<> Code   ⊙ Issues 5k+   ⊷ Pull requests 302   💬 Discussions   ▷ Actions   ⋯

New issue   Jump to bottom

go/parser: stack exhaustion in all Parse* functions #53616

⊘ Closed   **tatianab** opened this issue on Jun 29 · 5 comments

Labels	**NeedsFix** release-blocker Security
Milestone	⇪ Go1.19

---

tatianab commented on Jun 29 · edited by mknyszek ▾

Calling any of the Parse functions on Go source code which contains deeply nested types or declarations can cause a panic due to stack exhaustion.

Thanks to Juho Nurminen of Mattermost for reporting this issue.

This is CVE-2022-1962.

(This was a PRIVATE issue tracked in http://b/236145171 and fixed by http://tg/1491025.)

/cc https://github.com/orgs/golang/teams/security and https://github.com/orgs/golang/teams/release

👍 1

🏷 🖼 **tatianab** added Security **NeedsFix** release-blocker labels on Jun 29

⇪ 🖼 **tatianab** added this to the **Go1.19** milestone on Jun 29

---

tatianab commented on Jul 6   Author

@gopherbot please open backport issues for this security fix

↗ This was referenced on Jul 6

go/parser: stack exhaustion in all Parse* functions (CVE-2022-1962) [1.17 backport] #53707

⊘ Closed

go/parser: stack exhaustion in all Parse* functions (CVE-2022-1962) [1.18 backport] #53708

⊘ Closed

---

gopherbot commented on Jul 6

Backport issue(s) opened: #53707 (for 1.17), #53708 (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 commented on Jul 12

Change https://go.dev/cl/417056 mentions this issue: `[release-branch.go1.18] go/parser: limit recursion depth`

---

gopherbot commented on Jul 12

Change https://go.dev/cl/417063 mentions this issue: `go/parser: limit recursion depth`

---

gopherbot commented on Jul 12

Change https://go.dev/cl/417070 mentions this issue: `[release-branch.go1.17] go/parser: limit recursion depth`

---

gopherbot pushed a commit that referenced this issue on Jul 12

`[release-branch.go1.18] go/parser: limit recursion depth` ⋯   0d1615b

gopherbot closed this as completed in 695be96 on Jul 12

---

gopherbot pushed a commit that referenced this issue on Jul 12

`[release-branch.go1.17] go/parser: limit recursion depth` ⋯   ba8788e

mknyszek changed the title ~~security: fix CVE-2022-1962~~ go/parser: stack exhaustion in all Parse*

functions on Jul 12

tatianab mentioned this issue on Jul 12

x/vulndb: potential Go vuln in std: CVE-2022-1962 golang/vulndb#515

⊘ Closed

bradfitz pushed a commit to tailscale/go that referenced this issue on Jul 13

`[release-branch.go1.18] go/parser: limit recursion depth` ⋯   d69af72

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

`go/parser: limit recursion depth` ⋯   335c65e

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

`[release-branch.go1.17] go/parser: limit recursion depth` ⋯   36e93c2

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

`[release-branch.go1.17] go/parser: limit recursion depth` ⋯   e6e0769

seankhliao mentioned this issue 28 days ago

x/website: newer examples for security policy PRIVATE issues #56485

⊙ Open

Assignees

No one assigned

Labels

NeedsFix   release-blocker   Security

Projects

▦ **Release Status & Blockers (1.20)**   ⌄

Status: Done   +1 more

Milestone

Go1.19

Development

No branches or pull requests

---

2 participants