| | | |
|---|---|---|
| author | Edward Adam Davis <eadavis@qq.com> | 2025-04-04 13:31:29 +0800 |
| committer | Greg Kroah-Hartman <gregkh@linuxfoundation.org> | 2025-05-02 07:44:13 +0200 |
| commit | 63d5a3e207bf315a32c7d16de6c89753a759f95a (patch) | |
| tree | 096e22b203c176b2ab58aaddd83bb66bc9d18dd3 | |
| parent | cd83035b6f2a102c2d5acd3bfb2a11ff967aaba6 (diff) | |
| download | linux-63d5a3e207bf315a32c7d16de6c89753a759f95a.tar.gz | |



## isofs: Prevent the use of too small fid

```
commit 0405d4b63d082861f4eaff9d39c78ee9dc34f845 upstream.

syzbot reported a slab-out-of-bounds Read in isofs_fh_to_parent. [1]

The handle_bytes value passed in by the reproducing program is equal to 12.
In handle_to_path(), only 12 bytes of memory are allocated for the structure
file_handle->f_handle member, which causes an out-of-bounds access when
accessing the member parent_block of the structure isofs_fid in isofs,
because accessing parent_block requires at least 16 bytes of f_handle.
Here, fh_len is used to indirectly confirm that the value of handle_bytes
is greater than 3 before accessing parent_block.

[1]
BUG: KASAN: slab-out-of-bounds in isofs_fh_to_parent+0x1b8/0x210 fs/isofs/export.c:183
Read of size 4 at addr ffff0000cc030d94 by task syz-executor215/6466
CPU: 1 UID: 0 PID: 6466 Comm: syz-executor215 Not tainted 6.14.0-rc7-syzkaller-ga2392f333575 #0
Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 02/12/2025
Call trace:
 show_stack+0x2c/0x3c arch/arm64/kernel/stacktrace.c:466 (C)
 __dump_stack lib/dump_stack.c:94 [inline]
 dump_stack_lvl+0xe4/0x150 lib/dump_stack.c:120
 print_address_description mm/kasan/report.c:408 [inline]
 print_report+0x198/0x550 mm/kasan/report.c:521
 kasan_report+0xd8/0x138 mm/kasan/report.c:634
 __asan_report_load4_noabort+0x20/0x2c mm/kasan/report_generic.c:380
 isofs_fh_to_parent+0x1b8/0x210 fs/isofs/export.c:183
 exportfs_decode_fh_raw+0x2dc/0x608 fs/exportfs/expfs.c:523
 do_handle_to_path+0xa0/0x198 fs/fhandle.c:257
 handle_to_path fs/fhandle.c:385 [inline]
 do_handle_open+0x8cc/0xb8c fs/fhandle.c:403
 __do_sys_open_by_handle_at fs/fhandle.c:443 [inline]
 __se_sys_open_by_handle_at fs/fhandle.c:434 [inline]
 __arm64_sys_open_by_handle_at+0x80/0x94 fs/fhandle.c:434
 __invoke_syscall arch/arm64/kernel/syscall.c:35 [inline]
 invoke_syscall+0x98/0x2b8 arch/arm64/kernel/syscall.c:49
 el0_svc_common+0x130/0x23c arch/arm64/kernel/syscall.c:132
 do_el0_svc+0x48/0x58 arch/arm64/kernel/syscall.c:151
 el0_svc+0x54/0x168 arch/arm64/kernel/entry-common.c:744
 el0t_64_sync_handler+0x84/0x108 arch/arm64/kernel/entry-common.c:762
 el0t_64_sync+0x198/0x19c arch/arm64/kernel/entry.S:600
```

```
Allocated by task 6466:
 kasan_save_stack mm/kasan/common.c:47 [inline]
 kasan_save_track+0x40/0x78 mm/kasan/common.c:68
 kasan_save_alloc_info+0x40/0x50 mm/kasan/generic.c:562
 poison_kmalloc_redzone mm/kasan/common.c:377 [inline]
 __kasan_kmalloc+0xac/0xc4 mm/kasan/common.c:394
 kasan_kmalloc include/linux/kasan.h:260 [inline]
 __do_kmalloc_node mm/slub.c:4294 [inline]
 __kmalloc_noprof+0x32c/0x54c mm/slub.c:4306
 kmalloc_noprof include/linux/slab.h:905 [inline]
 handle_to_path fs/fhandle.c:357 [inline]
 do_handle_open+0x5a4/0xb8c fs/fhandle.c:403
 __do_sys_open_by_handle_at fs/fhandle.c:443 [inline]
 __se_sys_open_by_handle_at fs/fhandle.c:434 [inline]
 __arm64_sys_open_by_handle_at+0x80/0x94 fs/fhandle.c:434
 __invoke_syscall arch/arm64/kernel/syscall.c:35 [inline]
 invoke_syscall+0x98/0x2b8 arch/arm64/kernel/syscall.c:49
 el0_svc_common+0x130/0x23c arch/arm64/kernel/syscall.c:132
 do_el0_svc+0x48/0x58 arch/arm64/kernel/syscall.c:151
 el0_svc+0x54/0x168 arch/arm64/kernel/entry-common.c:744
 el0t_64_sync_handler+0x84/0x108 arch/arm64/kernel/entry-common.c:762
 el0t_64_sync+0x198/0x19c arch/arm64/kernel/entry.S:600

Reported-by: syzbot+4d7cd7dd0ce1aa8d5c65@syzkaller.appspotmail.com
Closes: https://syzkaller.appspot.com/bug?extid=4d7cd7dd0ce1aa8d5c65
Tested-by: syzbot+4d7cd7dd0ce1aa8d5c65@syzkaller.appspotmail.com
CC: stable@vger.kernel.org
Fixes: 1da177e4c3f4 ("Linux-2.6.12-rc2")
Signed-off-by: Edward Adam Davis <eadavis@qq.com>
Signed-off-by: Jan Kara <jack@suse.cz>
Link: https://patch.msgid.link/tencent_9C8CB8A7E7C6C512C7065DC98B6EDF6EC606@qq.com
Signed-off-by: Greg Kroah-Hartman <gregkh@linuxfoundation.org>
```

**Diffstat**

-rw-r--r-- fs/isofs/export.c 2

1 files changed, 1 insertions, 1 deletions

```
diff --git a/fs/isofs/export.c b/fs/isofs/export.c
index 35768a63fb1d23..421d247fae5230 100644
--- a/fs/isofs/export.c
+++ b/fs/isofs/export.c
@@ -180,7 +180,7 @@ static struct dentry *isofs_fh_to_parent(struct super_block *sb,
                return NULL;

        return isofs_export_iget(sb,
-                        fh_len > 2 ? ifid->parent_block : 0,
+                        fh_len > 3 ? ifid->parent_block : 0,
                         ifid->parent_offset,
                         fh_len > 4 ? ifid->parent_generation : 0);
 }
```