MWR LABS

Security Advisory

Huawei Frame Buffer Driver Information Leak

18/07/2017

Software	MediaTek Frame Buffer Driver
Affected Versions	Huawei Y6 Pro Dual SIM (TIT-L01C576B115)
Author	Mateusz Fruba
Severity	Medium
Vendor	Huawei
Vendor Response	Fix Released

Description:

Huawei is a company that provides networking and telecommunications equipment.

The MediaTek frame buffer driver, as shipped with Huawei Y6 Pro, implements an IOCTL interface vulnerable to an information leak due to insufficient input validation.

Impact:

Local processes running in the context of a system application, media server, or system server can leverage this issue for disclosing kernel memory.

Cause:

The MediaTek frame buffer driver fails to validate user-supplied data.

Solution:

This vulnerability was resolved by Huawei in version TIT-L01C576B119. More information can be found on the Huawei web page: http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20170527-01-smartphone-en

Technical details

The MediaTek frame buffer driver implements the ‘mtkfb_ioctl‘ IOCTL handler which receives data passed from user space to the kernel. This driver is implemented in ‘/drivers/misc/mediatek/videox/mt6735/’.

The ‘displayid’ variable is user-controlled and is used as an index into the ‘dispif_info’ array. Firstly, the IOCTL handler function initializes the ‘displayid’ variable by copying the data from user space using ‘copy_from_user’ as shown below:

```
static int mtkfb_ioctl(struct fb_info *info, unsigned int cmd, unsigned long arg)
{
...
	switch (cmd)
	{

		...
	case MTKFB_GET_DISPLAY_IF_INFORMATION:
		{
			int displayid = 0;
			if (copy_from_user(&displayid, (void __user *)arg, sizeof(displayid)))
			{
				MTKFB_LOG("[FB]: copy_from_user failed! line:%d \n", __LINE__);
				return -EFAULT;
			}
```

The ‘displayid’ variable is then verified to be less than ‘MTKFB_MAX_DISPLAY_COUNT’ which is set to 2.

```
…
if (displayid > MTKFB_MAX_DISPLAY_COUNT)
{
	DISPERR("[FB]: invalid display id:%d \n", displayid);
	return -EFAULT;
}
…
```

Finally, the ‘displayid’ variable is used as an index into the ‘dispif_info’ array to retrieve the source address used as a parameter for ‘copy_to_user’, as shown below:

```
if(displayid > MTKFB_MAX_DISPLAY_COUNT)
{
	DISPERR("[FB]: invalid display id:%d \n", displayid);
	return -EFAULT;
}

if (copy_to_user((void __user *)arg, &(dispif_info[displayid]), sizeof(mtk_dispif_info_t)))
{
	MTKFB_LOG("[FB]: copy_to_user failed! line:%d \n", __LINE__);
	r = -EFAULT;
}
```

The ‘displayid’ variable is defined as a signed integer, therefore an attacker could pass a negative value to access memory outside of the ‘dispif_info’ array and bypass the current validation.

Detailed Timeline

Date	Summary
2017-03-28	Issue reported to Huawei.
2017-06-05	Huawei confirmed this issue was fixed in version TIT-L01C576B119.