golang-fips / **openssl** Public

Code | Issues 8 | Pull requests 7 | Actions | Security 1 | Insights

Commit 85d31d0

gdams authored on Mar 20, 2024 Verified

```
Merge pull request from GHSA-78hx-gp6g-7mj6

Fix memory leak in setupEVP and newCipherCtx
```

v2 · v2.0.3 ••• v2.0.1

2 parents 576fe0d + 6e2197a commit 85d31d0

2 files changed +11 -11 lines changed

Top

Filter files…

- cipher.go
- evp.go

2 files changed +11 -11 lines changed

Search within code

cipher.go

```
@@ -533,12 +533,12 @@ func sliceForAppend(in []byte, n int) (head, tail
[]byte) {
533 533         return
534 534     }
535 535
536     - func newCipherCtx(kind cipherKind, mode cipherMode, encrypt cipherOp, key, iv
        []byte) (ctx C.GO_EVP_CIPHER_CTX_PTR, err error) {
    536 + func newCipherCtx(kind cipherKind, mode cipherMode, encrypt cipherOp, key, iv
        []byte) (_ C.GO_EVP_CIPHER_CTX_PTR, err error) {
537 537         cipher := loadCipher(kind, mode)
538 538         if cipher == nil {
539 539             panic("crypto/cipher: unsupported cipher: " + kind.String())
540 540         }
```

```
541       -     ctx = C.go_openssl_EVP_CIPHER_CTX_new()
      541 +     ctx := C.go_openssl_EVP_CIPHER_CTX_new()
542   542       if ctx == nil {
543   543           return nil, fail("unable to create EVP cipher ctx")
544   544       }
```

evp.go

```
          @@ -149,7 +149,15 @@ type verifyFunc func(C.GO_EVP_PKEY_CTX_PTR, *C.uchar,
          C.size_t, *C.uchar, C.size
149   149
150   150   func setupEVP(withKey withKeyFunc, padding C.int,
151   151       h, mgfHash hash.Hash, label []byte, saltLen C.int, ch crypto.Hash,
152       -     init initFunc) (ctx C.GO_EVP_PKEY_CTX_PTR, err error) {
      152 +     init initFunc) (_ C.GO_EVP_PKEY_CTX_PTR, err error) {
      153 +     var ctx C.GO_EVP_PKEY_CTX_PTR
      154 +     withKey(func(pkey C.GO_EVP_PKEY_PTR) C.int {
      155 +         ctx = C.go_openssl_EVP_PKEY_CTX_new(pkey, nil)
      156 +         return 1
      157 +     })
      158 +     if ctx == nil {
      159 +         return nil, newOpenSSLError("EVP_PKEY_CTX_new failed")
      160 +     }
153   161       defer func() {
154   162           if err != nil {
155   163               if ctx != nil {
          @@ -158,14 +166,6 @@ func setupEVP(withKey withKeyFunc, padding C.int,
158   166               }
159   167           }
160   168       }()
161       -
162       -     withKey(func(pkey C.GO_EVP_PKEY_PTR) C.int {
163       -         ctx = C.go_openssl_EVP_PKEY_CTX_new(pkey, nil)
164       -         return 1
165       -     })
166       -     if ctx == nil {
167       -         return nil, newOpenSSLError("EVP_PKEY_CTX_new failed")
168       -     }
169   169       if err := init(ctx); err != nil {
170   170           return nil, err
```

```
171  171          }
```

Comments 0

Please sign in to comment.