have any questions or comments about this advisory, we ask that you contact [AWS/Amazon] Security via our vulnerability reporting page or directly via email to aws-security@amazon.com. Please do not create a public GitHub issue.

Acknowledgement

We would like to thank Oleh Konko of 1seal for collaborating on this issue through the coordinated vulnerability disclosure process.

Severity

Moderate 5.9 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	High
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	High
Availability	Low

Learn more about base metrics

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

CVE ID

CVE-2026-6968

Weaknesses

No CWEs