3 Vulnerabilities Found on AvertX IP Cameras

32,691 people reacted

43 6 min. read

By Asher Davila
July 17, 2020 at 9:00 AM
Category: Malware, Ransomware, Unit 42
Tags: botnet, Cybercrime, DDoS, exploit kit, IoT, vulnerabilities

This post is also available in: 日本語 (Japanese)

Recommended For You

2022 Unit 42 Incident Response Report

Download now to better understand current threat trends and insights into:
- The most prevalent cybercriminal tactics.
- Which industries were the most affected.
- What contributes to attackers' success.How successful attacks were achieved.
- Top cybersecurity predictions from our incident responders.
- Actionable recommendations to get ahead of future threats.

Get the report

Executive Summary

On February 24, 2020, Palo Alto Networks Unit 42 researchers found vulnerabilities present in AvertX IP cameras running the latest firmware.

Three vulnerabilities were found in AvertX IP cameras with model number HD838 and 438IR, as confirmed by AvertX. These products are surveillance cameras intended to be used outdoors with infrared and object detection technology built-in. They also allow users to store the recordings in the cloud, in a network video recorder (NVR) and also create backups in an SD memory card.

The following are the three vulnerabilities we found:

- CVE-2020-11625: User enumeration
- CVE-2020-11624: Weak password requirements
- CVE-2020-11623: Exposed dangerous method or function

The detected vulnerabilities have the following impact:

- Attackers can remotely enumerate the usernames of IP camera accounts, facilitating brute-force attacks. Since it is possible to collect a set of valid usernames by interacting with the authentication mechanism of the application, it eases brute-force attacks, in which the attacker verifies if, given a valid username, it is possible to find the corresponding password.
- Attackers might be able to access the camera by using its default password because it does not force you to change the default password. A lot of IoT devices offer web-based configuration or administrative interfaces. Often these applications, once installed, are not properly configured and the default credentials provided for initial authentication and configuration are never changed. These default credentials can be obtained by reading the user manual of such a device. As a consequence, attackers, and most common IoT botnets, can use them to gain access to the IoT device.
- Attackers with physical access to the universal asynchronous receiver-transmitter (UART) interface can access its bootloader. As a consequence, they can access and modify additional configurations, reset the configuration and even render the camera inoperable.

The AvertX IP cameras that our team analyzed are rebranded Hikvision cameras with modifications. AvertX has released a patch for these vulnerabilities and has also removed the UART connector and disabled the interface in the latest production batch.

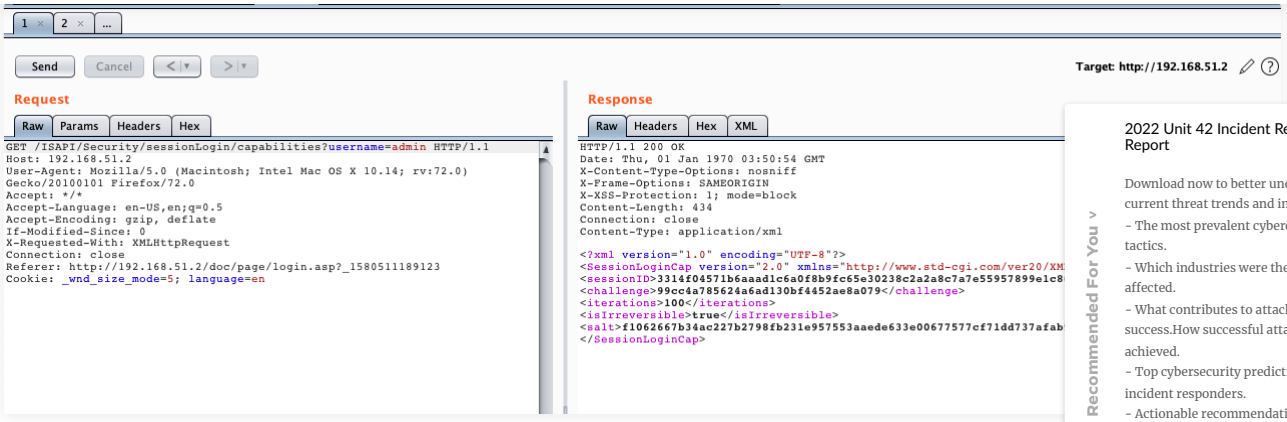
According to the 2020 Unit 42 IoT Threat Report, security cameras make up only 5% of enterprise IoT devices, but they account for 33% of all security issues. This is because many cameras are designed to be consumer-grade, focusing on simplicity of use and deployment over security.

Palo Alto Networks customers are protected from these vulnerabilities via the ML-Powered Next-Generation Firewall, and IoT Security, a subscription available for the NGFW.

CVE-2020-11625: User Enumeration

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. Privacy statement

Manage My Cookie Settings



2022 Unit 42 Incident Response Report

Download now to better understand current threat trends and insights into:
- The most prevalent cybercriminal tactics.
- Which industries were the most affected.
- What contributes to attackers' success.How successful attacks were achieved.
- Top cybersecurity predictions from our incident responders.
- Actionable recommendations to get ahead of future threats.

Get the report

Recommended For You

Figure 1. Request using an existing username

However, if a login request is sent using a username that is not present in the IP camera's database, it will return an empty salt value:

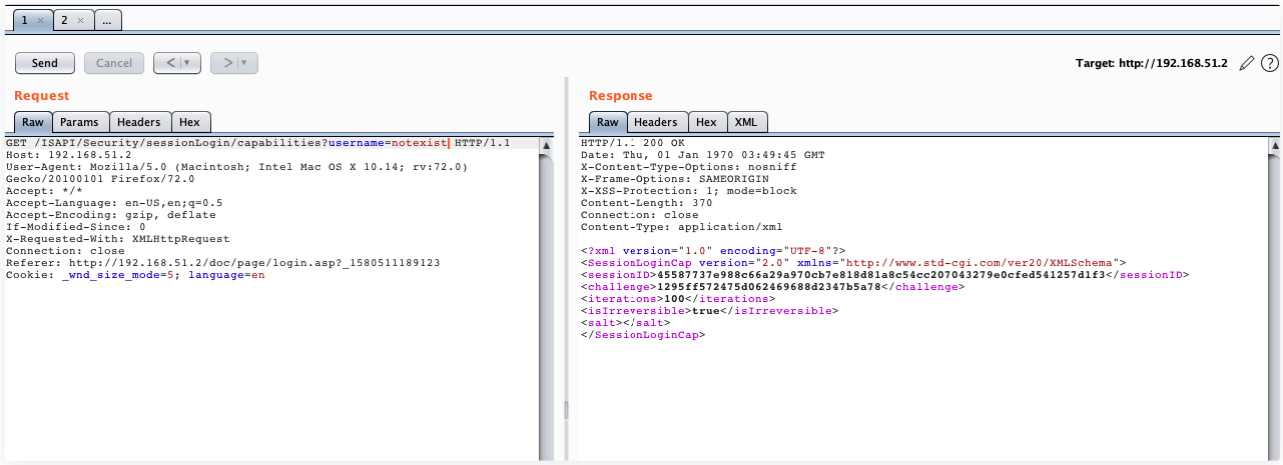


Figure 2. Request using a nonexistent username

This allows attackers to enumerate legitimate usernames, facilitating brute-force attacks.

CVE-2020-11624: Weak Password Requirements

The IP camera does not require users to change the default password for the admin account. Every time the user logs in with the default password, the camera shows a pop-up window suggesting the password be changed, but there's no enforcement. An administrator can click "Cancel" and proceed to use the device without changing the password:

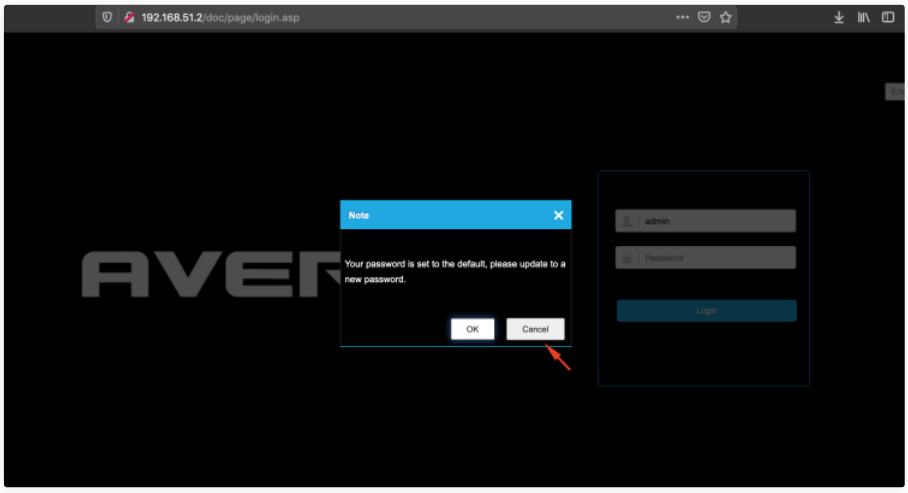


Figure 3. Default password pop-up window that can be ignored

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. Privacy statement

```
define(function(require, exports, module) {
    function e() {
        this.resize(), this.bError = !1, this.oLanLogin = null, this.szDefaultUser = "admin",
    }
    var t = require("common"),
        a = require("lib/base64"),
        i = require("webSession");
    require("config/ui.config");
    var n = require("translator"),
        o = require("dialog"),
        r = require("utils"),
        s = require("encryption"),
        l = require("isapi/response");
    require("config/ui.config");
    var u = require("common/plugin"),
```

Figure 4. Default username disclosed on login.js script

Recommended For You

2022 Unit 42 Incident Response Report

Download now to better understand current threat trends and insights into:
- The most prevalent cybercriminal tactics.
- Which industries were the most affected.
- What contributes to attackers' success.How successful attacks were achieved.
- Top cybersecurity predictions from our incident responders.
- Actionable recommendations to get ahead of future threats.

Get the report

CVE-2020-11623: Exposed Dangerous Method or Function

There is an exposed UART interface that allows access to diagnostic and configuration functionalities, and even to system information that can be modified. This security vulnerability can be exploited by attackers with physical access to the UART interface.

```
7 +0800), Build: jenkins-Frontend.BSP.CCI-1801

SPI Nor:  boot media is not spi nor
NAND:  Check Flash Memoryontroller v100 ... Found
MMC:  Boot media is not eMMC
eth0
[Uboot] In release mode!
Hit Ctrl+u to stop autoboot:  0
HKVS #
```

Figure 5. Bootloader console

The team was able to identify a 4-pin Molex connector that was unpopulated. Most UART interfaces in commercial products are between four and six pins, so the team proceeded to identify and test the pins.

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. Privacy statement

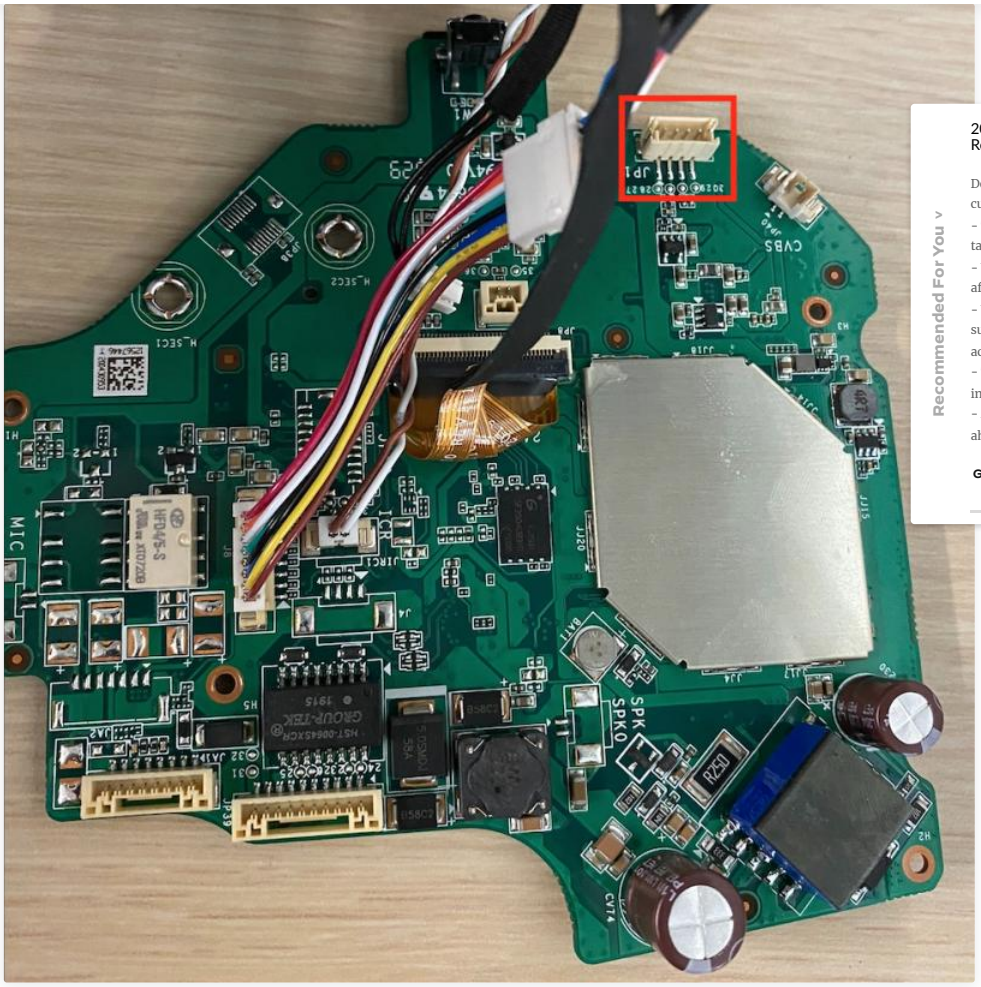


Figure 6. Image of the printed circuit board (PCB), with a 4-pin Molex connector present

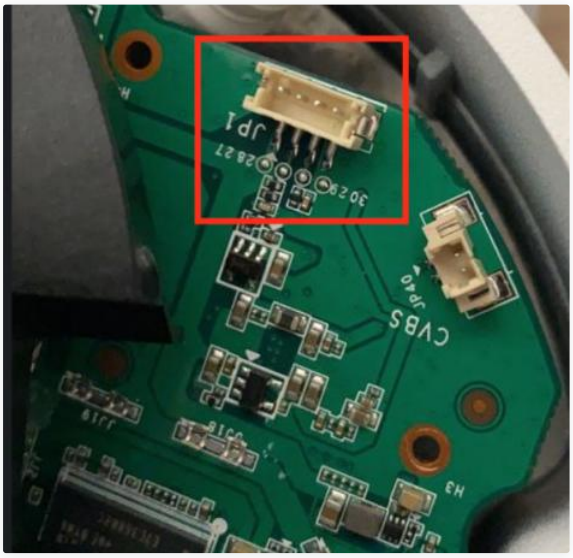


Figure 7. A closer view of the 4-pin Molex connector

Connecting to the UART

We connected to the UART interface through an Attify Badge, which is a hardware security tool that uses an FTDI chip, allowing it to speak a wide variety of communication protocols such as SPI, JTAG, I2C and UART. It also has a microUSB port, allowing it to be connected to a PC.

Recommended For You

2022 Unit 42 Incident Response Report

Download now to better understand current threat trends and insights into:
- The most prevalent cybercriminal tactics.
- Which industries were the most affected.
- What contributes to attackers' success.How successful attacks were achieved.
- Top cybersecurity predictions from our incident responders.
- Actionable recommendations to get ahead of future threats.

Get the report

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. Privacy statement

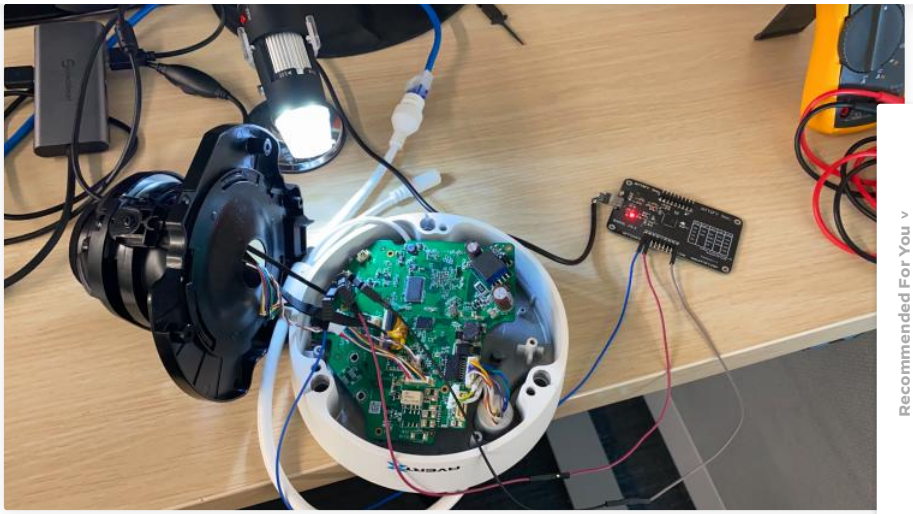


Figure 8. Connecting to the UART

Recommended For You

2022 Unit 42 Incident Response Report

Download now to better understand current threat trends and insights into:
- The most prevalent cybercriminal tactics.
- Which industries were the most affected.
- What contributes to attackers' success.How successful attacks were achieved.
- Top cybersecurity predictions from our incident responders.
- Actionable recommendations to get ahead of future threats.

Get the report

To determine the baud rate, we tested with the most common values. We opened a screen terminal to communicate with the camera's UART using a baud rate of 115200. To obtain a Uboot prompt, we interrupted the booting process pressing CTRL + U. No username or password was required:

```
ontend.BSP.CCI-1801

SPI Nor:  boot media is not spi nor
NAND:  Check Flash Memoryontroller v100 ... Found
MMC:  Boot media is not eMMC
In:    serial
Out:   serial
Err:   serial
Net:   Hisilicon ETH net controler
eth0
[Uboot] In release mode!
Hit Ctrl+u to stop autoboot:  0
HKVS #
```

Figure 9. Bootloader console access (U-boot)

At this point, several commands are available to obtain information about this device including the firmware and configuration settings. Since this device is intended to be used outdoors, it is especially important to protect it against physical attacks as well as remote attacks.

Conclusion

In summary, the AvertX IP camera models HD838 and 438IR are a rebranded version of Hikvision cameras with modifications and have three vulnerabilities that can be used to compromise the device and even render it inoperable.

- The first is the user enumeration, which allows attackers to perform brute force attacks more efficiently.
- The second vulnerability is the lack of strong password requirements, which facilitates attackers' efforts to find and compromise cameras using default credentials.
- The last one is an exposed UART interface, which allows attackers with physical access to the camera to extract information off the device, change configuration values and even render the device inoperable.

AvertX responded quickly when contacted and has released a patch for the issues mentioned above. In addition, AvertX has removed the UART connector and disabled the interface starting with the latest production batch.

Palo Alto Networks protects its customers from attacks on AvertX IP cameras through the following platforms:

1. The ML-Powered Next-Generation Firewall, which is capable of identifying brute force attacks to block or alert them.
2. IoT Security, a subscription available for the NGFW, which detects brute force attacks on IoT devices and anomalous traffic.

Appendix

CVEs:

CVE-ID	Vulnerability type
CVE-2020-11625	User enumeration

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. Privacy statement

Table 1. CVEs related to this post

**The CVE entries will be updated soon*

References:

https://owasp.org/

Recommended For You >

2022 Unit 42 Incident Response Report

Download now to better understand current threat trends and insights into:
- The most prevalent cybercriminal tactics.
- Which industries were the most affected.
- What contributes to attackers' success.How successful attacks were achieved.
- Top cybersecurity predictions from our incident responders.
- Actionable recommendations to get ahead of future threats.

Get the report

Get updates from Palo Alto Networks!

Sign up to receive the latest news, cyber threat intelligence and research from us

Email address

Subscribe

I'm not a robot

By submitting this form, you agree to our Terms of Use and acknowledge our Privacy Statement.

© 2022 Palo Alto Networks, Inc. All rights reserved.

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. Privacy statement