Missing Delegated Metadata Validation in awslabs/tough

Moderate **rpkelly** published **GHSA-4v58-8p28-2rq3** 43 minutes ago

Package

tough

Affected versions	Patched versions
0.9.0	0.22.0

tuftool

< 0.15.0	0.15.0

Description

Summary

Missing expiration, hash, and length enforcement in delegated metadata validation in awslabs/tough before tough-v0.22.0 allows remote authenticated users with delegated signing authority to bypass TUF specification integrity checks for delegated targets metadata and poison the local metadata cache, because load_delegations does not apply the same validation checks as the top-level targets metadata path.

Impact

The tough library, prior to 0.22.0, does not properly verify delegated target metadata. It allows someone with write access to the metadata to serve expired or otherwise invalid targets from a TUF repository which tough will then trust rather than reject.

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-2026-6967
  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-2026-6967

Weaknesses

No CWEs