author	Tzung-Bi Shih <tzungbi@kernel.org>	2023-03-24 09:06:58 +0800
committer	Greg Kroah-Hartman <gregkh@linuxfoundation.org>	2023-03-30 12:47:50 +0200
commit	ebea2e16504f40d2c2bac42ad5c5a3de5ce034b4 (patch)	
tree	58f5c288f6cb1a4fa7cf7f721ea54800e3be12d7	
parent	8efae2112d910d8e5166dd0a836791b08721eef1 (diff)	
download	linux-ebea2e16504f40d2c2bac42ad5c5a3de5ce034b4.tar.gz	

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 <sashal@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 0de7c255254e0b..d6de5a29412820 100644
--- a/drivers/platform/chrome/cros_ec_chardev.c
+++ b/drivers/platform/chrome/cros_ec_chardev.c
@@ -284,7 +284,7 @@ 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;
```