MWR LABS

Security Advisory

MediaTek Frame Buffer Debugging Interface Memory Disclosure

11/05/2017

Software	MediaTek Frame Buffer Debugging Interface
Affected Versions	MediaTek 6735
Author	Mateusz Fruba
Severity	Medium
Vendor	MediaTek
Vendor Response	Fix Released

Description:

MediaTek is a company that provides system-on-chip solutions for wireless communications, HDTV, DVD and Blu-ray. A number of MediaTek clients including Huawei, and Neffos were found to be affected by a vulnerability in the MediaTek Frame Buffer Debugging Interface code.

The '/d/fbconfig' file was found to leak kernel memory via one of the supported command types (FB_LAYER_GET_INFO) handled by a MediaTek IOCTL interface. In the example described below both stack and heap data were leaked. It is possible that other segments could be leaked as well.

Impact:

The Android Shell user can exploit this vulnerability to leak kernel memory. However, standard Android applications would be limited by SELinux.

Cause:

This vulnerability is due to insufficient input validation of user supplied data.

Solution:

MediaTek clients can receive the security fix directly from the vendor.

Technical details

In the code presented below we can see that user controlled data is copied into a ‘layer_info’ structure using ‘copy_from_user’. The ‘index’ member is then copied into ‘global_layer_id’.

Next the ‘layer_info.index’ variable is used as an array index without any additional validation. The vulnerable code is highlighted in bold:

```
static long fbconfig_ioctl(struct file * file, unsigned int cmd, unsigned long arg)
{
       int ret = 0;
       void __user *argp = (void __user *)arg;
       ...
              switch (cmd)
              {
                     ...
              case FB_LAYER_GET_INFO:
                     {
                            PM_LAYER_INFO layer_info;
                            OVL_BASIC_STRUCT ovl_all[OVL_LAYER_NUM];
                            if (copy_from_user(&layer_info, (void __user*)argp,
sizeof(layer_info)))
                                   ...
                                   global_layer_id = layer_info.index;
                            ovl_get_info(0, ovl_all);
                            layer_info.height = ovl_all[layer_info.index].src_h;
                            layer_info.width = ovl_all[layer_info.index].src_w;
                            layer_info.fmt =
DP_COLOR_BITS_PER_PIXEL(ovl_all[layer_info.index].fmt);
                            layer_info.layer_size = ovl_all[layer_info.index].src_pitch*
ovl_all[layer_info.index].src_h;
                            printk("===>: layer_size:0x%x height:%d \n",
layer_info.layer_size, layer_info.height);
                            printk("===>: width:%d src_pitch:%d \n", layer_info.width,
ovl_all[layer_info.index].src_pitch);
                            printk("===>: layer_id:%d fmt:%d\n", global_layer_id,
layer_info.fmt);
                            printk("===>: layer_en:%d \n",
(ovl_all[layer_info.index].layer_en));
                            …
                                   return copy_to_user(argp, &layer_info,
sizeof(layer_info)) ? -EFAULT : 0;
```

Detailed Timeline

Date	Summary
2016-10-22	Issue reported to MediaTek.
2016-11-16	MediaTek responded with confirmation of the issue.
2016-11-25	MWR queried MediaTek for the issue status and patch release plan.
2017-03-30	MWR queried MediaTek for the issue status and patch release plan.
2017-03-30	MediaTek confirmed that issue was fixed and a patch was available to its customers.