CVE-2015-3036

Background

This is a case of classic stack buffer overflow. The code is developed by Taiwanese company KCode. Basically their service provides a “USB over IP” utility that is used by a handful of companies. Some of the companies include big names like TP-Link and NetgearIt is a Linux kernel driver that launches a TCP server. This simulates the USB device plugged into the embedded Linux device that the client (user) can use via the network.

Vulnerability

When a client (user) connects to the TCP server, a name for the computer needs to be sent to the server. On the TCP server, this computer name is stored in a 64 byte array. The name is copied over without any bounds checking. This means that if the client were to supply a computer name that is longer than 64 characters, the data on the stack can be overwritten.

Fix

Literally any of the buffer overflow prevention mentioned in the Wikipedia article would have prevented this bug. A simple bounds check would suffice to prevent such easy access to the stack.