## TOTOLINK路由器N200RE存在密钥硬编码泄露漏洞

## 资产证明

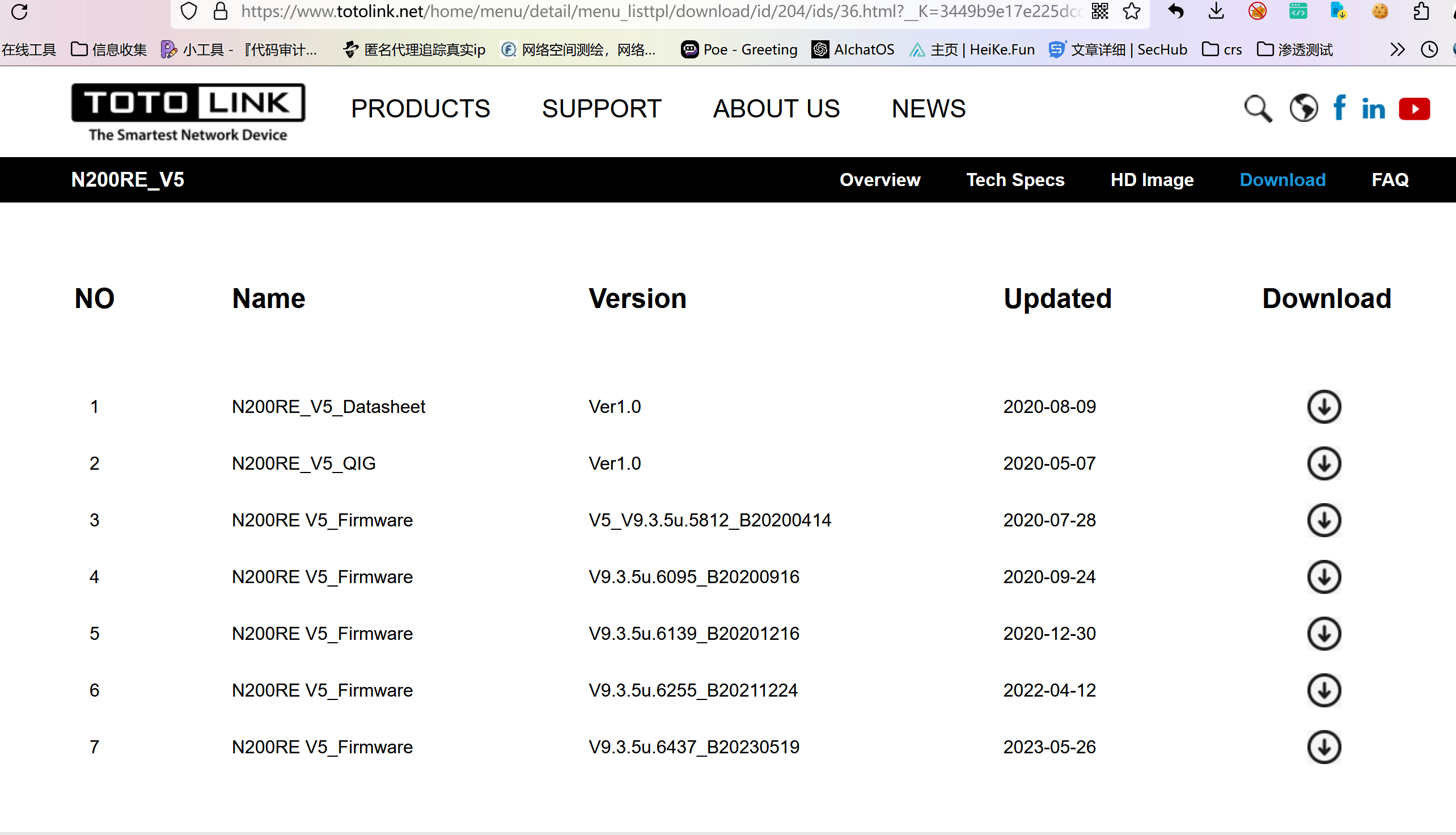
截图如下：



# 固件获取

https://www.totolink.net/home/menu/detail/menu\_listtpl/download/id/204/ids/36.html

V9.3.5u.6095\_B20200916版本的固件



## 漏洞证明与分析

截图如下：

binwalk --run-as=root -Me TOTOLINK\_C8352R\_N200RE\_IP04424\_MT7628NN\_SPI\_4M32M\_V9.3.5u.6095\_B20200916\_ALL.web --preserve-symlinks

使用WSL以及QEMU里的MIPSel将环境配置好，使用命令分离出固件文件

使用grep -r "TelnetKey" . 发现其远程链接密钥泄露了：

