some vulnerability - 0x01 an out-of-bound vulnerability in readPICFrame function #77

Closed **Jayl1n** opened this issue on Nov 19, 2020 · 3 comments

Jayl1n commented on Nov 19, 2020

Hello, I found some vulnerability in this respository, they are could be used to cause a denial of service via decode some evil file.

This is the first vulnerability in id3v2frames.go.

In readPICFrame function, you don't check the size of b parameter. If the size of b is zero or less than 6 , program will happen panic.

testcase 147678a9d5f9418743fccc6bd8e9e2ca8f4f2f59.zip

info

```
panic: runtime error: index out of range [4] with length 4

goroutine 1 [running]:
github.com/dhowden/tag.readPICFrame(0xc00001a114, 0x4, 0x4, 0x3, 0x12733a0, 0x0)
        /Users/jaylin/go/pkg/mod/github.com/dhowden/tag@v0.0.0-20200828214007-46e57f75dbfc/id3v2frames.go:566 +0x568
github.com/dhowden/tag.readID3v2Frames(0x1182da0, 0xc0000743c0, 0x14, 0xc00000c120, 0xc0000743c0, 0x0, 0xb)
        /Users/jaylin/go/pkg/mod/github.com/dhowden/tag@v0.0.0-20200828214007-46e57f75dbfc/id3v2.go:378 +0x913
github.com/dhowden/tag.ReadID3v2Tags(0x1183160, 0xc0000743c0, 0x1, 0x0, 0x0, 0x0)
        /Users/jaylin/go/pkg/mod/github.com/dhowden/tag@v0.0.0-20200828214007-46e57f75dbfc/id3v2.go:428 +0x158
github.com/dhowden/tag.ReadFrom(0x1183160, 0xc0000743c0, 0x106c936, 0x5fb6611c, 0x12044e00, 0xabb5e046976f)
        /Users/jaylin/go/pkg/mod/github.com/dhowden/tag@v0.0.0-20200828214007-46e57f75dbfc/tag.go:52 +0x486
gofuzz_test/tag.Fuzz(0x4010000, 0x14, 0x14, 0x4)
        /Users/jaylin/GolandProjects/gofuzz_test/tag/tag_fuzzer.go:9 +0xb2
go-fuzz-dep.Main(0xc0000b9f48, 0x1, 0x1)
        go-fuzz-dep/main.go:36 +0x1ad
main.main()
        gofuzz_test/tag/go.fuzz.main/main.go:15 +0x52
exit status 2
```

Jayl1n changed the title ~~some vulnerability - #1 an out-of-bound vulnerability in readPICFrame function~~ some vulnerability - 0x01 an out-of-bound vulnerability in readPICFrame function on Nov 19, 2020

dhowden closed this as completed in `6b18201` on Nov 19, 2020

swapnilpotnis commented on Dec 29, 2020

@dhowden: We are currently facing vulnerability(CVE-2020-29242) on similar lines for a different package:

Error: dhowden tag before 2020-11-19 allows "panic: runtime error: index out of range" via readPICFrame.

Package: taglibs-standard-impl-1.2.5

From the maven repository, 1.2.5(https://mvnrepository.com/artifact/org.apache.taglibs/taglibs-standard-spec) seems to be the latest package available.
Can you please suggests any workaround for the issue??

dhowden commented on Dec 30, 2020 • edited Owner

Hi **@swapnilpotnis**

This issue (along with a few others) were fixed on 2020-11-20.

I'm not familiar with that Java library, but the description is "An implementation of the JSP Standard Tag Library (JSTL) Specification API", dated 2015, which does not seem to be related to extracting metadata from music files?

How are you seeing this error? If you need to make a quick fix, I would recommend wrapping all calls to this library with recover methods so that you can stop panics before they crash the running process: see https://blog.golang.org/defer-panic-and-recover for more details.

jasonparallel commented on Jan 4, 2021

@swapnilpotnis Getting the error from https://github.com/jeremylong/DependencyCheck? Looks a like a false positive to me.

👍 6

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants