

microsoft / go-crypto-openssl Public

- <> Code
- Issues 3
- Pull requests
- Actions
- Projects
- Models
- Security

Commit 104fe7f

qmuntal committed on Feb 8, 2024

Fix memory leak in setupEVP

main (#64) · v0.2.9

1 parent ed177ef commit 104fe7f

1 file changed +9 -9 lines changed

↑ Top ⚙️

Filter files...

- openssl
 - evpkey.go

1 file changed +9 -9 lines changed

Search within code ⚙️

openssl/evpkey.go

```

@@ -101,7 +101,15 @@ type verifyFunc func(C.GO_EVP_PKEY_CTX_PTR, *C.uchar,
C.size_t, *C.uchar, C.size

101 101
102 102 func setupEVP(withKey withKeyFunc, padding C.int,
103 103 h, mgfHash hash.Hash, label []byte, saltLen C.int, ch crypto.Hash,
104 - init initFunc) (ctx C.GO_EVP_PKEY_CTX_PTR, err error) {
104 + init initFunc) (_ C.GO_EVP_PKEY_CTX_PTR, err error) {
105 + var ctx C.GO_EVP_PKEY_CTX_PTR
106 + withKey(func(pkey C.GO_EVP_PKEY_PTR) C.int {
107 +     ctx = C.go_openssl_EVP_PKEY_CTX_new(pkey, nil)
108 +     return 1
109 + })
110 + if ctx == nil {
111 +     return nil, newOpenSSLerError("EVP_PKEY_CTX_new failed")

```

```
112 + }
105 113     defer func() {
106 114         if err != nil {
107 115             if ctx != nil {
@@ -110,14 +118,6 @@ func setupEVP(withKey withKeyFunc, padding C.int,
110 118         }
111 119     }
112 120 }()
113 -
114 -     withKey(func(pkey C.GO_EVP_PKEY_PTR) C.int {
115 -         ctx = C.go_openssl_EVP_PKEY_CTX_new(pkey, nil)
116 -         return 1
117 -     })
118 -     if ctx == nil {
119 -         return nil, newOpenSSLError("EVP_PKEY_CTX_new failed")
120 -     }
121 121     if err := init(ctx); err != nil {
122 122         return nil, err
123 123     }
↓
```

Comments 0



Please [sign in](#) to comment.