PTA Cert

Security Advisory-No: 012

02 , July 2018

Threat Classification: Malware (botnet)

Name: VPNFilter

Target: Range of SOHO and enterprise routers and network attached storage (NAS) devices.

Affected Devices:

- Linksys model: ***(E1200,E2500,E3000,E3200,E4200,RV082,WRVS4400N)***
- TP-Link model: ***(TL-WR741ND,TL-WR841N,R600VPN)***
- DLink model: ***(DES-1210-08P,DIR-300,DIR-300A,DSR-250N,DSR-500N,DSR-1000,DSR-1000N)***
- ZTE Devices: ***(ZXHN H108N)***
- Ubiquiti model : ***(NSM2,PBE M5)***
- Asus model: ***(RT-AC66U,RT-N10,RT-N10E,RT-N10U,RT-N56U,RT-N66U)***
- Huawei model: ***(HG8245)***
- QNAP Network-Attached Storage Device model: ***(TS251, TS439 Pro)***
- MikroTik RouterOS Versions for Cloud Core Routers: ***(CCR1009,CCR1016,CCR1036,CCR1072,CRS109,CRS112,CRS125,RB411,RB450,RB750, RB911,RB921,RB941,RB951,RB952,RB960,RB962,RB1100,RB1200,RB2011,RB3011,RB Groove,RB Omnitik,STX5)***
- NETGEAR model: ***(DG834,DGN1000,DGN2200,DGN3500,FVS318N,MBRN3000,R6400,R7000,R8000,WNR1000,WNR2000,WNR2200,WNR4000,WNDR3700,WNDR4000,WNDR4300,WNDR4300-TN,UTM50)***

Impact:

Malware is capable to scan the traffic passing through affected device, to perform attack (man-in-the-middle) on the traffic passing through the effected devices. The malware is also capable to execute self-destructive commands to destroy the affected network devices and SCADA based equipment.

Possible attacks on infected devices may include, but are not limited to the following:

- Packet sniffer for spying on traffic that is routed through the device
- It maintain a persistent presence even after rebooting of affected device
- Can monitoring the Modbus protocols for SCADA based devices
- Malware can tamper of web traffic through man-in-the-middle attacks
- It can convert HTTPS requests into ordinary HTTP requests to read encrypted information
- Malware is Capable to destroy affected network devices by overwriting of own written firmware
- Capable to remove all traces of Malware activity before rendering the device
- Capable to contact a command and control (C&C) server to download further scripting based attacks

Recommendations:

1) Perform a factory reset, reboot and patch their devices with the latest respective firmware/software version
2) Upgrade Device firmware to defend against aforementioned malware
   - **https://www.linksys.com/cz/support-article?articleNum=132961**
   - **https://www.tp-link.com/us/faq-2212.html**
   - **https://forum.mikrotik.com/viewtopic.php?f=21&t=134776**
   - **https://kb.netgear.com/23442/How-do-I-update-my-NETGEAR-router-firmware-using-the-Check-button-in-the-router-s-web-interface**
   - **https://www.qnap.com/en/security-advisory/nas-201805-24**
3) Install any latest/updated Malware Remover, and then run a full scan for NAS device
4) Change default passwords of network device and set complex login password.
5) Enable firewall filters and apply ACL filters for trusted network
6) Turn off the remote administrative access feature on the device if not used