WHITEPAPER

Bitdefender®

Security

Cracking the August SmartLock: WiFi Password Eavesdropping Made Easy

CVE-2019-17098 – WI-FI NETWORK CREDENTIALS LEAK

www.bitdefender.com

Contents

Foreword

The rise of online property rental in an increasingly competitive sharing economy has had a significant impact on the adoption of Internet-connected smart locks. Packed with features that allow landlords to issue and revoke access by electronically sharing a token or PIN code during booking, smart locks have managed to eliminate the need to meet strangers or use key drops.

Unlike most IoT devices, smart locks create physical security boundaries, and products from top lock companies are preferred to generic brands. But do the devices made by lock companies that made history in the evolution of the modern lock live up to their digital promise?

This article – part of a series developed in partnership with PCMag – aims to shed light on the security of the world's best-sellers in the IoT space. PCMag asked the research team at Bitdefender to look at several popular devices, including the August Smart Lock and ConnectWi-Fi Bridge. More information is available in the article published on our partner's website.

Vulnerabilities at a glance

The Bitdefender IoT Vulnerability Research Team discovered that the device talks with the configuration application on the smartphone in an encrypted manner, but the encryption key is hardcoded into the app. This allows a potential attacker within range to eavesdrop on the traffic and intercept the Wi-Fi password.

This vulnerability is similar to the one identified in the Ring Video Doorbell Pro.

Disclosure timeline

- Dec 09, 2019: Initial contact with the affected vendor. PGP keys are exchanged
- Dec 10, 2019: Vendor receives a copy of the report in advance
- Dec 18, 2019: Information is sent once again to affected vendor
- Dec 18, 2019: Vulnerability confirmed
- Dec 18, 2019: Bitdefender reserves CVE-2019-17098
- May 11, 2020: Vendor requests coordinated pubic disclosure to be scheduled in early June 2020
- Jan 16, 2020: Bitdefender requests an update
- Jul 02, 2020: Bitdefender requests another update in preparation of public disclosure
- Aug 6, 2020: As we have not heard back from the vendor, the report becomes public

Cloud – device communication

The August Smart Lock Pro cannot connect directly to the internet, as it lacks the necessary hardware to connect to a wireless or wired network. Instead, it uses the August Connect Wi-Fi Bridge as a gateway and talks to it via BLE. The bridge connects to the local wireless network and acts as a relay, making it possible for the user to remotely control the lock over the internet. Every request between the bridge and the servers is encrypted with TLS and cannot be intercepted or modified due to certificate pinning.

Local network

The lock communicates with the August Home app through BLE, when the smartphone is near. Otherwise, the connection gets passed through the bridge and via the internet.

Initial device configuration

The August Smart Lock is paired to the smartphone and always communicates through BLE when nearby. August Connect talks to the local wireless network and is configured to work only if the user has a lock registered to their account.

To receive the required credentials, the bridge creates an open access point that the mobile phone would connect to. The app will then use the API provided by the device to require additional information and send the local network credentials. However, this approach has some flaws, as detailed in [1].

Smartphone app – cloud communication

a. Account management

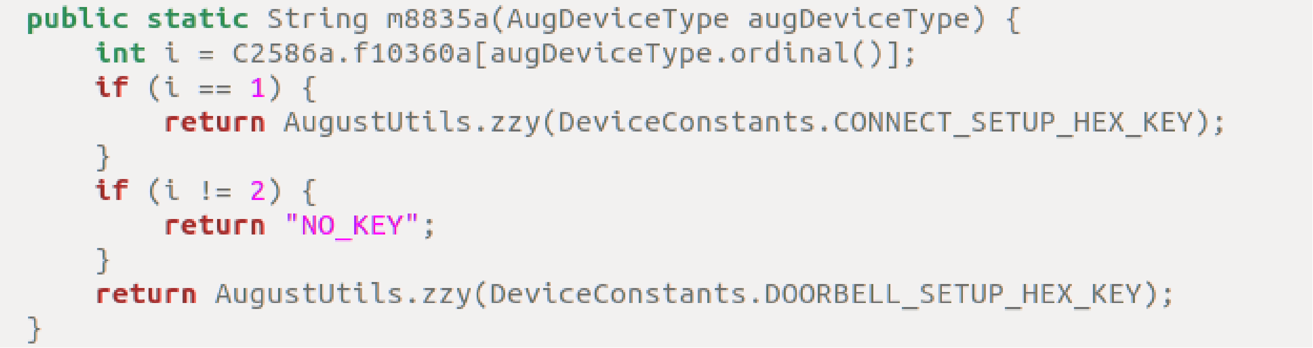
The user is required to register their own August Home account. The app also uses two-factor authentication to log users in. Each device is then linked to the user's account.

b. Device access control

Only the owner can fully control the lock, either from the internet or in proximity. Other users need permission from the owner, who has the option to give full or limited access.

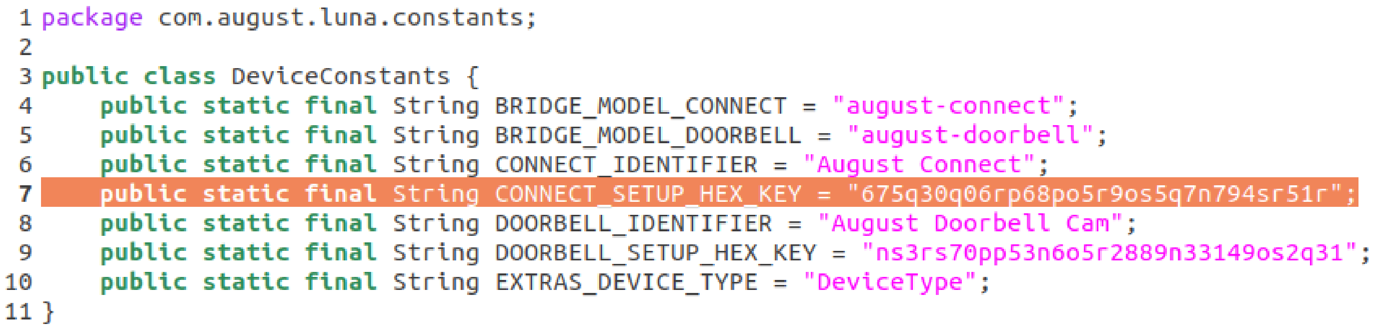
[1] Wireless network credentials leak

As stated above, when configuring the August Connect, the device acts as an access point that the smartphone connects to. This access point is open, so communication between the device and the smartphone is not encrypted and can be sniffed. In an attempt to mitigate this, the app will encrypt the payload containing the local wireless network credentials before sending it to the device.



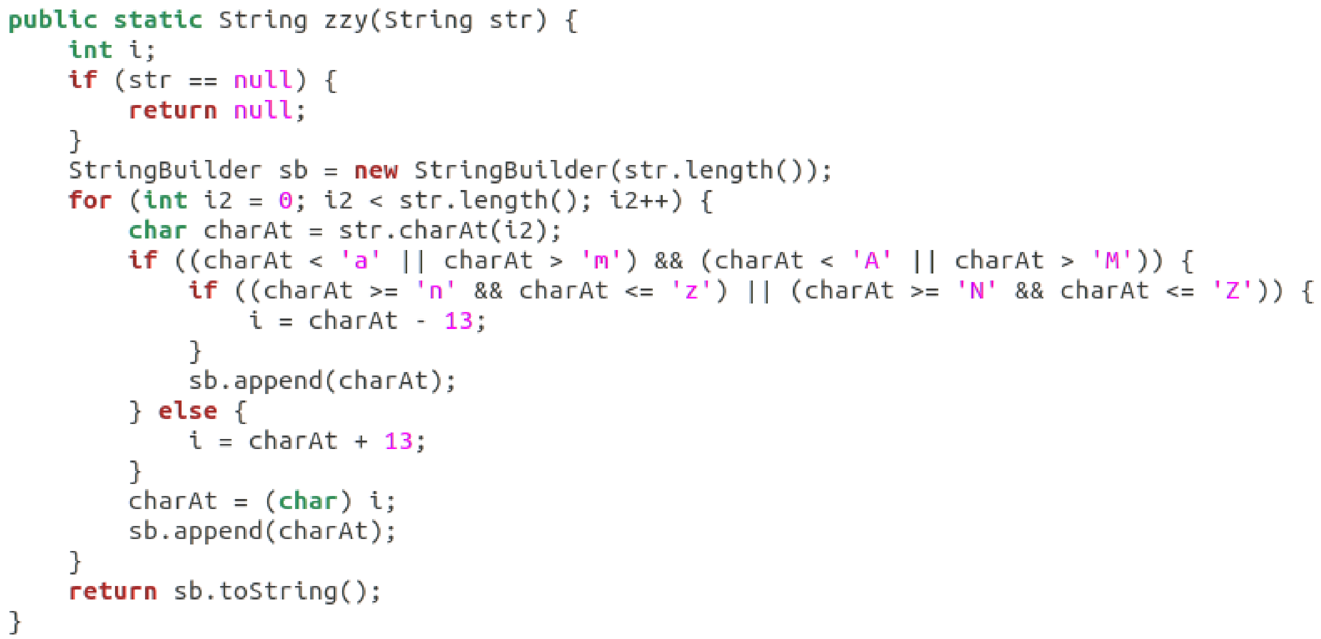
```
public static String m8835a(AugDeviceType augDeviceType) {
    int i = C2586a.f10360a[augDeviceType.ordinal()];
    if (i == 1) {
        return AugustUtils.zzy(DeviceConstants.CONNECT_SETUP_HEX_KEY);
    }
    if (i != 2) {
        return "NO_KEY";
    }
    return AugustUtils.zzy(DeviceConstants.DOORBELL_SETUP_HEX_KEY);
}
```

The encryption scheme used is AES/CBC with the encryption key hardcoded in the smartphone app, although obfuscated using ROT13. To get the encryption key, the app verifies the device type and will pull a constant string based on this.



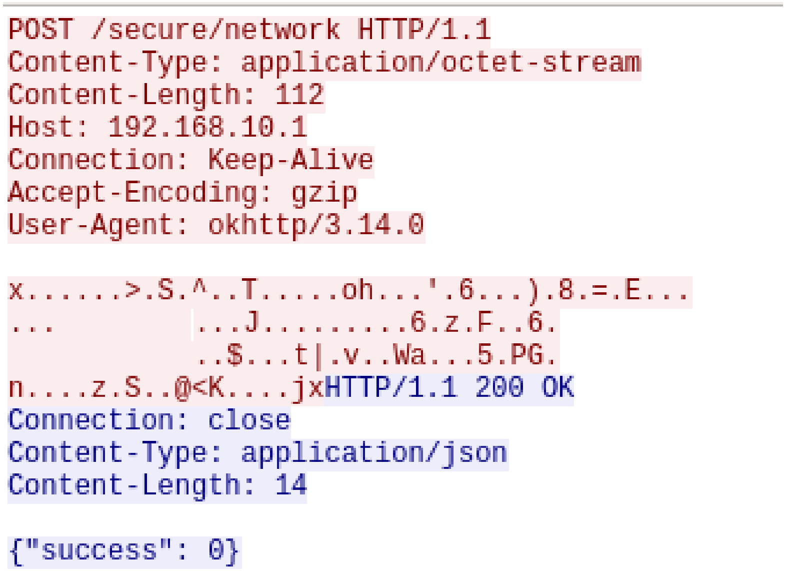
```java
package com.august.luna.constants;

public class DeviceConstants {
    public static final String BRIDGE_MODEL_CONNECT = "august-connect";
    public static final String BRIDGE_MODEL_DOORBELL = "august-doorbell";
    public static final String CONNECT_IDENTIFIER = "August Connect";
    public static final String CONNECT_SETUP_HEX_KEY = "675q30q06rp68po5r9os5q7n794sr51r";
    public static final String DOORBELL_IDENTIFIER = "August Doorbell Cam";
    public static final String DOORBELL_SETUP_HEX_KEY = "ns3rs70pp53n6o5r2889n33149os2q31";
    public static final String EXTRAS_DEVICE_TYPE = "DeviceType";
}
```

The key is then deobfuscated by applying ROT13:



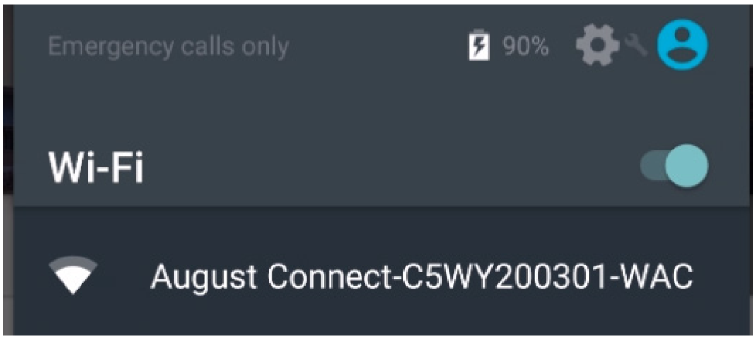
```java
public static String zzy(String str) {
    int i;
    if (str == null) {
        return null;
    }
    StringBuilder sb = new StringBuilder(str.length());
    for (int i2 = 0; i2 < str.length(); i2++) {
        char charAt = str.charAt(i2);
        if ((charAt < 'a' || charAt > 'm') && (charAt < 'A' || charAt > 'M')) {
            if ((charAt >= 'n' && charAt <= 'z') || (charAt >= 'N' && charAt <= 'Z')) {
                i = charAt - 13;
            }
            sb.append(charAt);
        } else {
            i = charAt + 13;
        }
        charAt = (char) i;
        sb.append(charAt);
    }
    return sb.toString();
}
```

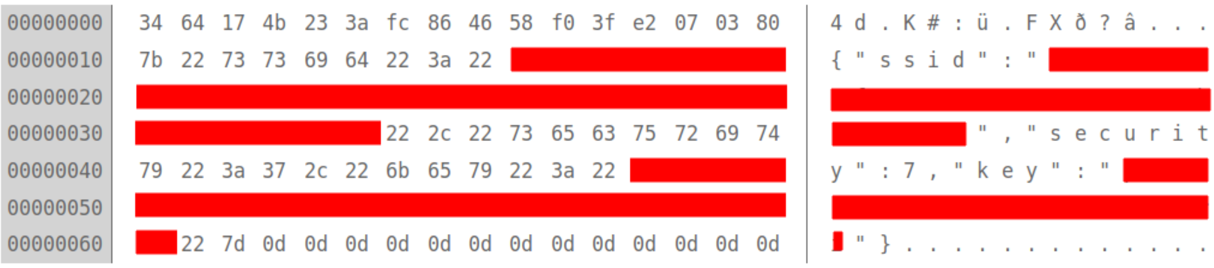
The resulting key will be used to encrypt the payload and send it to the device:



```
POST /secure/network HTTP/1.1
Content-Type: application/octet-stream
Content-Length: 112
Host: 192.168.10.1
Connection: Keep-Alive
Accept-Encoding: gzip
User-Agent: okhttp/3.14.0

x......>.S.^..T.....oh...'.6...).8.=.E...
...          ...J.........6.z.F..6.
             ..$...t|.v..Wa...5.PG.
n....z.S..@<K....jxHTTP/1.1 200 OK
Connection: close
Content-Type: application/json
Content-Length: 14

{"success": 0}
```

However, because the wireless network is open, anybody can sniff this interaction and grab the encrypted payload. Then, using the same key hardcoded in the smartphone app, they can decrypt and get the credentials.





```
00000000  34 64 17 4b 23 3a fc 86 46 58 f0 3f e2 07 03 80   4 d . K # : ü . F X ð ? â . . .
00000010  7b 22 73 73 69 64 22 3a 22 [redacted]              { " s s i d " : " [redacted]
00000020  [redacted]                                         [redacted]
00000030  [redacted] 22 2c 22 73 65 63 75 72 69 74           [redacted] " , " s e c u r i t
00000040  79 22 3a 37 2c 22 6b 65 79 22 3a 22 [redacted]    y " : 7 , " k e y " : " [redacted]
00000050  [redacted]                                         [redacted]
00000060  [redacted] 22 7d 0d 0d 0d 0d 0d 0d 0d 0d 0d 0d 0d 0d 0d   [redacted] " } . . . . . . . . . . . . .
```

This page is left blank

Why Bitdefender

Proudly Serving Our Customers

Bitdefender provides solutions and services for small business and medium enterprises, service providers and technology integrators. We take pride in the trust that enterprises such as **Mentor, Honeywell, Yamaha, Speedway, Esurance or Safe Systems** place in us.

Leader in Forrester's inaugural Wave™ for Cloud Workload Security
NSS Labs "Recommended" Rating in the NSS Labs AEP Group Test
SC Media Industry Innovator Award for Hypervisor Introspection, 2nd Year in a Row
Gartner® Representative Vendor of Cloud-Workload Protection Platforms

Dedicated To Our +20.000 Worldwide Partners

A channel-exclusive vendor, Bitdefender is proud to share success with tens of thousands of resellers and distributors worldwide.

CRN 5-Star Partner, 4th Year in a Row. Recognized on CRN's Security 100 List. CRN Cloud Partner, 2nd year in a Row
More MSP-integrated solutions than any other security vendor
3 Bitdefender Partner Programs - to enable all our partners – resellers, service providers and hybrid partners – to focus on selling Bitdefender solutions that match their own specializations

Trusted Security Authority

Bitdefender is a proud technology alliance partner to major virtualization vendors, directly contributing to the development of secure ecosystems with **VMware, Nutanix, Citrix, Linux Foundation, Microsoft, AWS, and Pivotal.**

Through its leading forensics team, Bitdefender is also actively engaged in countering international cybercrime together with major law enforcement agencies such as FBI and Europol, in initiatives such as NoMoreRansom and TechAccord, as well as the takedown of black markets such as Hansa. Starting in 2019, Bitdefender is also a proudly appointed CVE Numbering Authority in MITRE Partnership.

RECOGNIZED BY LEADING ANALYSTS AND INDEPENDENT TESTING ORGANIZATIONS

TECHNOLOGY ALLIANCES

Bitdefender®

Founded 2001, Romania
Number of employees 1800+

Headquarters
Enterprise HQ – Santa Clara, CA, United States
Technology HQ – Bucharest, Romania

WORLDWIDE OFFICES
USA & Canada: Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
Europe: Copenhagen, DENMARK | Paris, FRANCE | München, GERMANY | Milan, ITALY | Bucharest, Iasi, Cluj, Timisoara, ROMANIA | Barcelona, SPAIN | Dubai, UAE | London, UK | Hague, NETHERLANDS
Australia: Sydney, Melbourne

UNDER THE SIGN OF THE WOLF

A trade of brilliance, data security is an industry where only the clearest view, sharpest mind and deepest insight can win — a game with zero margin of error. Our job is to win every single time, one thousand times out of one thousand, and one million times out of one million.

And we do. We outsmart the industry not only by having the clearest view, the sharpest mind and the deepest insight, but by staying one step ahead of everybody else, be they black hats or fellow security experts. The brilliance of our collective mind is like a **luminous Dragon-Wolf** on your side, powered by engineered intuition, created to guard against all dangers hidden in the arcane intricacies of the digital realm.

This brilliance is our superpower and we put it at the core of all our game-changing products and solutions.

Bitdefender-PR-Whitepaper-AugustConnect-creat4699-en_EN
07/30/20August 3, 2020 9:02 am08/03/20