New issue

Jump to bottom

some vulnerability - 0x04 an out-of-bound vulnerability in readAPICFrame function #80

Closed **Jayl1n** opened this issue on Nov 19, 2020 · 0 comments

Jayl1n commented on Nov 19, 2020

This is the fourth vulnerability in id3v2frames.go.

In readAPICFrame function, you don't check the size of b parameter. If the b parameter don't end with double zero, the size of mimeDataSplit is one after bytes.SplitN and then program will happen panic beause your check logic is a little late in line 609 .

testcase 09c7c9d4e8fcee39048684570266ce162d9437c7.zip

```
panic: runtime error: index out of range [1] with length 1

goroutine 1 [running]:
github.com/dhowden/tag.readAPICFrame(0xc0000d403e, 0x2, 0x2, 0x4, 0x122b1a0, 0x0)
        /Users/jaylin/go/pkg/mod/github.com/dhowden/tag@v0.0.0-20200828214007-46e57f75dbfc/id3v2frames.go:608 +0x556
github.com/dhowden/tag.readID3v2Frames(0x114d680, 0xc0000d2000, 0x60c1844, 0xc0000d6000, 0xc0000d2000, 0x0, 0xb)
        /Users/jaylin/go/pkg/mod/github.com/dhowden/tag@v0.0.0-20200828214007-46e57f75dbfc/id3v2.go:371 +0x810
github.com/dhowden/tag.ReadID3v2Tags(0x114daa0, 0xc0000d2000, 0x1, 0x0, 0x0, 0x0)
        /Users/jaylin/go/pkg/mod/github.com/dhowden/tag@v0.0.0-20200828214007-46e57f75dbfc/id3v2.go:428 +0xde
github.com/dhowden/tag.ReadFrom(0x114daa0, 0xc0000d2000, 0xc0000d0000, 0x1b, 0x21b, 0x0)
        /Users/jaylin/go/pkg/mod/github.com/dhowden/tag@v0.0.0-20200828214007-46e57f75dbfc/tag.go:52 +0x324
main.main()
        /Users/jaylin/GolandProjects/gofuzz_test/main.go:20 +0xb5
```

dhowden closed this as completed in a922134 on Nov 19, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant