Signature Threshold Bypass in awslabs/tough Delegated Roles

Moderate **rpkelly** published **GHSA-8m7c-8m39-rv4x** 42 minutes ago

Package

tough

Affected versions	Patched versions
< 0.22.0	0.22.0

tuftool

tuftool	0.15.0

Description

Summary

Improper verification of cryptographic signature uniqueness in delegated role validation in awslabs/tough before tough-v0.22.0 allows remote authenticated users to bypass the TUF signature threshold requirement by duplicating a valid signature, causing the client to accept forged delegated role metadata.

Impact

The tough library, prior to 0.22.0, does not properly verify the uniqueness of keys in the signatures provided to meet the threshold of cryptographic signatures in delegated targets. It allows actors with access to a valid signing key to create multiple valid signatures in order to circumvent TUF requiring a minimum threshold of unique keys before the metadata is considered valid.

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-2026-6966

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 Emily Albini of Oxide Computer and Oleh Konko of 1seal for collaborating on this issue through the coordinated vulnerability disclosure process

Severity

Moderate 5.3 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-6966

Weaknesses

No CWEs