Fix DecodeAltNames length check #10024

Merged **dgarske** merged 2 commits into `wolfSSL:master` from `embhorn:zd21390` 3 weeks ago

Conversation Commits 2 Checks Files changed

embhorn commented 3 weeks ago Member

Description

In `DecodeAltNames()`, the non-template ASN path (`--enable-asn=original`) needs a bounds check before `length -= strLen`.

Fixes zd21390

Testing

Added `test_DecodeAltNames_length_underflow`

Checklist

- [x] added tests
- [ ] updated/added doxygen
- [ ] updated appropriate READMEs
- [ ] Updated manual and documentation

`Fix DecodeAltNames length check` ✕ `6446bb2`

embhorn self-assigned this 3 weeks ago

Copilot AI review requested due to automatic review settings 3 weeks ago

Copilot started reviewing on behalf of **embhorn** 3 weeks ago

View session

Copilot AI reviewed 3 weeks ago

View reviewed changes

Copilot AI left a comment

Contributor

Pull request overview

Fixes an integer underflow in `DecodeAltNames()` when parsing Subject Alternative Name (SAN) entries in the non-template ASN path, and adds a regression test to ensure malformed SAN lengths are rejected.

Changes:

- Added bounds checks before decrementing the remaining SEQUENCE length in `DecodeAltNames()`.
- Added an API-level regression test covering SAN length underflow.
- Registered the new test in the ASN test suite declarations.

Reviewed changes

Copilot reviewed 3 out of 3 changed files in this pull request and generated 5 comments.

File	Description
wolfcrypt/src/asn.c	Adds bounds checks to prevent `length` underflow while decoding SAN entries.
tests/api/test_asn.h	Declares and registers the new regression test.
tests/api/test_asn.c	Adds a regression test certificate with malformed SAN length and a control certificate.

▶ Comments suppressed due to low confidence (2)

💡 Add Copilot custom instructions for smarter, more guided reviews. Learn how to get started.

tests/api/test_asn.c Outdated Show resolved

tests/api/test_asn.c Outdated Show resolved

tests/api/test_asn.c Show resolved

tests/api/test_asn.c Show resolved

tests/api/test_asn.c Outdated Show resolved

Fix from review 8ffb096

embhorn commented 3 weeks ago Member Author

Fix confirmed by reporter

embhorn assigned **wolfSSL-Bot** and unassigned **embhorn** 3 weeks ago

dgarske approved these changes 3 weeks ago

View reviewed changes

dgarske merged commit `0f41e99` into `wolfSSL:master` 3 weeks ago

490 of 499 checks passed

View details

Sign up for free **to join this conversation on GitHub**. Already have an account? Sign in to comment

Reviewers

Copilot


dgarske

Assignees


wolfSSL-Bot

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

4 participants