TP-Link, Mercury and FAST Router Vulnerability Report

A lot of TP-Link, Mercury and FAST router have a stack overflow issue in `MntAte` function.

Local users could get remote code execution, this vulnerability currently affects latest WDR series (TP-Link), including WDR5660, WDR7620, WDR7660, WDR7661, etc. We believe there are much more models suffered from this vuln.

Affected Products & Version

TL-WDR7660 2.0.30

Mercury D196G 20200109_2.0.4

Fast FAC1900R 20190827_2.0.2

Vulnerability Description

This vulnerability happen when `MntAte` receive a malicious string by using `recvfrom` from `UDP port 1060`.

1. The malicious input(`a1+23060`) is provided by attackers and the length of malicious input is up to 3072 bytes.
2. The first 6 bytes must be "iwpriv" or "wioctl"
3. And then, the malicious input(`a1+23060`) deliver to `MmtAteParse` and `MntAte` function.
4. `MntAte` will use `spliter` for truncate the input data. But `spliter` is a `strcpy` like function. No length limitation in `spliter`.
5. However, `MntAte` copy these data to a stack buffer without checking the length and lead to a stack buffer overflow to execute arbitrary code.