

New issue

Jump to bottom

x/text: panic in language.ParseAcceptLanguage while processing bcp47 tag #42536



ph1048 opened this issue on Nov 12, 2020 · 8 comments

Labels FrozenDueToAge NeedsInvestigation
Milestone Unreleased

ph1048 commented on Nov 12, 2020

What version of Go are you using (go version)?

```
$ go version
go version go1.15.4 linux/amd64
```

Does this issue reproduce with the latest release?

What operating system and processor architecture are you using (go env)?

go env Output

What did you do?

<https://play.golang.org/p/SwAU9tKYRsj>

What did you expect to see?

Error via return value

What did you see instead?

```
panic: runtime error: slice bounds out of range [9:8]

goroutine 1 [running]:
golang.org/x/text/internal/language.(*scanner).resizeRange(0xc00068d08, 0x6, 0x8, 0x3)
    /tmp/gopath300097471/pkg/mod/golang.org/x/text@v0.3.4/internal/language/parse.go:142 +0x2e7
golang.org/x/text/internal/language.(*scanner).replace(...)
    /tmp/gopath300097471/pkg/mod/golang.org/x/text@v0.3.4/internal/language/parse.go:151
golang.org/x/text/internal/language.parseTag(0xc00068d08, 0x0, 0x0, 0xc0007e0a3)
    /tmp/gopath300097471/pkg/mod/golang.org/x/text@v0.3.4/internal/language/parse.go:296 +0x13b
golang.org/x/text/internal/language.parseExtension(0xc00068d08, 0x8)
    /tmp/gopath300097471/pkg/mod/golang.org/x/text@v0.3.4/internal/language/parse.go:552 +0xe74
golang.org/x/text/internal/language.parseExtensions(0xc00068d08, 0x3030000000000)
    /tmp/gopath300097471/pkg/mod/golang.org/x/text@v0.3.4/internal/language/parse.go:451 +0xa5
golang.org/x/text/internal/language.parse(0xc00068d08, 0x4d9210, 0x7, 0x3030000000000, 0x0, 0x0, 0x0, 0x0)
    /tmp/gopath300097471/pkg/mod/golang.org/x/text@v0.3.4/internal/language/parse.go:268 +0x2bc
golang.org/x/text/internal/language.Parse(0x4d9210, 0x7, 0x0, 0x0, 0x0, 0x4b1185, 0x4d9210)
    /tmp/gopath300097471/pkg/mod/golang.org/x/text@v0.3.4/internal/language/parse.go:250 +0x1c7
golang.org/x/text/language.CanonicalType.Parse(0x17, 0x4d9210, 0x7, 0x4d9210, 0x7, 0x0, 0x0, 0x3fc0389239a6386c)
    /tmp/gopath300097471/pkg/mod/golang.org/x/text@v0.3.4/language/parse.go:46 +0x3f
golang.org/x/text/language.Parse(...)
    /tmp/gopath300097471/pkg/mod/golang.org/x/text@v0.3.4/language/parse.go:34
golang.org/x/text/language.ParseAcceptLanguage(0x4d9210, 0x7, 0xc00068f48, 0x442bca, 0x56ed40, 0xc00032778, 0xc00068f78, 0x405e25, 0xc0005e058, 0x0)
    /tmp/gopath300097471/pkg/mod/golang.org/x/text@v0.3.4/language/parse.go:154 +0x165
main.main()
    /tmp/sandbox168582112/prog.go:10  ##+0x3a
```

odeke-em changed the title ~~text/language: panic in language.ParseAcceptLanguage while processing bcp47 tag~~ x/text: panic in language.ParseAcceptLanguage while processing bcp47 tag on Nov 12, 2020

gopherbot added this to the Unreleased milestone on Nov 12, 2020

odeke-em commented on Nov 12, 2020

Member

Thank you for this report @ph1048! Kindly paging @mpvl

1

odeke-em added the NeedsInvestigation label on Nov 12, 2020

mengzhuo commented on Nov 17, 2020

Contributor

Hmm...Gobot not working

<https://go-review.googlesource.com/c/text/+270697>

odeke-em commented on Nov 17, 2020

Member

@mengzhao thanks for mailing the fix! To get gobot to attach to the proper issue, for any repo that isn't the main Go repository, please use this format:
Fixes golang/go#NNNN

gopherbot commented on Nov 17, 2020

Change <https://golang.org/cl/270697> mentions this issue: internal/language: fix resizeRange index wrong way

mengzhao commented on Nov 17, 2020

Contributor

@odeke-em it works, thanks for the info.



gopherbot closed this as completed in [golang/text@4482a91](#) on Nov 17, 2020

carnil commented on Jan 2, 2021

CVE-2020-28852 appears to have been assigned for this issue.

andyledwardsibm commented on Jan 7, 2021

It looks like the fix isn't in a "released" version yet (<https://github.com/golang/text/releases/tag/v0.3.4> looks like the latest release and that's from before the fix went in). Is that accurate? How do I get the fixed code?

rsc commented on Jan 8, 2021

Contributor

This is fixed in the just-released v0.3.5. Sorry for the delayed tagging.



dvasilen mentioned this issue on Jan 21, 2021

x/text: panic in language.ParseAcceptLanguage while parsing -u- extension #42535

Closed

sfowl mentioned this issue on Jan 29, 2021

x/net: bump x/text to v0.3.5 to fix CVE-2020-28852 #43983

Closed

sfowl mentioned this issue on Feb 17, 2021

Update affected version info for CVE-2020-28852 CVEProject/cvelist#855

Merged

RaduBerinde mentioned this issue on Apr 20, 2021

vendor/language: v20.2.6: mysterious index out of bounds in golang.org/x/text/internal/language cockroachdb/cockroach#63562

Closed

dims mentioned this issue on May 28, 2021

Bump golang.org/x/text to v0.3.6 kubernetes/kubernetes#102409

Merged

ncopa added a commit to ncopa/k0s that referenced this issue on Oct 28, 2021

Lock golang.org/x/text to v0.3.6 in go.mod (CVE-2020-28852) ...

abfa8b4

ncopa added a commit to ncopa/k0s that referenced this issue on Oct 28, 2021

Lock golang.org/x/text to v0.3.6 in go.mod (CVE-2020-28852) ...

7b0793d

ncopa added a commit to ncopa/k0s that referenced this issue on Oct 28, 2021

Lock golang.org/x/text to v0.3.6 in go.mod (CVE-2020-28852) ...

ac41ead

ncopa added a commit to ncopa/k0s that referenced this issue on Oct 28, 2021


Lock golang.org/x/text to v0.3.6 in go.mod (CVE-2020-28852) ...


7284218


ncopa added a commit to ncopa/k0s that referenced this issue on Oct 28, 2021

Lock golang.org/x/text to v0.3.6 in go.mod (CVE-2020-28852) ...

01246ac

 **golang** locked and limited conversation to collaborators on Jan 8

 **gopherbot** added the `FrozenDueToAge` label on Jan 8

 **xhit** pushed a commit to xhit/text that referenced this issue on Oct 10

 `internal/language: fix resizeRange index wrong way` ...

33ac990

Assignees

No one assigned

Labels

`FrozenDueToAge` **`NeedsInvestigation`**

Projects

None yet

Milestone

Unreleased

Development

No branches or pull requests

7 participants

