New issue

Jump to bottom

some vulnerability - 0x02 an out-of-bound vulnerability in readAtomData function #78

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

Jayl1n commented on Nov 19, 2020

This is the second vulnerability in mp4.go.

In readAtomData function, although you check the size of b , program also will happen panic when the size of b is 3 .

testcase 8a27ec34f36eb99f06de03422f00340f091b7b67.zip

```
panic: runtime error: slice bounds out of range [:4] with capacity 3

goroutine 1 [running]:
github.com/dhowden/tag.metadataMP4.readAtomData(0x0, 0x0, 0xc000078180, 0x114daa0, 0xc000078150, 0xc0000d4028, 0x4, 0xb, 0x0, 0x0, ...)
        /Users/jaylin/go/pkg/mod/github.com/dhowden/tag@v0.0.0-20200828214007-46e57f75dbfc/mp4.go:155 +0xe28
github.com/dhowden/tag.metadataMP4.readAtoms(0x0, 0x0, 0xc000078180, 0x114daa0, 0xc000078150, 0x0, 0x0)
        /Users/jaylin/go/pkg/mod/github.com/dhowden/tag@v0.0.0-20200828214007-46e57f75dbfc/mp4.go:125 +0x16f
github.com/dhowden/tag.ReadAtoms(...)
        /Users/jaylin/go/pkg/mod/github.com/dhowden/tag@v0.0.0-20200828214007-46e57f75dbfc/mp4.go:76
github.com/dhowden/tag.ReadFrom(0x114daa0, 0xc000078150, 0xc0000d2000, 0x2f, 0x22f, 0x0)
        /Users/jaylin/go/pkg/mod/github.com/dhowden/tag@v0.0.0-20200828214007-46e57f75dbfc/tag.go:49 +0x3a1
main.main()
        /Users/jaylin/GolandProjects/gofuzz_test/main.go:20 +0xb5
```

dhowden closed this as completed in 4b595ed 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