MWR LABS

Security Advisory

MediaTek M4U Driver Arbitrary Memory Overwrite

11/05/2017

Software	MediaTek M4U Driver
Affected Versions	MediaTek 6735
Author	Mateusz Fruba
Severity	High
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 M4U driver code.

The '/proc/m4u' file provides an IOCTL interface which is vulnerable to a one-byte kernel memory overwrite while processing the 'MTK_M4U_T_CONFIG_TF' command.

Impact:

Local attackers can exploit this issue to gain root privileges or achieve kernel mode code execution.

Cause:

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

Solution:

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

Technical details

In the code listed below we can see that the user controlled data is copied into ‘rM4UTF’ and is subsequently passed to the ‘m4u_enable_tf’ function. The ‘m4u_enable_tf’ function has an argument ‘port’ which is controlled by an attacker and it is used as an array index without any validation. The code below demonstrates this:

```
static long MTK_M4U_ioctl(struct file *filp, unsigned int cmd, unsigned long arg)
{
	int ret = 0;
	...
		switch (cmd)
		{
			...
		case MTK_M4U_T_CONFIG_TF:
			{
				M4U_TF_STRUCT rM4UTF;
				ret = copy_from_user(&rM4UTF, (void *)arg,
sizeof(M4U_TF_STRUCT));
				...
					ret = m4u_enable_tf(rM4UTF.port, rM4UTF.fgEnable);
			}
			...
		}

	int m4u_enable_tf(int port, bool fgenable)
	{
		gM4uPort[port].enable_tf = fgenable;
		return 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.