Issues in tough library and tuftool CLI utility

Bulletin ID: 2026-019-AWS
Scope: AWS
Content Type: Important (requires attention)
Publication Date: 04/24/2026 12:45 PM PDT

Description:

Multiple security issues have been identified in the tough library and tuftool CLI utility. tough is a Rust library used for generating, signing, and managing TUF (The Update Framework) repositories, and tuftool is the command-line interface for repository management Operations.

The following issues have been identified:

- CVE-2026-6966
- CVE-2026-6967
- CVE-2026-6968

Impacted versions:

- tough: versions 0.1.0 through 0.21.x (inclusive)
- tuftool: versions 0.1.0 through 0.14.x (inclusive)

Resolution:

These issues have been addressed in the following versions:

- tough 0.22.0 or later
- tuftool 0.15.0 or later

We recommend upgrading immed
review and update any forked or c

Workarounds:

There are no known workarounds

References:

- CVE-2026-6966
- CVE-2026-6967
- CVE-2026-6968

- GHSA-8m7c-8m39-rv4x
- GHSA-4v58-8p28-2rq3
- GHSA-v57p-gppj-p9vg
- Tough GitHub Repository

Acknowledgment:

We would like to thank Emily Albini of Oxide Computer Company and Oleh Konko of 1seal.org for for collaborating on this issue through the coordinated disclosure process.

Please email aws-security@amazon.com with any security questions or concerns.