wolfSSL / **wolfssl** Public

Code Issues 17 **Pull requests** 92 Actions Projects Wiki Secu

Various GI and ZD fixes #10079

Merged **douzzer** merged 11 commits into `wolfSSL:master` from `rlm2002:ghi10063` last week

Conversation 1 Commits 11 Checks 477 Files changed 5

rlm2002 commented 2 weeks ago • edited Contributor

Description

Fixes various issues reported by #GI10063 and zd21436

Testing

```
./configure --enable-all && make check
./configure --enable-harden-tls && make check
```

Checklist

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

`add guard for integer underflow in DecryptTls13` `50448ef`

rlm2002 self-assigned this 2 weeks ago

rlm2002 added 8 commits 2 weeks ago

`guard against heap buffer overflow` d4b25d0

`upper bounds check for DSA signature` 75e6406

`zeroize ssl->encrypt after transferring ownership to dup` 14695fb

`bounds check when parsing dual-algo cert sigs` 3bc72b5

`check idx before accessing certificate list` 1766b91

`if len is 0, do not subtract 1 when calling XMALLOC` a696d11

`add check to prevent integer underflow` a963c5f

`break when idx greater than MAX_CHAIN_DEPTH` ✕ ce7b81b

rlm2002 force-pushed the `ghi10063` branch from **`8eb7677`** to **`ce7b81b`** 2 weeks ago Compare

rlm2002 added 2 commits 2 weeks ago

`return null if len<=0` a827a82

`free authInPadded if alloc'd on early return` ✕ 8b2fd34

rlm2002 force-pushed the `ghi10063` branch from **`432640b`** to **`8b2fd34`** 2 weeks ago Compare

rlm2002 commented 2 weeks ago • edited Contributor Author

Retest this please Jenkins: java.io.IOException: Unexpected termination of the channel

rlm2002 marked this pull request as ready for review 2 weeks ago

rlm2002 assigned **wolfSSL-Bot** and unassigned **rlm2002** 2 weeks ago

rlm2002 mentioned this pull request 2 weeks ago

Memory safety code review: 17 findings across compiled sources #10063

Closed

rlm2002 added the For This Release label 2 weeks ago

douzzer added the Staged label 2 weeks ago

douzzer approved these changes last week

View reviewed changes

douzzer merged commit `df05597` into `wolfSSL:master` last week

View details

651 of 656 checks passed

rlm2002 deleted the `ghi10063` branch last week

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

Reviewers

douzzer

Assignees

wolfSSL-Bot

Labels

For This Release Staged

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

3 participants