author	Theodore Ts'o <tytso@mit.edu>	2023-03-06 13:54:50 -0500
committer	Greg Kroah-Hartman <gregkh@linuxfoundation.org>	2023-03-17 08:48:47 +0100
commit	f8cd8754a03a3748384ee438c572423643c9c315 (patch)	
tree	d1fa872ecfd0ee48ffd399d3df219c15487dd91e	
parent	2ddbd0f967b34872290e0f98fae32b91b4de7b87 (diff)	
download	linux-f8cd8754a03a3748384ee438c572423643c9c315.tar.gz	

diff options

context: 3

space: include

mode: unified

fs: prevent out-of-bounds array speculation when closing a file descriptor

```
commit 609d54441493c99f21c1823dfd66fa7f4c512ff4 upstream.

Google-Bug-Id: 114199369
Signed-off-by: Theodore Ts'o <tytso@mit.edu>
Signed-off-by: Al Viro <viro@zeniv.linux.org.uk>
Signed-off-by: Greg Kroah-Hartman <gregkh@linuxfoundation.org>
```

Diffstat

-rw-r--r-- fs/file.c 1

1 files changed, 1 insertions, 0 deletions

```
diff --git a/fs/file.c b/fs/file.c
index 214364e19d76f4..ee1c350ec58a2c 100644
--- a/fs/file.c
+++ b/fs/file.c
@@ -646,6 +646,7 @@ static struct file *pick_file(struct files_struct *files, unsigned fd)
                file = ERR_PTR(-EINVAL);
                goto out_unlock;
        }
+       fd = array_index_nospec(fd, fdt->max_fds);
        file = fdt->fd[fd];
        if (!file) {
                file = ERR_PTR(-EBADF);
```