

[New issue](#)[Jump to bottom](#)

# v3: panic "attempted to parse unknown event (please report): none" #666

✓ Closed

bradleyjkemp opened this issue on Oct 21, 2020 · 23 comments

bradleyjkemp commented on Oct 21, 2020

Hi folks 🙋 Found this panic (along with #665) while fuzzing my own project.

Minimal example of the panic ([https://play.golang.org/p/gLM\\_eHzcrgz](https://play.golang.org/p/gLM_eHzcrgz)):

```
package main

import (
    "gopkg.in/yaml.v3"
)

func main() {
    var t interface{}
    yaml.Unmarshal([]byte("0: [!00 \xef"), &t)
}
```

Output:

```
panic: internal error: attempted to parse unknown event (please report): none [recovered]
    panic: internal error: attempted to parse unknown event (please report): none

goroutine 1 [running]:
gopkg.in/yaml%2ev3.handleErr(0xc000043f60)
    /tmp/gopath818249317/pkg/mod/gopkg.in/yaml.v3@v3.0.0-20200615113413-eeeca48fe776/yaml.go:294 +0x85
panic(0x50f120, 0xc000010330)
    /usr/local/go-faketime/src/runtime/panic.go:969 +0x1b9
gopkg.in/yaml%2ev3.(*parser).parse(0xc000036c00, 0x0)
    /tmp/gopath818249317/pkg/mod/gopkg.in/yaml.v3@v3.0.0-20200615113413-eeeca48fe776/decode.go:163 +0x277
gopkg.in/yaml%2ev3.(*parser).parseChild(...)
    /tmp/gopath818249317/pkg/mod/gopkg.in/yaml.v3@v3.0.0-20200615113413-eeeca48fe776/decode.go:194
gopkg.in/yaml%2ev3.(*parser).sequence(0xc000036c00, 0xc00000e007)
```

```
/tmp/gopath818249317/pkg/mod/gopkg.in/yaml.v3@v3.0.0-20200615113413-
eeeca48fe776/decode.go:259 +0xff
gopkg.in/yaml%2ev3.(*parser).parse(0xc000036c00, 0x0)
/tmp/gopath818249317/pkg/mod/gopkg.in/yaml.v3@v3.0.0-20200615113413-
eeeca48fe776/decode.go:154 +0xe7
gopkg.in/yaml%2ev3.(*parser).parseChild(0xc000036c00, 0xc00007e3c0, 0xc00007e460)
/tmp/gopath818249317/pkg/mod/gopkg.in/yaml.v3@v3.0.0-20200615113413-
eeeca48fe776/decode.go:194 +0x2f
gopkg.in/yaml%2ev3.(*parser).mapping(0xc000036c00, 0x9)
/tmp/gopath818249317/pkg/mod/gopkg.in/yaml.v3@v3.0.0-20200615113413-
eeeca48fe776/decode.go:285 +0x1ad
gopkg.in/yaml%2ev3.(*parser).parse(0xc000036c00, 0xc000000003)
/tmp/gopath818249317/pkg/mod/gopkg.in/yaml.v3@v3.0.0-20200615113413-
eeeca48fe776/decode.go:152 +0x10d
gopkg.in/yaml%2ev3.(*parser).parseChild(...)
/tmp/gopath818249317/pkg/mod/gopkg.in/yaml.v3@v3.0.0-20200615113413-
eeeca48fe776/decode.go:194
gopkg.in/yaml%2ev3.(*parser).document(0xc000036c00, 0x3)
/tmp/gopath818249317/pkg/mod/gopkg.in/yaml.v3@v3.0.0-20200615113413-
eeeca48fe776/decode.go:203 +0x8b
gopkg.in/yaml%2ev3.(*parser).parse(0xc000036c00, 0x0)
/tmp/gopath818249317/pkg/mod/gopkg.in/yaml.v3@v3.0.0-20200615113413-
eeeca48fe776/decode.go:156 +0x87
gopkg.in/yaml%2ev3.unmarshal(0xc00002c590, 0xa, 0xa, 0x50a080, 0xc000010320, 0x0, 0x0, 0x0)
/tmp/gopath818249317/pkg/mod/gopkg.in/yaml.v3@v3.0.0-20200615113413-
eeeca48fe776/yaml.go:161 +0x26a
gopkg.in/yaml%2ev3.Unmarshal(...)
/tmp/gopath818249317/pkg/mod/gopkg.in/yaml.v3@v3.0.0-20200615113413-
eeeca48fe776/yaml.go:89
main.main()
/tmp/sandbox604520862/prog.go:9 +0x99
```



1

niemeyer commented on Oct 22, 2020

Contributor

Thanks for the report, I'll look into it.

hasheddan commented on Apr 21, 2021

As another data point, I found this occurs on invalid YAML that includes `{{`, which is common in manifests that are deployed with helm, such as [this one](#).



hasheddan mentioned this issue on Apr 21, 2021

Improve Yaml Parsing & CRD Selection crdsdev/doc#145

🔗 Open

howardjohn commented on Jul 20, 2021

[repro.txt](#)

Same issue with YAML above ^

stevebeattie commented on May 20

This issue was assigned [CVE-2022-28948](#)



crenshaw-dev commented on May 20

Issue 666. 🐙



crenshaw-dev commented on May 20 • edited ▼

For people who land here from Snyk: they incorrectly [marked the vulnerability as being in v2](#). I've been unable to reproduce the issue in v2, and can only reproduce it in v3. I've notified Snyk of the error.

UPDATE: They fixed it!

UPDATE 2: For people who land here from the GitHub security advisory: they incorrectly [marked the vulnerability as being in v2](#). Trying to find an appropriate version range to suggest...



 niemeyer closed this as completed in [8f96da9](#) on May 21

niemeyer commented on May 21

Contributor

Sorry for being slow. The *post mortem* is that long ago I was thrown off by an awkward API in the underlying library: it returns success (true) in error cases in that particular function call, while in general it does not. Instead of fixing the underlying API, we'll continue to tolerate it for the time being and handle the issue on the high-level decoder, so that it remains somewhat easy to compare the original libyaml logic to what remains of it in go-yaml.



CityOfLight77 commented on May 22

@niemeyer @stevebeattie why this crash worth a CVE, and no severity?

crenshaw-dev commented on May 22

@CityOfLight77 it's a CVE because a lot of apps use go-yaml. If a malicious user sends one of these payloads to such an app, they can shut down the app (Denial of Service).

Snyk assigned a severity of 7.5. The severity really depends on how your app uses go-yaml. If an unauthenticated user can send a malicious payload, then the severity is higher than it would be if they must be authenticated.



CityOfLight77 commented on May 22

@CityOfLight77 it's a CVE because a lot of apps use go-yaml. If a malicious user sends one of these payloads to such an app, they can shut down the app (Denial of Service).

Snyk assigned a severity of 7.5. The severity really depends on how your app uses go-yaml. If an unauthenticated user can send a malicious payload, then the severity is higher than it would be if they must be authenticated.

Thanks for the explanation



  Zenithar mentioned this issue on May 23

**fix(decoder): panic raised on fuzzer inputs. #850**



  nabbar mentioned this issue on May 23

**Yaml.v2 / Yaml.v3 - CVE 2022-28948 nabbar/golib#139**



benjifin commented on May 23

@crenshaw-dev thanks for the heads up - we (Snyk) have updated our advisory now to only show versions of yaml v3 as vulnerable, and also included the fix advice released in v3.0.0. That should be live in an hour or so



niemeyer commented on May 23

Contributor

Thanks all.



🔗 yongtang added a commit to yongtang/coredns that referenced this issue on May 26



Update gopkg.in/yaml.v3 to v3.0.0 to fix security issues ...

✓ 46784d8

🔗 yongtang mentioned this issue on May 26

Update gopkg.in/yaml.v3 to v3.0.0 to fix security issues coredns/coredns#5408

🔗 Merged

🔗 alemorcuq mentioned this issue on May 26

Update gopkg.in/yaml.v3 to v3.0.0 bitnami-labs/sealed-secrets#852

🔗 Merged

🔗 edigaryev mentioned this issue on May 26

Bump gopkg.in/yaml.v3 to 3.0.0 stretchr/testify#1190

🔗 Closed

🔗 rafaeljusto added a commit to Teamwork/kommentaar that referenced this issue on May 26



Fix: Upgrade gopkg.in/yaml.v2 to gopkg.in/yaml.v3 due to security issue ...

✗ cf184d7

🔗 rafaeljusto mentioned this issue on May 26

Fix: Upgrade gopkg.in/yaml.v2 to gopkg.in/yaml.v3 due to security issue

## Teamwork/kommentaar#91

 Merged

 **rafaeljusto** added a commit to Teamwork/kommentaar that referenced this issue on May 26



Fix: Upgrade gopkg.in/yaml.v2 to gopkg.in/yaml.v3 due to security issue ...

✓ 8cea7c5

 **willfindlay** added a commit to willfindlay/tetragon that referenced this issue on May 26



vendor: upgrade yaml.v3 to v3.0.0 ...

d6f426f

  **willfindlay** mentioned this issue on May 26

**vendor: upgrade yaml.v3 to v3.0.0 cilium/tetragon#86**

 Merged

 **michi-covalent** pushed a commit to cilium/tetragon that referenced this issue on May 26



vendor: upgrade yaml.v3 to v3.0.0 ...

✓ 2122de7

  **vara-bonthu** mentioned this issue on May 26

**Fix for Go package CVE-2022-28948 aws-ia/terraform-aws-eks-blueprints#583**

 Merged

 6 tasks

 **chrisohaver** pushed a commit to coredns/coredns that referenced this issue on May 26



Update gopkg.in/yaml.v3 to v3.0.0 to fix security issues (#5408) ...

✓ bd4675b

**codyoss** commented on May 26

For people who land here from Snyk: they incorrectly [marked the vulnerability as being in v2](#). I've been unable to reproduce the issue in v2, and can only reproduce it in v3. I've notified Snyk of the error.

This seems to be correct from my testing too, maybe the OP could be edited to say there is no issue in v2 at the top. The GH advisory that came out on this is misleading people to upgrade I believe.

**crenshaw-dev** commented on May 26

@codyoss which GH SA? I'm not seeing one on this repo.

73 hidden items

[Load more...](#)

  lpar mentioned this issue on Jun 3

**Update to gopkg.in/yaml.v3** pariz/gountries#47

 Merged

  sks mentioned this issue on Jun 6

**Update to gopkg.in/yaml.v3** onsi/gomega#556

 Merged

 This was referenced on Jun 6

**New CVE was discovered CVE-2022-28948** sirupsen/logrus#1336

 Closed



**update gopkg.in/yaml.v3 to v3.0.1** sirupsen/logrus#1337

 Merged

  kentwelcome mentioned this issue on Jun 7

**CVE-2022-28948 Go-Yaml v3** InfuseAI/TaoKanOperator#1

 Open

  nareshkumarthota mentioned this issue on Jun 7

**CVE-2022-28948 (High) detected in github.com/go-yaml/yaml-496545a6307b2a7d7a710fd516e5e16e8ab62dbc - autoclosed** TIBCOSoftware/be-tools#282

 Closed

 kaworu added a commit to cilium/cilium-cli that referenced this issue on Jun 10

 vendor: update yaml.v3 to v3.0.1 ...

✓ 58422e9

  **kaworu** mentioned this issue on Jun 10

**vendor: update yaml.v3 to v3.0.1 cilium/cilium-cli#911**

 Merged

 **kaworu** added a commit to cilium/fake that referenced this issue on Jun 10

 vendor: update yaml.v3 to v3.0.1 ... fecb944

 **kaworu** added a commit to cilium/hubble-ui that referenced this issue on Jun 10

 backend/vendor: update yaml.v3 to v3.0.1 ... 02d6636

 **kaworu** added a commit to cilium/fake that referenced this issue on Jun 10

 vendor: update yaml.v3 to v3.0.1 ... 7ce2426

 **kaworu** added a commit to cilium/fake that referenced this issue on Jun 10

 vendor: update yaml.v3 to v3.0.1 ... 5bf18a0

 **tklauser** pushed a commit to cilium/cilium-cli that referenced this issue on Jun 10

 vendor: update yaml.v3 to v3.0.1 ... ✓ b04add2

 **kaworu** added a commit to cilium/hubble-ui that referenced this issue on Jun 10


 backend/vendor: update yaml.v3 to v3.0.1 ... dbd8172

  **dims** mentioned this issue on Jun 11

**Update gopkg.in/yaml.v3 to v3.0.1 kubernetes/kubernetes#110520**

 Merged

 **qu1queee** added a commit to qu1queee/pkg that referenced this issue on Jun 17

 Add fix for [CVE-2022-28948](#) ... 2ac4c7f

  **qu1queee** mentioned this issue on Jun 17



## Add fix for CVE-2022-28948 knative/pkg#2532

 Merged

 qu1queee added a commit to qu1queee/pkg that referenced this issue on Jun 17



Add fix for CVE-2022-28948 ...

a3595e1

 qu1queee added a commit to qu1queee/pkg that referenced this issue on Jun 17





Add fix for CVE-2022-28948 ...

81f533d

 6543 mentioned this issue on Jun 18

**Migrate from gopkg.in/yaml.v2 to gopkg.in/yaml.v3** go-gitea/gitea#18239

 Closed

 knative-prow  pushed a commit to knative/pkg that referenced this issue on Jun 21



Add fix for CVE-2022-28948 (#2532) ...

✗ 1f01575

ZiViZiViZ commented on Jul 7

Issue 666 



2

 jzding mentioned this issue on Jul 29

**Bug 2091213: Update gopkg.in/yaml.v3 to v3.0.0 for security fix** redhat-cne/cloud-event-proxy#130

 Merged

 KnVerey mentioned this issue on Aug 17

**Update internal go-yaml fork to v3.0.1** kubernetes-sigs/kustomize#4764

 Merged

 heyLu mentioned this issue on Aug 19

## Incorrect vulnerability details for sonatype-2022-4070 (does not apply to yaml.v2)

OSSIndex/vulns#322

🔗 Open

🔗  stefanb mentioned this issue on Aug 21

**Bump github.com/stretchr/testify from 1.7.1 to 1.8.0** stretchr/objx#121

🔗 Merged

🔗  Lepidopteron mentioned this issue on Sep 27

**Updated Redis v8 to v9** hellofresh/health-go#78

🔗 Merged

🔗  paulyeo21 mentioned this issue on Oct 3

**Bump kubernetes API version which uses yaml lib** aws/aws-app-mesh-controller-for-k8s#642

🔗 Merged

🔗  Slijkhuis mentioned this issue on Oct 10

**Upgrade dependencies, add Go 1.19 as target** jinzhu/configor#82

🔗 Open

🔗  ColbertBrave mentioned this issue on Oct 13

**The current package gopkg.in/yaml.v3 should be updated to the latest version** gin-gonic/gin#3362

🔗 Open

### Assignees

No one assigned

### Labels

None yet

### Projects

None yet

---

Milestone

No milestone

---

Development

Successfully merging a pull request may close this issue.

 **Bump gopkg.in/yaml.v3 to 3.0.0**  
edigaryev/testify

---

13 participants

