IoTSecure™

Internet of Things (IoT)

Threat Check Report

September 10, 2021

S/N: CF2A0B31914C

Contact: Jeff@IoTSecure.io

Powered by IoTSecure™

iotsecure.io

2180 Satellite Blvd., Ste 400 | Duluth, GA 30097 | +1 (770) 224-7961

Executive Overview

The IoT Problem

30-billion IoT devices are connected around the world. They are finding ways into every network, including yours. Most are unmanaged and unpatched. Are you ready to detect, monitor and control IoT devices when they invade your network?

#1: IoT VISIBILITY

You cannot secure and segment devices that you don't know exist. Traditional tools can identify a device's IP, MAC and hostname, but they lack capabilities to provide device detail like true manufacturer, type, category or model, especially on unmanaged and IoT devices that cannot run agents. This adds manual work to segmentation and remediation.

#2: IoT VULNERABILITY

Vulnerability scanners crash IoT devices. They are too intrusive to run on resource constrained IoT devices and they cannot scan in real time. This result in untested and potentially vulnerable devices connected to your network.

#3: IoT MONITORING

Analyzing IoT traffic is useless without an IoT database. IoT devices don't support agents for monitoring, which mean you either ignore unmanged devices or try to build and maintain your database of IoT security rules.

#4: IoT CONTROL

You cannot patch or upgrade most IoT devices. IoT devices commonly open up vulnerable services by default or come with vulnerabilities straight from the manufacturer with limited or no patching.

The IoTSecure Solution

In under 48-hours the IoTSecure IoT-mini™ will find every device on your network and every known vulnerability. No agents. No configuration. The IoT-mini™ is fully automated.

3-Step Assessment

You Requested A Free IoT-mini™

You Connected it to Your Network

You Received this IoT Threat Report

Your Environment

This assessment was performed on the following network:

Network: 10.0.0.0/8

It took approximately 24 hours to collect and process all necessary data. Customer data stored in the IoT Secure CloudPortal® is fully encrypted. Below is a detailed configuration of your IoT-mini™ used for this assessment.

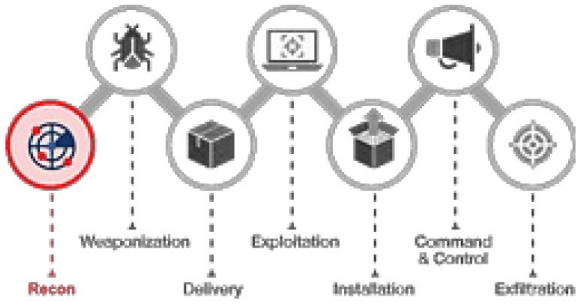
```
S/N:        CF2A0B31914C
Model:      IoTSA-MINI
CPU:        MIPS
Interface:  ether1
MAC:        70:B3:D5:12:53:27
Hostname:   CF2A0B31914C-IoTSA-MINI
DHCP:       Enabled
IP Addr.:   10.0.0.42
Gateway:    10.0.0.1
```

Connection Details

Location-Based Threats

Your public IP address, which often reveals your physical location, can easily be identified and used to target your network with malware "designed" for your region, industry or organization. Attackers leverage your local language, local events and local government regulations to create and deliver highly-targeted attacks.

The Cyber Kill Chain - Phase 1: **Reconnaissance**



Another common attack is perpetrated by utilizing just the IP address or addresses of systems owned or maintained by the target organization. With one or more IP addresses, malicious actors can determine precisely which IP addresses or blocks belong to the organization. Once a list of target IP ranges is discovered, malicious actors no longer need to find ways into more publicly known systems; they can instead look for the most vulnerable to use as their entry point into the network.

Your Connection

Your IoT-mini™ is connected to the Internet with the public IP address listed below. IoTSecure used this IP address to obtain publicly available Location and Provider information.

Public IP:	*24.4.63.241*
Continent:	*North America*
Country:	*United States*
State/Province:	*California*
City:	*Sacramento*
Internet Provider:	*Comcast Cable Comm.*
Connection Type:	*Business*
Organization:	*Comcast Cable Comm.*

IoT Asset Discovery Detail

#1 Critical Security Control

Inventory and Control of Hardware Assets

The Center for Internet Security (CIS) Top 20 Critical Security Controls are a prioritized list of highly effective best practices created to stop the most pervasive and dangerous cyber threats of today. 85% of attacks can be prevented by adopting just the first 5 controls, according to Verizon's DBIR.

- #1 Inventory and Control of Hardware Assets
- #2 Inventory and Control of Software Assets
- #3 Continuous Vulnerability Management
- #4 Controlled Use of Administrative Privileges
- #5 Secure Configuration for Hardware and Software

The IoTSecure IoT-mini™ can be used to implement Critical Security Controls #1 and #3.

#1 Inventory and Control of Hardware Assets

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

#3 Continuous Vulnerability Management

Continuously acquire, assess, and act upon information to identify vulnerabilities, remediate, and minimize opportunity for attackers.

- Download CIS Controls
- Download Verizon DIBR

- Upgrade Your IoT-mini™

IoTSecure Asset Discovery
IoTSecure gives you complete, real-time visibility of every device (managed and unmanaged) connected to your network; without installing an agent.
Your Results
Your IoT-mini™ automatically discovered, identified and classified the following devices on your network.

Total Devices	20
Managed	0
Unmanaged	20
At Risk	9
Unique Device Types[1]	17
Unique Manufacturers[2]	19
Unique Operating Systems[3]	10

[1] IoTSecure can identify 500+ categories of IoT and connected devices.

[2] IoTSecure can identify devices from 20,000+ manufacturers.

[3] IoTSecure can identify 250+ operating systems including version, build and patch level.

IoT Asset Vulnerability Overview

IP Address	MAC Address	Name	Type[4]	Manufacturer	Operating System
10.1.200.201 ⚠	00:1A:FA:01:F5:C2	Connex Vital Signs Monitor	Patient Monitor	Welch Allyn	Windows
10.2.100.101	28:24:FF:97:10:AD	Talis-Hub	Medical Device Hub	Talis Clinical	Linux
10.10.0.223 ⚠	00:07:4D:9B:8B:1D	Thermal Label Printer GX420t	Barcode Printer	Zebra	Embedded
10.10.0.201	44:4B:5D:97:F5:99	GE Health Discovery VCT PET/CT Scanner	PET/CT Scanner	GE Health	Windows
10.0.22.222	F9:EB:13:DC:CC:54	Hologic Dimensions 3D Mammography Scanner	Mammogram Scanner	Hologic	Windows
10.10.1.55 ⚠	00:12:21:9B:8B:1D	B. Braun SpaceStation	Infusion Pump	B. Braun	Linux
10.10.1.101 ⚠	00:08:00:71:1A:02	FaxFinder FF840 Fax Server	Fax	MultiTech	Linux
10.10.1.112	00:09:0F:09:00:14	FortiGuard Security Device	Firewall	Fortinet	Linux
10.10.2.3 ⚠	00:1B:17:17:9E:00	Palo Alto Networks Firewall	Firewall	Palo Alto Networks	PAN-OS
10.0.22.100	00:40:58:15:26:74	Time System	Time Clock	Kronos	Embedded
10.1.200.21 ⚠	00:C0:B7:DF:8E:77	APC Power Device	Power Management	APC	Embedded
10.10.0.201 ⚠	30:F7:72:34:B6:10	Color MFC-9130CW	Color Multifunction	Brother	Embedded
10.0.44.32	44:61:32:39:80:55	Ecobee Thermostat	HVAC Controller	Ecobee	Linux
10.10.1.201	A0:04:60:38:F4:D5	Arlo Pro Security Base Station	IP Camera	Netgear	Embedded
10.0.22.212 ⚠	D4:AE:52:76:B6:B5	Poweredge idRAC	Server	Dell	Linux
10.0.22.99 ⚠	EC:1A:59:EF:94:E1	Wemo Smart Home Device	Building Automation	Belkin	Linux
10.0.22.112	08:F1:EA:91:12:C0	ProLiant iLO	Server	Hewlett Packard	Embedded
10.1.200.98	10:DD:B1:BE:D5:C2	MacBook Pro	Laptop	Apple	Mac OS X
10.10.1.43	18:F6:43:53:3E:DE	iPhone	Mobile Phone	Apple	iOS
10.3.44.43	2C:B8:ED:02:16:99	SonicWALL	Firewall	SonicWALL	SonicOS

⚠ A vulnerability was detected. More information is available in the IoT Vulnerability Detail section.

[4] Forwarding DHCP and DNS logs to the IoT-mini™ can significantly improve device profiling accuracy. Log forwarding requires a paid IoT Secure subscription. (see below)

Threat Category	Vulnerability[5]	Severity	Count	Devices Affected
Ransomware	Eternal Blue	High	-	
Device Takeover	Default Credential	High	4	Thermal Printer, APC Power Device, Color MFC, PowerEdge iDRAC
	Remote Code Execution	High	-	-
	RDP Denial of Service	High	-	-
	Unauthenticated Access	High	1	B. Braun SpaceStation
	HTTP Shellshock	High	-	-
Sensitive Data Leak	Public Video Feed	High	-	-
	SSL/TLS Vulnerabilities	Medium	3	FaxFinder, Palo Alto FW, Connex Vital Signs Monitor
	Unsecure Document Access	Low	-	-
Security Gap	Unprotected DNS Server	Medium	1	WeMo Smarthome Device

[5] Only a partial list of IoT Secure threat categories and vulnerabilities are displayed.

IoT Asset Vulnerability Detail

Incident #: 548042 **Severity: Medium** **Thermal Label Printer GX420t** IP: 10.10.0.223 MAC: 00:07:4D:9B:8B:1D	========== SUMMARY: ========== * Port 21 is subject to exploit by Default Passwords on device 00:07:4D:9B:8B:1D MAC Address: 00:07:4D:9B:8B:1D Device: zbr10193693.eps.local Manufacturer: Zebra Model: Label Printer IP Address: 10.10.0.223 Network Name: 10.0.0.0/8 ========== RECOMMENDED ACTIONS: ========== * Change device configuration to remove the vulnerability. If unable to do so, remove the device from the network.

IoT Asset Vulnerability Detail

Incident #: 551399 **Severity: Low** **FaxFinder FF840 Fax Server** IP: 10.10.1.101 MAC: 00:08:00:71:1A:02	========== SUMMARY: ========== * Port 443 is subject to exploit by SSL POODLE on device 00:08:00:71:1A:02 * IDs: CVE:CVE-2014-3566 OSVDB:113251. The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the POODLE issue. MAC Address: 00:08:00:71:1A:02 Device: faxfinder.co.bingham.id.us Manufacturer: MultiTech Model: Multitech Systems Device IP Address: 10.10.1.101 Network Name: 10.0.0.0/8 ======== DETAILS: ======== * https://www.imperialviolet.org/2014/10/14/poodle.html * http://osvdb.org/113251 * http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566 * https://www.openssl.org/~bodo/ssl-poodle.pdf ========== RECOMMENDED ACTIONS: ========== * Change device configuration to remove the vulnerability. If unable to do so, remove the device from the network

IoT Asset Vulnerability Detail

Incident #: 551401 **Severity: Low** **FaxFinder FF840 Fax Server** IP: 10.10.1.101 MAC: 00:08:00:71:1A:02	========== SUMMARY: ========== *Port 443 is subject to exploit by SSL Weak Diffie-Hellman Key Exchange on device 00:08:00:71:1A:02 *Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam) *The Transport Layer Security (TLS) protocol contains a flaw that is triggered when handling Diffie-Hellman key exchanges defined with the DHE_EXPORT cipher. his may allow a man-in-the-middle attacker to downgrade the security of a TLS session to 512-bit export-grade cryptography, which is significantly weaker, allowing the attacker to more easily break the encryption and monitor or tamper with the encrypted stream. *Diffie-Hellman Key Exchange Insufficient Diffie-Hellman Group Strength *Transport Layer Security (TLS) services that use Diffie-Hellman groups of insuffficient strength, especially those using one of a few commonly shared groups, may be susceptible to passive eavesdropping attacks. *Diffie-Hellman Key Exchange Potentially Unsafe Group Parameters This TLS service appears to be using a modulus that is not a safe prime and does not correspond to any well-known DSA group for Diffie-Hellman key exchange. MAC Address: 00:08:00:71:1A:02 Device: faxfinder.co.bingham.id.us Manufacturer: MultiTech Model: Generic Multitech Systems Device IP Address: 10.10.1.101 Network Name: 10.0.0.0/8 Further Information: https://weakdh.org ========== RECOMMENDED ACTIONS: ========== * Change device configuration to remove the vulnerability. If unable to do so, remove the device from the network.

IoT Asset Vulnerability Detail

Incident #: 549210 **Severity: Low** **Palo Alto Networks Firewall** IP: 10.10.2.3 MAC: 00:1B:17:17:9E:00	========== SUMMARY: ========== * Port 443 is subject to exploit by SSL POODLE on device 00:1B:17:17:9E:00 * IDs: CVE:CVE-2014-3566 OSVDB:113251. The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the POODLE issue. MAC Address: 00:1B:17:17:9E:00 Device: Palo Alto Networks Firewall Manufacturer: Palo Alto Networks Model: Palo Alto Networks Firewall IP Address: 10.10.2.3 Network Name: 10.0.0.0/8 ======== DETAILS: ======== * https://www.imperialviolet.org/2014/10/14/poodle.html * http://osvdb.org/113251 * http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566 * https://www.openssl.org/~bodo/ssl-poodle.pdf ========== RECOMMENDED ACTIONS: ========== * Change device configuration to remove the vulnerability. If unable to do so, remove the device from the network.

IoT Asset Vulnerability Detail

Incident #: 549211 **Severity: Low** **Palo Alto Networks Firewall** IP: 10.10.2.3 MAC: 00:1B:17:17:9E:00	========== SUMMARY: ========== * Port 443 is subject to exploit by SSL CCS Injection on device 00:1B:17:17:9E:00 * OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the CCS Injection vulnerability. MAC Address: 00:1B:17:17:9E:00 Device: Palo Alto Networks Firewall Manufacturer: Palo Alto Networks Model: Palo Alto Networks Firewall IP Address: 10.10.2.3 Network Name: 10.0.0.0/8 ======== DETAILS: ======== * https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224 * http://www.cvedetails.com/cve/2014-0224 * http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566 * http://www.openssl.org/news/secadv_20140605.txt ========== RECOMMENDED ACTIONS: ========== * Change device configuration to remove the vulnerability. If unable to do so, remove the device from the network.

IoT Asset Vulnerability Detail

Incident #: 550442 **Severity: Medium** **APC Power Device** IP: 10.1.200.21 MAC: 00:C0:B7:DF:8E:77	========== SUMMARY: ========== * Port 21 is subject to exploit by Default Passwords on device 00:C0:B7:DF:8E:77 MAC Address: 00:C0:B7:DF:8E:77 Device: apcdf8e77.pacworldwide.com Manufacturer: APC Model: APC Power Device IP Address: 10.1.200.21 Network Name: 10.0.0.0/8 ========== RECOMMENDED ACTIONS: ========== * Change device configuration to remove the vulnerability. If unable to do so, remove the device from the network.

IoT Asset Vulnerability Detail

Incident #: 549907 **Severity: Medium** **Color MFC-9130CW** IP: 10.10.0.201 MAC: F4:B7:E2:28:B0:22	========== SUMMARY: ========== * Port 21 is subject to exploit by Default Passwords on device F4:B7:E2:28:B0:22 MAC Address: F4:B7:E2:28:B0:22 Device: Generic Hon Hai Precision Computer Manufacturer: Hon Hai Precision Model: Generic Hon Hai Precision Computer IP Address: 10.10.0.201 Network Name: 10.0.0.0/8 ========== RECOMMENDED ACTIONS: ========== * Change device configuration to remove the vulnerability. If unable to do so, remove the device from the network.

IoT Asset Vulnerability Detail

Incident #: 551130 **Severity: High** **PowerEdge iDRAC** IP: 10.0.22.212 MAC: D4:AE:52:76:B6:B5	========== SUMMARY: ========== * Port 22 is subject to exploit by Default Passwords on device D4:AE:52:76:B6:B5 MAC Address: D4:AE:52:76:B6:B5 Device: Dell Computer Manufacturer: Dell Model: Dell Computer IP Address: 10.0.22.212 Network Name: 10.0.0.0/8 ========== RECOMMENDED ACTIONS: ========== * Change device configuration to remove the vulnerability. If unable to do so, remove the device from the network.

IoT Asset Vulnerability Detail

Incident #: 550297 **Severity: Low** **Wemo Smart Home Device** IP: 10.0.22.99 MAC: EC:1A:59:EF:94:E1	========== SUMMARY: ========== * Port 53 is subject to exploit by Open DNS server on device EC:1A:59:EF:94:E1 MAC Address: EC:1A:59:EF:94:E1 Device: wemo.lan Manufacturer: Belkin Model: Wemo Smart Home Device IP Address: 10.0.22.99 Network Name: 10.0.0.0/8 ========== RECOMMENDED ACTIONS: ========== * Change device configuration to remove the vulnerability. If unable to do so, remove the device from the network.

IoT Asset Vulnerability Detail

Incident #: 546786 **Severity: Low** **Connex Vital Signs Monitor** IP: 10.1.200.201 MAC: 00:1A:FA:01:E7:36	========== SUMMARY: ========== * Port 443 is subject to exploit by SSL DROWN on device 00:1A:FA:01:E7:36 * The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a DROWN attack. MAC Address: 00:1A:FA:01:E7:36 Device: Welch Allyn Device Manufacturer: Welch Allyn Model: Welch Allyn Device IP Address: 10.1.200.201 Network Name: 10.0.0.0/8 ======== DETAILS: ======== * https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0800 * https://www.openssl.org/news/secadv/20160301.txt ========== RECOMMENDED ACTIONS: ========== * Change device configuration to remove the vulnerability. If unable to do so, remove the device from the network.

IoT Asset Vulnerability Detail

Incident #: 548099 **Severity: High** **B. Braun SpaceStation** IP: 10.10.1.55 MAC: 00:12:21:9B:8B:1D	========== SUMMARY: ========== * Device at MAC address 00:12:21:9B:8B:1D vulnerable to CVE-2021-33882. A Missing Authentication for Critical Function vulnerability in B. Braun SpaceCom2 prior to 012U000062 allows a remote attacker to reconfigure the device from an unknown source because of lack of authentication on proprietary networking commands. MAC Address: 00:12:21:9B:8B:1D Device: B. Braun Infusion Pump Manufacturer: B. Braun Medical Model: Label SpaceCOM L82 IP Address: 10.10.1.55 Network Name: 10.0.0.0/8 ========== RECOMMENDED ACTIONS: ========== * Change device configuration to remove the vulnerability. If unable to do so, remove the device from the network.

IoT Asset Vulnerability Detail

Incident #: 548100 **Severity: High** **B. Braun SpaceStation** IP: 10.10.1.55 MAC: 00:12:21:9B:8B:1D	========== SUMMARY: ========== * Device at MAC address 00:12:21:9B:8B:1D vulnerable to CVE-2021-33885. An Insufficient Verification of Data Authenticity vulnerability in B. Braun SpaceCom2 prior to 012U000062 allows a remote unauthenticated attacker to send the device malicious data that will be used in place of the correct data. This results in full system command access and execution because of the lack of cryptographic signatures on critical data sets. MAC Address: 00:12:21:9B:8B:1D Device: B. Braun Infusion Pump Manufacturer: B. Braun Medical Model: Label SpaceCOM L82 IP Address: 10.10.1.55 Network Name: 10.0.0.0/8 ========== RECOMMENDED ACTIONS: ========== * Change device configuration to remove the vulnerability. If unable to do so, remove the device from the network.