Appendix A: Vendor Devices Exploited by Mirai-Variant Botnet

Below is a list of vendor device vulnerabilities exploited by the Mirai-variant IoT botnet targeting the financial sector in January 2018. A column depicting Checkpoint's observations of the IoTroop botnet as well as a listing of whether the same vendor devices were seen in the original Mirai botnet have been included for reference.

Vendor	Details	CVE #	Date Published (cvedetails.com)	Vendor devices observed by Recorded Future in Mirai-variant IoT botnet attacks in January 2018	Vendor devices noted in Checkpoint research on IoTroop botnet activity in October 2017	Vendor devices noted as being vulnerable to original Mirai malware
AVTECH	AVTECH Devices Multiple vulnerabilities	CVE-2013-4981 CVE-2013-4980	3-Mar-14	Yes	Yes	No
Dahua Technology Co.	Use of password hash instead of password for authentication, cwe-836, Dahua DVR	CVE-2017-7927	5-May-17	Yes	No	Yes
	Password in configuration file, cwe-260, Dahua DVR	CVE-2017-7925	5-May-17	Yes	No	Yes
GoAhead	Wireless IP Camera (P2P) WIFICAM Cameras Information Disclosure	CVE-2017-8225	25-Apr-17	Yes	Yes	Yes
	Wireless IP Camera (P2P) WIFICAM Cameras Remote Code Execution	CVE-2017-8224	25-Apr-17	Yes	Yes	Yes
Linksys	Linksys WRH54G HTTP Management Interface DoS Code Execution – Ver2	CVE-2008-2636	9-Jun-08	Yes	No	No
	Belkin Linksys WRT110 Remote Command Execution – Ver2	CVE-2013-3568	23-Sep-13	Yes	No	No
	Cisco Linksys PlayerPT ActiveX Control Buffer Overflow	CVE-2012-0284	19-Jul-12	Yes	No	No

MikroTik	MikroTik RouterOS SNMP Security Bypass	CVE-2008-6976	19-Aug-09	Yes	No	No
	MikroTik RouterOS Admin Password Change	CVE-2015-2350	19-Mar-15	Yes	No	No
	Mikrotik Router Remote Denial Of Service	CVE-2012-6050	26-Nov-12	Yes	No	No
Samsung	Samsung UE55D7000 TV http config	Unknown	Unknown	Yes	No	No
Synology	Synology DiskStation Manager SLICEUPLOAD Code Execution	CVE-2013-6955	9-Jan-14	Yes	No	No
TP-Link	TP-Link Wireless Lite N Access Point Directory Traversal	CVE-2012-5687	1-Nov-12	Yes	No	No
	TP-LINK WR1043N Multiple Cross-Site Request Forgery	CVE-2013-2645	5-Oct-14	Yes	No	No
Ubiquity	Airgrid m5 hp series, 5ghz, 27dbi grid antenna with integrated radio by Ubiquiti networks	Unknown	Unknown	Yes	No	Yes
	Ubiquiti EdgeRouter Lite Router - Gigabit	Unknown	Unknown	Yes	No	Yes
	Ubiquiti EdgeRouter Router - 1 Gbps - Gigabit	Unknown	Unknown	Yes	No	Yes
	Ubiquiti EdgeRouter X SFP Router - 5-port - Gigabit	Unknown	Unknown	Yes	No	Yes