

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

panic: runtime error: slice bounds out of range #219

🔒 Closed toptotu opened this issue on Dec 6, 2020 · 10 comments · Fixed by #221

toptotu commented on Dec 6, 2020

```
payload:
func main() {
testJson := {
s, _ := jsonparser.GetString([]byte(testJson), testJson)
fmt.Println(s)
}

panic: runtime error: slice bounds out of range [1:0]

goroutine 1 [running]:
github.com/buger/jsonparser.searchKeys(0x2c050000, 0x1, 0x1, 0xc000d7e78, 0x1, 0x1, 0xc0003a000)
D:/Go/golibsrc/src/github.com/buger/jsonparser/parser.go:311 +0xfdb
github.com/buger/jsonparser.internalGet(0x2c050000, 0x1, 0x1, 0xc000d7e78, 0x1, 0x1, 0xc000d7d38, 0x65e120, 0x56afb0, 0xc000d7dc0, ...)
D:/Go/golibsrc/src/github.com/buger/jsonparser/parser.go:891 +0x3a6
github.com/buger/jsonparser.Get(0x2c050000, 0x1, 0x1, 0xc000d7e78, 0x1, 0x1, 0xc000d7e87, 0x0, 0xc000d7e14, 0xc000d7e87, ...)
D:/Go/golibsrc/src/github.com/buger/jsonparser/parser.go:885 +0x90
github.com/buger/jsonparser.GetString(0x2c050000, 0x1, 0x1, 0xc000d7e78, 0x1, 0x1, 0x9, 0x9, 0x0, 0x0)
D:/Go/golibsrc/src/github.com/buger/jsonparser/parser.go:1122 +0x9e
```

shgsky commented on Dec 15, 2020

@AllenX2018 Any new progress on repairing this issue ?

rathann commented on Dec 16, 2020

FYI, this was assigned [CVE-2020-35381](#).

d-hat commented on Dec 17, 2020 • edited



Contributor

A fix seems to be:

```
diff --git a/parser.go b/parser.go
index 5caeece..dab4574 100644
--- a/parser.go
+++ b/parser.go
@@ -307,7 +307,7 @@ func searchKeys(data []byte, keys ...string) int {
    }
    case '[':
        // If we want to get array element by index
        if keyLevel == level && keys[level][0] == '[' {
+
            if keyLevel == level && keys[level][0] == '[' && len(keys[level]) > 1 {
                aIdx, err := strconv.Atoi(keys[level][1 : len(keys[level])-1])
                if err != nil {
                    return -1
                }
            }
        }
    }
```

👍 1 👁 1

buger commented on Dec 22, 2020

Owner@d-hat can you submit a PR pls?
Thanks!  d-hat mentioned this issue on Dec 22, 2020

Cve 2020 35381 #221

➡ Merged

d-hat commented on Dec 22, 2020


Contributor

Modified slightly to return an error instead of continue trying to index. Please correct any errors or poor style on my part, my golang expertise is approximately nil

eclipseo commented on Jan 8, 2021

Any chance this can get fixed soonish? Thanks.

 buger closed this as completed in #221 on Jan 8, 2021

 **buger** added a commit that referenced this issue on Jan 8, 2021

 Merge pull request [#221](#) from d-hat/[CVE-2020-35381](#) ...

✗ [df3ea76](#)

buger commented on Jan 8, 2021

Owner

Should be fixed now!

satta commented on Jan 8, 2021

Will there also be a new release incorporating this? Thanks!

buger commented on Jan 8, 2021

Owner

Just did v1.1.1 release 🚀

 2  2

satta commented on Jan 8, 2021

Thanks!

 **naveensrinivasan** added a commit to ossf/scorecard that referenced this issue on Sep 21, 2021

  Fix GO-2021-0089 vulnerability ...

✓ [2b4b07d](#)

 **naveensrinivasan** added a commit to ossf/scorecard that referenced this issue on Sep 21, 2021

  Fix GO-2021-0089 vulnerability ...

✓ [51e11e6](#)

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

 [Cve 2020 35381](#)
d-hat/jsonparser

7 participants

