v1: Fix EVP_DigestSignFinal call for HMAC #198

Merged **karianna** merged 2 commits into `golang-fips:master` from `ueno:wip/v1-hmac-fixes` on Oct 1, 2024

Conversation 0 Commits 2 Checks 0 Files changed 3

ueno commented on Sep 27, 2024 — Collaborator

EVP_DigestSignFinal requires the length argument to be initialized if the output is non-NULL. This changes the _goboringcrypto_HMAC_Final to take the output length as an input argument, and pass it along to EVP_DigestSignFinal.

ueno requested a review from **dbenoit17** 2 years ago

ueno added 2 commits 2 years ago

`v1: Fix EVP_DigestSignFinal call for HMAC` ··· `9ea95e1`

`hmac: Check return value of C functions` ··· `aca7f01`

ueno force-pushed the `wip/v1-hmac-fixes` branch from **`e1d71c3`** to **`aca7f01`** 2 years ago Compare

qmuntal approved these changes on Sep 30, 2024

View reviewed changes

dbenoit17 approved these changes on Sep 30, 2024

View reviewed changes

karianna approved these changes on Oct 1, 2024

View reviewed changes

karianna merged commit `8c1c6aa` into `golang-fips:master` on Oct 1, 2024

---

qmuntal mentioned this pull request on Oct 28, 2024

GHSA-3h3x-2hwv-hr52: remove v2 version from affected versions list github/advisory-database#4950

Merged

Reviewers

- **karianna** ✓
- **qmuntal** ✓
- **dbenoit17** ✓

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

4 participants