



index : kernel/git/stable/linux.git

Linux kernel stable tree

master

switch

Stable Group

[about](#) [summary](#) [refs](#) [log](#) [tree](#) [commit](#) [diff](#) [stats](#)

log msg

search

author Tzung-Bi Shih <tzungbi@kernel.org> 2023-03-24 09:06:58 +0800
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2023-04-05 11:16:38 +0200
commit [13493ad6a220cb3f6f3552a16b4f2753a118b633](#) (patch)
tree [a542d176a632225ddf3ae7a5136e66f58300f4bc](#)
parent [a18fb433ceb56e0787546a9d77056dd0f215e762](#) (diff)
download [linux-13493ad6a220cb3f6f3552a16b4f2753a118b633.tar.gz](#)

diff options

context:
space:
mode:

platform/chrome: cros_ec_chardev: fix kernel data leak from ioctl

[Upstream commit b20cf3f89c56b5f6a38b7f76a8128bf9f291bbd3]

It is possible to peep kernel page's data by providing larger `insize` in struct cros_ec_command[1] when invoking EC host commands.

Fix it by using zeroed memory.

[1]: https://elixir.bootlin.com/linux/v6.2/source/include/linux/platform_data/cros_ec_proto.h#L74

Fixes: [eda2e30c6684](#) ("mfd / platform: cros_ec: Miscellaneous character device to talk with the EC")

Signed-off-by: Tzung-Bi Shih <tzungbi@kernel.org>

Reviewed-by: Guenter Roeck <groeck@chromium.org>

Link: <https://lore.kernel.org/r/20230324010658.1082361-1-tzungbi@kernel.org>

Signed-off-by: Sasha Levin <sasha@kernel.org>

Diffstat

-rw-r--r-- [drivers/platform/chrome/cros_ec_chardev.c](#) 2

1 files changed, 1 insertions, 1 deletions

diff --git a/drivers/platform/chrome/cros_ec_chardev.c b/drivers/platform/chrome/cros_ec_chardev.c
index 1f5f4a46ab748b..4791b62c2923f7 100644

--- a/drivers/platform/chrome/cros_ec_chardev.c

+++ b/drivers/platform/chrome/cros_ec_chardev.c

@@ -285,7 +285,7 @@ static long cros_ec_chardev_ioctl_xcmd(struct cros_ec_dev *ec, void __user *arg)
 u_cmd.insize > EC_MAX_MSG_BYTES)
 return -EINVAL;

- s_cmd = kmalloc(sizeof(*s_cmd) + max(u_cmd.outsize, u_cmd.insize),

+ s_cmd = kzalloc(sizeof(*s_cmd) + max(u_cmd.outsize, u_cmd.insize),
 GFP_KERNEL);

if (!s_cmd)
 return -ENOMEM;