

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

# crypto/rand: Read hangs when passed buffer larger than 1<<32 - 1 #52561

Closed

rolandshoemaker opened this issue on Apr 25 · 5 comments

Labels NeedsFix OS-Windows Security

Milestone Go1.19

rolandshoemaker commented on Apr 25 • edited ▾

Member

Passing a buffer larger than  $1 \ll 32 - 1$  to `crypto/rand.Read` hangs on windows due to an infinite loop because of how batching works with `RtlGenRandom`. Since `RtlGenRandom` only supports reading at most  $1 \ll 32 - 1$  bytes at a time, `rngReader` truncates the requested number of bytes to `uint32(len(b))` (or `len(b) % 1 << 32`). After the first call, which will return `len(b) % 1 << 32` bytes, the truncation will always result in 0, causing the infinite loop.

Since this requires such a large buffer, this has minimal impact, since it's incredibly unlikely anyone actually wants this much randomness (and there are no paths from the remotely reachable libraries where this can be realistically triggered.)

This is [CVE-2022-30634](#).

 rolandshoemaker added OS-Windows NeedsFix labels on Apr 25

gopherbot commented on Apr 25

Change <https://go.dev/cl/402257> mentions this issue: `crypto/rand`: properly handle large Read on windows

 gopherbot closed this as completed in [bb1f441](#) on May 5

rolandshoemaker commented on May 16

Member

Author

@gopherbot please open backport issues, this is a minor security issue.

 This was referenced on May 16

**crypto/rand: Read hangs when passed buffer larger than 1<<32 - 1 [1.17 backport] #52932**

 Closed

**crypto/rand: Read hangs when passed buffer larger than 1<<32 - 1 [1.18 backport] #52933**

 Closed

gopherbot commented on May 16

Backport issue(s) opened: [#52932](#) (for 1.17), [#52933](#) (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 May 16

Change <https://go.dev/cl/406635> mentions this issue: [release-branch.go1.17] crypto/rand: properly handle large Read on windows

gopherbot commented on May 16


Change <https://go.dev/cl/406634> mentions this issue: [release-branch.go1.18] crypto/rand: properly handle large Read on windows

 gopherbot pushed a commit that referenced this issue on May 25



[release-branch.go1.18] [release-branch.go1.18] crypto/rand: properly ...

32dedaa


 gopherbot pushed a commit that referenced this issue on May 25



[release-branch.go1.17] crypto/rand: properly handle large Read on wi...

2be03d7

  dmitshur added the `Security` label on May 31

📌  **dmitshur** added this to the **Go1.19** milestone on May 31

#### Assignees

No one assigned

---

#### Labels

**NeedsFix**   **OS-Windows**   *Security*

---

#### Projects

None yet

---

#### Milestone

**Go1.19**

---

#### Development

No branches or pull requests

---

#### 3 participants

