

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

math/big: index out of range in Float.GobDecode #53871

✓ Closed

catenacyber opened this issue on Jul 14 · 11 comments

Labels

NeedsFix

release-blocker

Security

Milestone

Go1.19

catenacyber commented on Jul 14

Contributor

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

```
$ go version
go version go1.17.6 darwin/amd64
```

Does this issue reproduce with the latest release?

Yes

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

► go env Output

What did you do?Run <https://go.dev/play/p/-iOX1cXown9> ie Float0.GobDecode([]byte{0x1, 0x0, 0x0, 0x0})**What did you expect to see?**

The program finishing and printing somme Hello, without having allocated too much space

What did you see instead?

```
panic: runtime error: index out of range [3] with length 2
```

```
goroutine 1 [running]:
encoding/binary.bigEndian.Uint32(...)
    /usr/local/go-faketime/src/encoding/binary/binary.go:112
math/big.(*Float).GobDecode(0x60?, {0xc000070f34?, 0xc00006a000?, 0x0?})
    /usr/local/go-faketime/src/math/big/floatmarsh.go:83 +0x23d
main.main()
    /tmp/sandbox1173043807/prog.go:12 +0x56

Program exited.
```

Found by <https://github.com/catenacyber/ngolo-fuzzing> on oss-fuzz
<https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=49120>

mknyszek commented on Jul 14

Contributor

CC @griesemer @golang/security

  mknyszek added the **NeedsInvestigation** label on Jul 14

  mknyszek added this to the **Backlog** milestone on Jul 14

catenacyber commented on Jul 14

Contributor

Author

Oh I thought GobDecode was not a security issue...

mknyszek commented on Jul 14 • edited ▼

Contributor

Ah, no, it's just owned in part by the Go security team. I don't know whether this is a security issue. (See <https://dev.golang.org/owners>.)

  rolandshoemaker added **Security** **NeedsFix** and removed **NeedsInvestigation** labels on Jul 15

rolandshoemaker commented on Jul 15

Member

Generally we consider panics in functions which take external input to be security issues. If you are not sure, feel free to send a message to security@golang.org before opening an issue and we will be happy to check.

gopherbot commented on Jul 15

Change <https://go.dev/cl/417774> mentions this issue: math/big: check buffer lengths in GobDecode

catenacyber commented on Jul 21

Contributor

Author

Another reproducer for Rat : https://go.dev/play/p/6Qpskg2_Abp

rolandshoemaker commented on Jul 27

Member

@gopherbot please open backports, this is a security issue.

 This was referenced on Jul 27

math/big: index out of range in Float.GobDecode [1.17 backport] #54094

✓ Closed

math/big: index out of range in Float.GobDecode [1.18 backport] #54095

✓ Closed

gopherbot commented on Jul 27

Backport issue(s) opened: #54094 (for 1.17), #54095 (for 1.18).

Remember to create the cherry-pick CL(s) as soon as the patch is submitted to master, according to <https://go.dev/wiki/MinorReleases>.



gopherbot closed this as completed in [055113e](#) on Jul 27

gopherbot commented on Jul 27

Change <https://go.dev/cl/419814> mentions this issue: [release-branch.go1.17] math/big: check buffer lengths in GobDecode

gopherbot commented on Jul 27

Change <https://go.dev/cl/419815> mentions this issue: [release-branch.go1.18] math/big: check buffer lengths in GobDecode

catenacyber commented on Jul 28

Contributor

Author

please open backports, this is a security issue.

So, I should have sent a mail instead of opening a GitHub issue, sorry about missing it.
Will there be a CVE and security release for 1.18 ?

 gopherbot pushed a commit that referenced this issue on Jul 29



[release-branch.go1.18] math/big: check buffer lengths in GobDecode ...

9240558

 gopherbot pushed a commit that referenced this issue on Jul 29



[release-branch.go1.17] math/big: check buffer lengths in GobDecode ...

703c8ab

 dmitshur modified the milestones: **Backlog, Go1.19** on Jul 31



 tatianab mentioned this issue on Aug 1



x/vulndb: potential Go vuln in std: CVE-2022-32189 golang/vulndb#537

🔒 Closed

 MonsieurNicolas mentioned this issue on Aug 1



define rules and cleanup dependency tree to enable sustainable releases in the future
stellar/rs-soroban-env#289

🔓 Open

 dmitshur added the `release-blocker` label on Aug 1



 jproberts pushed a commit to jproberts/go that referenced this issue on Aug 9



math/big: check buffer lengths in GobDecode ...

5da50c5

 danbudris pushed a commit to danbudris/go that referenced this issue on Sep 9



[release-branch.go1.17] math/big: check buffer lengths in GobDecode ...

268843b



danbudris pushed a commit to danbudris/go that referenced this issue on Sep 9



[release-branch.go1.17] math/big: check buffer lengths in GobDecode ...

f10c299



danbudris pushed a commit to danbudris/go that referenced this issue on Sep 12



[release-branch.go1.17] math/big: check buffer lengths in GobDecode ...

6f7210d



danbudris pushed a commit to danbudris/go that referenced this issue on Sep 14



[release-branch.go1.17] math/big: check buffer lengths in GobDecode ...

2fcd1ec



rcrozean pushed a commit to rcrozean/go that referenced this issue on Oct 5



math/big: check buffer lengths in GobDecode ...

6d6e4ca



rcrozean pushed a commit to rcrozean/go that referenced this issue on Oct 12



math/big: check buffer lengths in GobDecode ...

30f6a98



rcrozean pushed a commit to rcrozean/go that referenced this issue on Oct 12



math/big: check buffer lengths in GobDecode ...

8d0b474

Assignees

No one assigned

Labels

NeedsFix release-blocker Security

Projects

None yet

Milestone

Go1.19

Development

No branches or pull requests

5 participants

