# Tenda N300 Wireless Router

# Model: F3

# Buffer Overflow Remote Code Execution Vulnerability

Tenda is a manufacturer of routers for home use. The reason for the popularity of their devices is their low price and easy installation. For these reasons, we decided to take a closer look at each of this devices. Unfortunately, it has been proven that cheap devices may not always be the best choice. We have discovered a number of issues with the devices that allow remote code to run on the device or cause the device to crash completely.

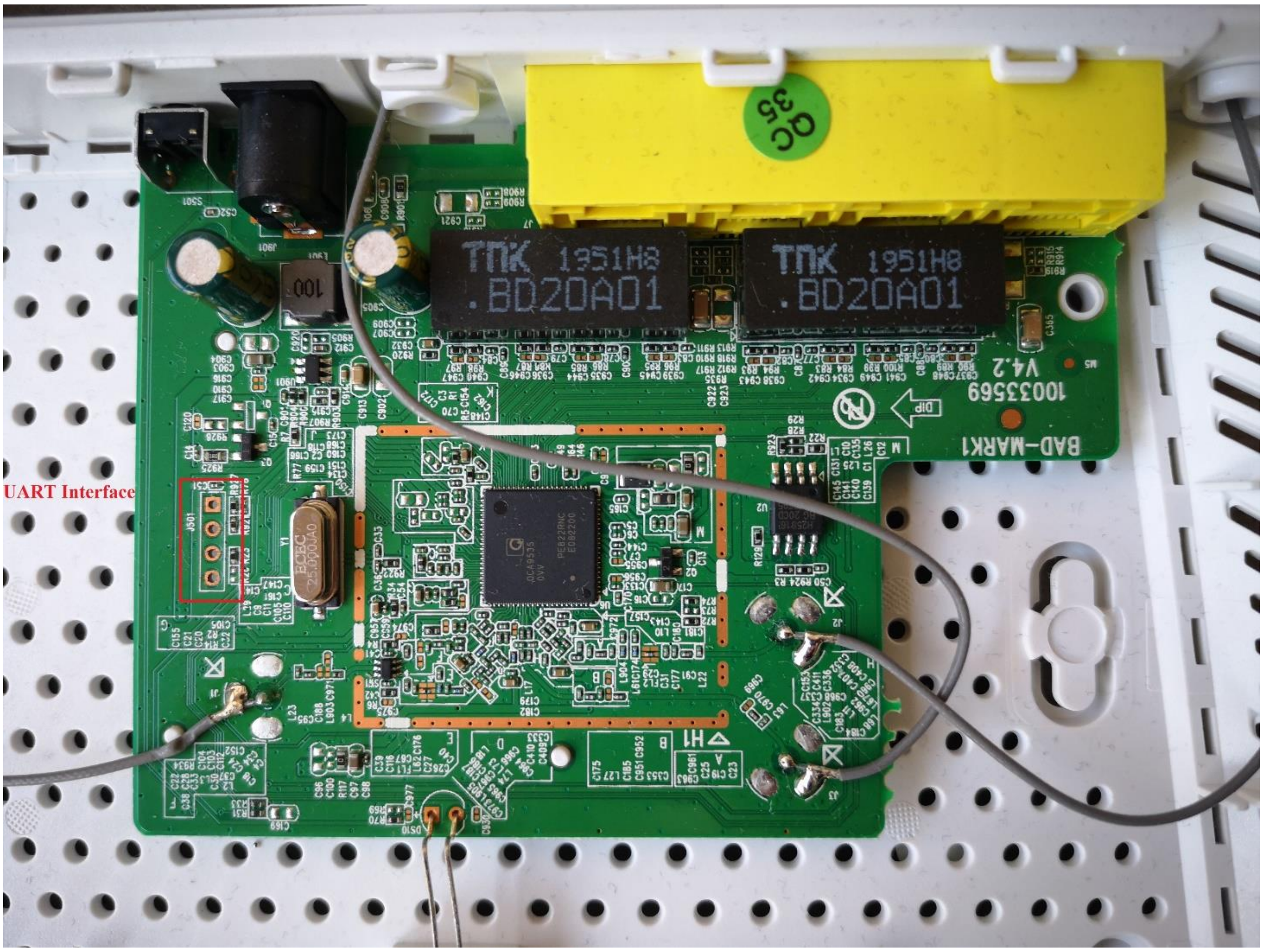
We started testing the device in the usual way, the interface is simple, really easy to install. We started examining the input fields. We wanted to find a classic Overflow error.

At this point, events accelerated, and very soon we were able to find an input field on the interface where the input data caused a problem in the device during processing.

Since we didn’t know exactly what was causing the problem in the device, we just saw that the device was not responding, so we decided to disassemble the device and try to communicate through the UART interface with the device, to find out what happened during the data processing.

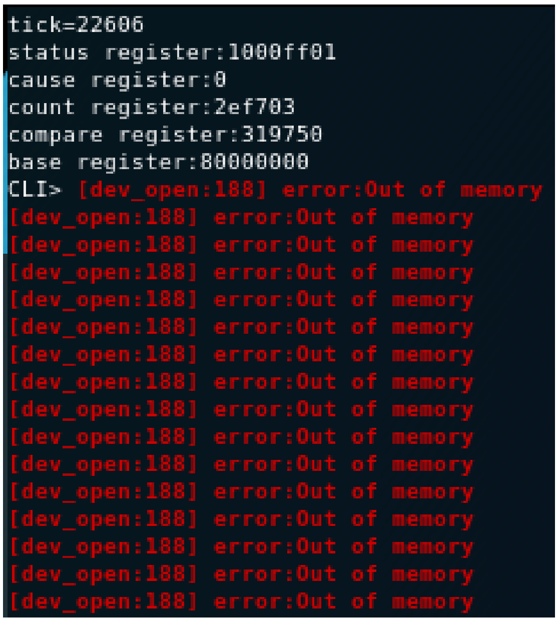
What is the UART?

Universal Asynchronous Receiver-Transmitter (UART) is a hardware serial communication bus used by most processors and chips. this a very common type of debug serial communication protocol that can be used to obtain low-level access to a devices.



After successfully connecting to the device through the interface and we have a limited shell access to the device, we resent the request that caused the error and monitored the error messages on the device.

Device error messages are very eloquent, this is an buffer overflow error and the error is caused by the copyHostname2TendaArp function.



```
tick=22606
status register:1000ff01
cause register:0
count register:2ef703
compare register:319750
base register:80000000
CLI> [dev_open:188] error:Out of memory
[dev_open:188] error:Out of memory
[dev_open:188] error:Out of memory
[dev_open:188] error:Out of memory
[dev_open:188] error:Out of memory
[dev_open:188] error:Out of memory
[dev_open:188] error:Out of memory
[dev_open:188] error:Out of memory
[dev_open:188] error:Out of memory
[dev_open:188] error:Out of memory
[dev_open:188] error:Out of memory
[dev_open:188] error:Out of memory
[dev_open:188] error:Out of memory
[dev_open:188] error:Out of memory
[dev_open:188] error:Out of memory
```

The Proof of Concept codes that cause the error can be found in the Quadron Research Lab's github repository.