author	Theodore Ts'o <tytso@mit.edu>	2023-03-06 13:54:50 -0500
committer	Greg Kroah-Hartman <gregkh@linuxfoundation.org>	2023-03-17 08:57:45 +0100
commit	eea8e4e056a5ffbeb539a13854c017d5d62c756a (patch)	
tree	27697750145217ada89a02de4146530f51439057	
parent	fbe1871b562af6e9cffcf622247e821d1dd16c64 (diff)	
download	linux-eea8e4e056a5ffbeb539a13854c017d5d62c756a.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 c942c89ca4cda9..7893ea161d7707 100644
--- a/fs/file.c
+++ b/fs/file.c
@@ -642,6 +642,7 @@ static struct file *pick_file(struct files_struct *files, unsigned fd)
        if (fd >= fdt->max_fds)
                return NULL;

+       fd = array_index_nospec(fd, fdt->max_fds);
        file = fdt->fd[fd];
        if (file) {
                rcu_assign_pointer(fdt->fd[fd], NULL);
```