VPNFilter-affected Devices Still Riddled with 19 Bugs

blog.trendmicro.com/trendlabs-security-intelligence/vpnfilter-affected-devices-still-riddled-with-19-vulnerabilities

July 13, 2018

Our IoT scanning tool allows users to identify if connected devices (e.g. routers, network attached storage devices, IP cameras, and printers) in a given network are vulnerable to security risks and vulnerabilities, such as those related to Mirai, Reaper, and WannaCry.

We gather our data from the Trend Micro™ Home Network Security solution and HouseCall™ for Home Networks scanner. HouseCall for Home Networks is a free tool that features device recognition and vulnerability scanning in users' networks and connected devices. Home Network Security is a solution plugged into users' routers that protects connected devices from potential cyberattacks. Our scanning can cover multiple operating systems, including Linux, Mac, Windows, Android, iOS, and other software development kit (SDK) platforms.

This blog tackles the recently ill-famed VPNFilter malware and if deployed devices are vulnerable to it and other vulnerabilities. VPNFilter is a newly discovered, multi-stage malware (detected by Trend Micro as ELF_VPNFILT.A, ELF_VPNFILT.B, ELF_VPNFILT.C, and ELF_VPNFILT.D) that affects many models of connected devices. Initially reported at the tail end of May to have infected at least 500,000 networking devices across 54 countries, including those from Linksys, MikroTik, Netgear, and TP-Link, to steal website credentials and even render devices unusable, the malware is now seen targeting more devices to

deliver exploits and even override reboots. The Federal Bureau of Investigation (FBI) has even released a public service announcement (PSA), warning that it is the work of foreign threat actors looking to compromise networked devices worldwide.

Different brands and models affected by VPNFilter and more

VPNFilter is known to affect over ten brands and 70 models of devices. Our IoT scanning tool can identify other publicly known vulnerabilities targeting the devices as listed below:

Manufacturer	Model	Device Type
Asus	RT-AC66U, RT-N10, RT-N10E, RT-N10U, RT-N56U, and RT-N66U	Routers
D-Link	DES-1210-08P DIR-300, DIR-300A, DSR-250N, DSR-500N, DSR-1000, and DSR-1000N	Ethernet switch Routers
Huawei	HG8245	Router
Linksys	E1200, E2500, E3000 E3200, E4200, RV082, and WRVS4400N	Routers
MikroTik	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, and STX5	Routers
Netgear	DG834, DGN1000, DGN2200, DGN3500, FVS318N, MBRN3000, R6400, R7000, R8000, WNR1000, WNR2000, WNR2200, WNR4000, WNDR3700, WNDR4000, WNDR4300, WNDR4300-TN, and UTM50	Routers
QNAP	TS251, TS439 Pro, and other QNAP NAS devices running QTS software	NAS devices
TP-Link	R600VPN, TL-WR741ND, and TL-WR841N	Routers
Ubiquiti	NSM2 and PBE M5	Wireless access points
ZTE	ZXHN H108N	Router

Table 1. Some of the known affected devices by VPNFilter

Based on our data from June 1 to July 12, plenty of the devices are still using old firmware versions. In fact, 19 known vulnerabilities, not only taken advantage of by VPNFilter but other malware as well, can still be detected in devices up to this day.

At the time of our scanning, we observed that 34 percent of home networks had at least one device with a known vulnerability. We found that 9 percent of vulnerable devices are potentially affected by VPNFilter.

Device Vulnerabilities	Vulnerable Devices/Services
Authentication Bypass Vulnerability CVE-2015-7261	QNAP FTP Service
Reaper Remote Code Execution CVE-2011-4723	D-Link DIR-300
Remote Code Execution CVE-2014-9583	ASUS RT-AC66U, RT-N66U
Reaper OS Command Injection CVE-2013-2678	Linksys E2500
Buffer Overflow Vulnerability CVE-2013-0229	Vulnerable UPnP Service (e.g. Netgear/TP-Link/D-Link)
Stack Overflow Vulnerability CVE-2013-0230	Vulnerable UPnP Service (e.g. Netgear/TP-Link/D-Link)
Remote Code Execution CVE-2017-6361	QNAP QTS before 4.2.4 Build 20170313
Router JSONP Info Leak CVE-2017-8877	ASUS RT-AC* and RT-N*
Router Password Disclosure CVE-2017-5521	Netgear R6400, R7000, R8000
Stack Overflow Vulnerability CVE-2012-5958	Vulnerable UPnP Service (e.g. Netgear/TP-Link/D-Link)
Stack Overflow Vulnerability CVE-2012-5959	Vulnerable UPnP Service (e.g. Netgear/TP-Link/D-Link)
Reaper Router Remote Code Execution	D-Link DIR-300
Router Password Disclosure	Netgear WNR2000
Remote Code Execution CVE-2016-6277	Netgear R6400, R7000
Router Session Stealing CVE-2017-6549	ASUS RT-N66U
OS Command Injection CVE-2013-2679	Linksys E4200
Authentication Bypass Vulnerability	Netgear WNR1000
Router Password Disclosure	Netgear WNR1000
Unauthenticated Router Access Vulnerability	TP-Link TL-WR841N

Table 2. 19 vulnerability detections on VPNFilter-affected devices

As expected, the 19 vulnerabilities primarily affect routers. Interestingly, the Authentication Bypass Vulnerability CVE-2015-7261, an FTP (File Transfer Protocol) flaw in the QNAP NAS firmware, mostly affects printers based on our detection. While determining the possible reason behind this, we found that many of the detected printers' FTP could connect to the network without any authentication. In some cases, this may be the printer's default configuration, but it still poses a potential security risk if the FTP is set as open on the internet.


Figure 1. A Shodan result of an FTP connection to a printer without authentication

Figure 1. A Shodan result of an FTP connection to a printer without authentication

The other vulnerabilities detected, such as the Buffer Overflow CVE-2013-0229 and Stack Overflow CVE-2013-0230, can allow attackers to cause a denial-of-service (DoS) and execute arbitrary code in systems, respectively. Vulnerable UPnP Services detected, moreover, aren't exclusively associated with Netgear/TP-Link/D-Link devices, as other brands could also have the same vulnerability. In that case, we can expect more detections.

Protecting devices and networks against VPNFilter malware and other vulnerabilities

The threat of VPNFilter malware is augmented by the fact that other publicly known vulnerabilities were detected in the affected devices. Since not all device manufacturers provide immediate fixes for discovered vulnerabilities and not all users regularly apply patches, users should first secure the way they set up their devices and networks. Trend Micro™ Home Network Security solution can check internet traffic between the router and all connected devices. Our IoT scanning tool has been integrated into the Home Network Security solution and HouseCall™ for Home Networks scanner. Enterprises can also monitor all ports and network protocols for advanced threats and thwart targeted attacks with the Trend Micro™ Deep Discovery™ Inspector network appliance.

Aside from adopting security solutions that can protect networks and connected devices from the vulnerabilities through the identification and assessment of potential risks, we recommend standard security measures, such as:

- Updating the firmware versions of devices once they're available to avoid attacks that exploit known vulnerabilities.
- Avoiding the use of public Wi-Fi on devices that are also used in home or corporate networks.
- Changing device's default credentials and using strong passwords to deter unauthorized access.
- Being wary of suspicious URLs or attachments from unknown sources that may lead to infecting devices connected to the network.

Users of the Trend Micro Home Network Security solution are also protected from particular vulnerabilities via these rules:

- 1058981 WEB Directory Traversal -21
- 1130327 EXPLOIT ASUSWRT 3.0.0.4.376_1071 LAN Backdoor Command Execution (CVE-2014-9583)