Bug 2060606 (CVE-2022-0850) - CVE-2022-0850 kernel: information leak in copy_page_to_iter() in iov_iter.c

Keywords: Security ×

Status: CLOSED WONTFIX

Alias: CVE-2022-0850

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Red Hat Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks: 2047348

TreeView+ depends on / blocked

Reported: 2022-03-03 20:32 UTC by Rohit Keshri

Modified: 2022-10-19 08:32 UTC (History)

CC List: 49 users (show)

Fixed In Version: kernel 5.14 rc1

Doc Type: If docs needed, set a value

Doc Text:

Clone Of:

Environment:

Last Closed: 2022-03-04 20:49:35 UTC

Attachments	(Terms of Use)
Add an attachment (proposed patch, testcase, etc.)	

Rohit Keshri 2022-03-03 20:32:54 UTC Description

```
There is a kernel information leak vulnerability which was
produced by my improved syzkaller, The output message is as
follows:

Syzkaller hit 'KMSAN: kernel-infoleak in copy_page_to_iter'
bug.

==================================================
BUG: KMSAN: kernel-infoleak in instrument_copy_to_user
build/../include/linux/instrumented.h:121 [inline]
BUG: KMSAN: kernel-infoleak in copyout
build/../lib/iov_iter.c:156 [inline]
BUG: KMSAN: kernel-infoleak in copy_page_to_iter_iovec
build/../lib/iov_iter.c:231 [inline]
```

```
BUG: KMSAN: kernel-infoleak in __copy_page_to_iter
build/../lib/iov_iter.c:855 [inline]
BUG: KMSAN: kernel-infoleak in copy_page_to_iter+0xa65/0x2630
build/../lib/iov_iter.c:883
instrument_copy_to_user
build/../include/linux/instrumented.h:121 [inline]
copyout build/../lib/iov_iter.c:156 [inline]
copy_page_to_iter_iovec build/../lib/iov_iter.c:231 [inline]
__copy_page_to_iter build/../lib/iov_iter.c:855 [inline]
copy_page_to_iter+0xa65/0x2630 build/../lib/iov_iter.c:883
filemap_read+0xf7a/0x1b10 build/../mm/filemap.c:2697
generic_file_read_iter+0x19c/0xa50 build/../mm/filemap.c:2792
ext4_file_read_iter+0xa09/0xd10
call_read_iter build/../include/linux/fs.h:2156 [inline]
new_sync_read build/../fs/read_write.c:400 [inline]
vfs_read+0x1631/0x1980 build/../fs/read_write.c:481
ksys_read+0x28b/0x510 build/../fs/read_write.c:619
__do_sys_read build/../fs/read_write.c:629 [inline]
__se_sys_read build/../fs/read_write.c:627 [inline]
__x64_sys_read+0xdb/0x120 build/../fs/read_write.c:627
do_syscall_x64 build/../arch/x86/entry/common.c:51 [inline]
do_syscall_64+0x54/0xd0 build/../arch/x86/entry/common.c:82
entry_SYSCALL_64_after_hwframe+0x44/0xae
```

Product Security DevOps Team 2022-03-04 20:49:31 UTC Comment 2

This bug is now closed. Further updates for individual products will be reflected on the CVE page(s):

https://access.redhat.com/security/cve/cve-2022-0850

Salvatore Bonaccorso 2022-03-05 15:58:48 UTC Comment 3

Should this CVE be rejected? I'm not sure as the traces do not completely correspond. There is on one hand https://syzkaller.appspot.com/bug?id=602bc454598b9bc1186ea9f927f6225ef64a397b which was auto-closed as invalid, and https://syzkaller.appspot.com/bug?id=78e9ad0e6952a3ca16e8234724b2fa92d041b9b8 which though is fixed 5.14-rc1 (with ce3aba43599f0b50adbebff133df8d08a3d5fffe).

Thanks for clarifying.

Rohit Keshri 2022-03-13 13:23:45 UTC Comment 4

Hello, looking closely at both the traces we will notice they are similar occurrences and relates to a similar problem.

Below is the trace in common

```
~~~
 copy_page_to_iter_iovec lib/iov_iter.c:212 [inline]
 copy_page_to_iter+0x77a/0x1ac0 lib/iov_iter.c:846
 generic_file_buffered_read mm/filemap.c:2185 [inline]
```

```
 generic_file_read_iter+0x3469/0x4430 mm/filemap.c:2362
 blkdev_read_iter+0x20d/0x270 fs/block_dev.c:1936
 call_read_iter include/linux/fs.h:1801 [inline]
 new_sync_read fs/read_write.c:406 [inline]
~~~

thank you.
```

Note

You need to log in before you can comment on or make changes to this bug.
