New issue

Jump to bottom

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

Closed ph1048 opened this issue on Nov 12, 2020 · 16 comments

Labels FrozenDueToAge NeedsInvestigation

Milestone Unreleased

ph1048 commented on Nov 12, 2020 • edited

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/FCHj_rCBdiH

What did you expect to see?

Error via return value

What did you see instead?

```
panic: runtime error: index out of range [17] with length 14

goroutine 1 [running]:
golang.org/x/text/internal/language.Tag.findTypeForKey(0x202000000013e, 0xc00002c070, 0xe, 0x4d8c35, 0x2, 0x2d01104014010d0, 0x21127901ec11a0, 0x14e1470015e1424)
        /tmp/gopath829095260/pkg/mod/golang.org/x/text@v0.3.4/internal/language/language.go:456 +0x366
golang.org/x/text/internal/language.Tag.TypeForKey(0x202000000013e, 0xc00002c070, 0xe, 0x4d8c35, 0x2, 0xe, 0x20)
        /tmp/gopath829095260/pkg/mod/golang.org/x/text@v0.3.4/internal/language/language.go:307 +0x4d
golang.org/x/text/internal/language/compact.Make(0x202000000013e, 0xc00002c070, 0xe, 0xc00002c070, 0xe, 0x4fbf00)
        /tmp/gopath829095260/pkg/mod/golang.org/x/text@v0.3.4/internal/language/compact/language.go:38 +0x65
golang.org/x/text/language.makeTag(...)
        /tmp/gopath829095260/pkg/mod/golang.org/x/text@v0.3.4/language/language.go:25
golang.org/x/text/language.CanonType.Parse(0x17, 0x4da9c2, 0x10, 0x4da9c2, 0x10, 0x0, 0x0, 0x3fc0389239a6386c)
        /tmp/gopath829095260/pkg/mod/golang.org/x/text@v0.3.4/language/parse.go:48 +0x145
golang.org/x/text/language.Parse(...)
        /tmp/gopath829095260/pkg/mod/golang.org/x/text@v0.3.4/language/parse.go:34
golang.org/x/text/language.ParseAcceptLanguage(0x4da9c2, 0x10, 0xc000068f48, 0x442bca, 0x56ed40, 0xc000032778, 0xc000068f78, 0x405e25, 0xc00005e058, 0x0)
        /tmp/gopath829095260/pkg/mod/golang.org/x/text@v0.3.4/language/parse.go:154 +0x165
main.main()
        /tmp/sandbox226474929/prog.go:10 +0x3a
```

ph1048 changed the title ~~text/language: panic in language.ParseAcceptLanguage while parsing -u- extension~~ x/text: panic in language.ParseAcceptLanguage while parsing -u- extension on Nov 12, 2020

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

cagedmantis added the NeedsInvestigation label on Nov 13, 2020

cagedmantis commented on Nov 13, 2020 Contributor

/cc @mpvl

carnil commented on Jan 2, 2021

CVE-2020-28851 appears to have been assigned for this issue.

andyedwardsibm commented on Jan 7, 2021 • edited

Is a fix available for this, or any info on what version of go it will go into? Or is it just x/text that's affected and the fix will be there (may already be there)?

dvasilen commented on Jan 21, 2021 • edited

The latest text v0.3.5 #42536 (comment) still does not have a fix for this issue.

```
package main

import (
        "fmt"

        "golang.org/x/text/language"
)

func main() {
//      _, _, err := language.ParseAcceptLanguage("00-t-0o") // fixed CVE-2020-28852
//      fmt.Println("Error:", err)
// Error: language: tag is not well-formed


        _, _, err := language.ParseAcceptLanguage("ES-v-00-u-000-00") // not fixed CVE-2020-28851
        fmt.Println("Error:", err)
// panic: runtime error: index out of range [17] with length 14
}
```

/cc **@rsc**

dvasilen commented on Jan 30, 2021

Any update/ETA on this issue is appreciated.

benjsmi commented on Feb 4, 2021

+1 -- any word on the progress of this?

rsc commented on Feb 10, 2021 Contributor

Discussed with **@mpvl** - this is in a different part of the code and still needs to be fixed. He will work on it.

gopherbot commented on Feb 18, 2021

Change https://golang.org/cl/293549 mentions this issue: `language: allow variable number of types per key in -u- extension`

Jethzabell commented on Feb 26, 2021

"Any update/ETA on this issue is appreciated."

gopherbot closed this as completed in `golang/text@e3aa4ad` on Feb 27, 2021

---

mpvl commented on Feb 27, 2021 Contributor

@Jethzabell: submitted a fix.

1

zhsj commented on Feb 28, 2021

A new tag on x/text is appreciated.

dvasilen commented on Feb 28, 2021

+1

dvasilen commented on Mar 1, 2021

While we are waiting for the tag ... here is the go.mod update to pick up the fix

```
golang.org/x/text v0.3.6-0.20210227105805-e3aa4adf54f6
```

benjsmi commented on Mar 18, 2021 • edited

I'm somewhat new to the Go community, but I have observed that with go1.16.2, when you run `go get golang.org/x/text/language`, it still pulls version v0.3.5 of this module instead of the newly-fixed 0.3.6. Can someone help me track when that would/will change? So far, I've been watching on https://golang.org/doc/devel/release.html#go1.16 and also https://github.com/golang/go/issues?q=milestone%3AGo1.16.2+label%3ACherryPickApproved as examples.

I should note: I'm aware I can change the version that is used in my `go.mod`, but my team uses countless Go components that would need to be checked for the existence of golang.org/x/text -- it would be much much easier if the default version installed is the one mentioned by **@dvasilen** above.

1

RSAlderman commented on Mar 26, 2021

Any idea when the tagged v0.3.6 version with the fix will be available?

mpvl commented on Mar 26, 2021 — Contributor

There is another urgent fix pending and will tag afterwards.

> On Fri, Mar 26, 2021 at 12:06 RSAlderman ***@***.***> wrote:
> Any idea when the tagged v0.3.6 version
> <https://github.com/golang/text/tags> with the fix will be available?
>
> —
> You are receiving this because you were mentioned.
> Reply to this email directly, view it on GitHub
> <#42535 (comment)>, or
> unsubscribe
> <https://github.com/notifications/unsubscribe-auth/ABRFSR6BGN6LTZHUFMVJAL3TFRTCPANCNFSM4TTEOOYA>
> .

--
Marcel van Lohuizen -- Google Switzerland GmbH -- Identifikationsnummer:
CH-020.4.028.116-1

👍 1

Madhu-1 added a commit to Madhu-1/ceph-csi that referenced this issue on Jun 4, 2021

`rebase: update golang.org/x/text to 0.3.6` ··· `34dc43d`

Madhu-1 mentioned this issue on Jun 4, 2021

rebase: update golang.org/x/text to 0.3.6 ceph/ceph-csi#2132

Closed

golang locked and limited conversation to collaborators on Mar 26

gopherbot added the FrozenDueToAge label on Mar 26

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

`language: allow variable number of types per key in -u- extension` ··· `3b780af`

Assignees

No one assigned

Labels

FrozenDueToAge NeedsInvestigation

Projects

None yet

Milestone

Unreleased

Development

No branches or pull requests

12 participants