syscall: Faccessat checks wrong group #52313

Closed **neild** opened this issue on Apr 12 · 10 comments

Labels NeedsFix release-blocker Security

Milestone Go1.19

neild commented on Apr 12 Contributor

The `syscall.Faccessat` function checks whether the calling process can access a file.

`Faccessat` contains a bug where it checks a file's group permission bits if the process's user is a member of the *process's* group rather than a member of the *file's* group.

go/src/syscall/syscall_linux.go
Line 112 in `c9fe126`

```
112      if uint32(gid) == st.Gid || isGroupMember(gid) {
```

```
        var fmode uint32
        if uint32(uid) == st.Uid {
                fmode = (st.Mode >> 6) & 7
        } else {
                var gid int
                if flags&_AT_EACCESS != 0 {
                        gid = Getegid()
                } else {
                        gid = Getgid()
                }

                if uint32(gid) == st.Gid || isGroupMember(gid) { // <-- this should be
isGroupMember(st.Gid), not gid
                        fmode = (st.Mode >> 3) & 7
                } else {
                        fmode = st.Mode & 7
                }
        }
```

Since a process's user is usually a member of the process's group, this causes Faccessat to usually check a file's group permissions even if the process's user is not a member of the file's group.

Thanks to **@256dpi** for reporting this.

ianlancetaylor self-assigned this on Apr 12

neild assigned **neild** and unassigned **ianlancetaylor** on Apr 12

neild commented on Apr 12 — Contributor — Author

This bug only occurs on Linux systems, and when `syscall.Faccessat` is called with a non-zero `flags` parameter.

gopherbot commented on Apr 12

Change https://go.dev/cl/399539 mentions this issue: `syscall: check correct group in Faccessat`

gopherbot commented on Apr 12

Change https://go.dev/cl/400074 mentions this issue: `unix: check correct group in Faccessat`

neild commented on Apr 12 — Contributor — Author

`"golang.org/x/sys/unix".Faccessat` suffers from the same problem, but only on Linux kernels < 5.8.

gopherbot pushed a commit to golang/sys that referenced this issue on Apr 12

`unix: check correct group in Faccessat` ... `33da011`

gopherbot pushed a commit that referenced this issue on Apr 12

`syscall: check correct group in Faccessat` ... `f66925e`

seankhliao added the NeedsFix label on Apr 14

neild commented on Apr 19 Contributor Author

@gopherbot please open backport issues.

This was referenced on Apr 19

syscall: Faccessat checks wrong group [1.17 backport] #52439

Closed

syscall: Faccessat checks wrong group [1.18 backport] #52440

Closed

gopherbot commented on Apr 19

Backport issue(s) opened: #52439 (for 1.17), #52440 (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 Apr 19

Change https://go.dev/cl/401078 mentions this issue: `[release-branch.go1.17] syscall: check correct group in Faccessat`

gopherbot commented on Apr 19

Change https://go.dev/cl/401079 mentions this issue: `[release-branch.go1.18] syscall: check correct group in Faccessat`

neild added the Security label on May 4

dmitshur added this to the **Go1.19** milestone on May 4

julieqiu added the release-blocker label on May 5

gopherbot pushed a commit that referenced this issue on May 9

[release-branch.go1.18] syscall: check correct group in Faccessat ··· c0599c5

gopherbot pushed a commit that referenced this issue on May 9

[release-branch.go1.17] syscall: check correct group in Faccessat ··· 04781d1

heschi commented on May 11 — Contributor

This shipped in yesterday's minor releases.

heschi closed this as completed on May 11

---

dmitshur commented on May 11 • edited — Contributor

Fixed for Go 1.19 in CL 399539. (This didn't get closed because its commit message had "For" rather than "Fixes".)

rsc unassigned **neild** on Jun 22

nywilken mentioned this issue on Aug 19

Bump golang.org/x/sys to address CVE-2022-29526 hashicorp/packer#11953

Merged

nywilken added a commit to hashicorp/packer that referenced this issue on Aug 19

Bump golang.org/x/sys to address CVE-2022-29526 ··· ✓ dcddbf1

nywilken added a commit to hashicorp/packer that referenced this issue on Aug 22

Bump golang.org/x/sys to address CVE-2022-29526 (#11953) ··· ✓ ed72488

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

[release-branch.go1.17] syscall: check correct group in Faccessat ··· e13d51d

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

`[release-branch.go1.17] syscall: check correct group in Faccessat` ··· `8d227ed`

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

`[release-branch.go1.17] syscall: check correct group in Faccessat` ··· `24414fb`

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

`[release-branch.go1.17] syscall: check correct group in Faccessat` ··· `a4d1586`

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

`syscall: check correct group in Faccessat` ··· `285b160`

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

`syscall: check correct group in Faccessat` ··· `881b2ab`

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

`syscall: check correct group in Faccessat` ··· `141ef63`

Assignees

No one assigned

Labels

NeedsFix release-blocker Security

Projects

None yet

Milestone

Go1.19

Development

No branches or pull requests

7 participants