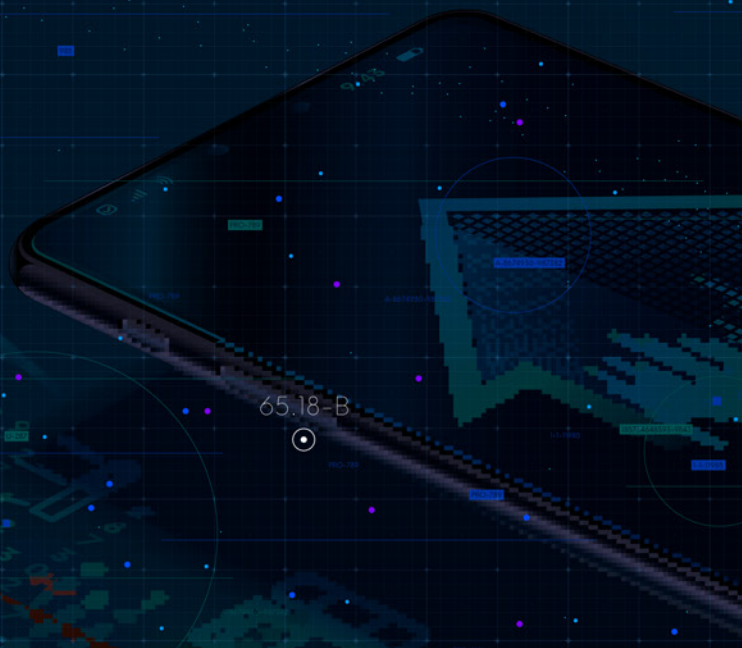
WHITEPAPER

Bitdefender



Security

Maximus Answer DualCam Video Doorbell

www.bitdefender.com

Contents

Foreword....3

Device at a glance....3

1. Cloud-device communication:....4

a. Authentication/Identification....4

b. Communication protocols used:....4

c. Communication channel security:....4

d. Information sent in logs:....5

f. Firmware update:....5

2. Local network:....5

3. Setup:....5

4. Application – cloud communication:....6

5. Hardware access:....6

Foreword

Internet-connected doorbells with motion-sensing and notification capabilities have become extremely popular among smart home enthusiasts. Convenient and easy to use, they are often regarded as the first line of physical security defense, but these devices often end up exposing private customer information or granting attackers access to the customer network.

As the creator of the world's first smart-home cybersecurity hub, Bitdefender constantly audits popular IoT hardware for vulnerabilities that might affect customers if left unaddressed. *This research paper, part of a series developed in partnership with* **Tom's Guide,** *aims to shed light on the security of the world's best-sellers in the IoT space.*

Device at a glance

The Maximus Answer DualCam Video Doorbell is a dual-camera IoT device with night-vision capabilities. It is designed to monitor both the entrance and packages left on the porch with a 180-degree view, day or night.

The good

- Use of OpenVPN tunneling with unique client certificates to prevent eavesdropping on traffic
- Signed firmware binary to ensure integrity
- Overall good security practices

The bad

- The device does not validate the server certificate on HTTPS connections
- Logs and video alerts can be intercepted using trivial man-in-the-middle attacks

1. Cloud-device communication:

a. Authentication/Identification

The device uses OpenVPN to establish a connection with the server (vpn.kunasystems.com). The connection requires a client certificate that is unique for each camera and is stored on the flash memory in production.

The device also stores a 32-character hexadecimal secret that, together with a nonce, can be hashed into a token. Some services require the token and the nonce value so the server can verify that the message originated from the camera.

b. Communication protocols used:

- OpenVPN protocol – for most of the communication
- HTTPS – for uploading recordings to an AWS S3 bucket, sending logs and firmware update

c. Communication channel security:

The OpenVPN protocol is secure against tampering and eavesdropping. A warning in the log files suggests that the server certificate is not verified (*WARNING: No server certificate verification method has been enabled. See http://openvpn.net/howto.html#mitm for more info.*)

This could theoretically allow an attacker to impersonate the server, but the attack requires knowledge of both the ta.key file (to authenticate TLS connections), and a way to trick the camera into connecting to the rogue server.

The HTTPS protocol is used in sending logs to logs-01.loggly.com and recordings to a bucket on s3.amazonaws.com. Both connections are vulnerable to a man-in-the-middle attack, as the camera does not verify the server certificate. As a result, an attacker sitting between the camera and the servers could intercept the uploaded logs and recordings.

Intercepted upload request:

```
PUT /kuna--production--us-east-1--recordings/V1C441908132/2021_08_13__14_50_48+0300/V1C441908132-2021_08_13__14_50_48+0300-0
HTTP/1.1
Host: s3.amazonaws.com
Accept: */*
x-amz-content-sha256: a5031ed6c854dcd45c5966a276a4408fdc2cadc47125da07ed966ac5f2bec067
x-amz-date: 20210813T115109Z
x-amz-meta-timestamp: 2021-08-13 14:51:09
x-amz-security-token:
FwoGZXIvYXdzEP3/////////wEaDOrin+pcfiMnmrTaBiKpAh4SGyqMrRsKogalbvlc1skaz5CRqwR0YHjMaP6fQA+7sHGj/lK756i4jyUsvZCxNN3EBIlMtMiOEC
Lej//o9/xMAsSsZwN1/sjMsOzzOxj63A0k+q/MnJFbJUahHo7KCavRpP+5QkZpVa1ngz8kbkCGWGGxCaC9tBp2lHqpw7l329Kv65BNWHUuE8HoDfVWczi/LXzWwo9L
GW7zvK5qlsZA9LL/Vwz8fnHX+KXaMZxsmU3I19QdatmLNCheuYWvWx5jGwsikpoRsxfhHXQC7goXTZvgjVBldYL5tmV8GDYhSscSB3DQnoF2BF3K4C73Zn+Ha70RZ7
OlqQKfggDUCKOHI9u6WolJxFOdECNX8D6TV8XvD43SeMEItOJ3Mr9kMoJpvi8TBUUwMyiZudmIBjItBirsI6l5K/cHHBMgkmdpYYxrVjdb1aNdzsUDCgNtKbISmRXK
OBF7EKDzd+3S
Authorization: AWS4-HMAC-SHA256
Credential=ASIA2HDF7UJZP34IY5W4/20210813/us-east-1/s3/aws4_request,SignedHeaders=host;x-amz-content-sha256;x-amz-date;x-amz-me
ta-timestamp;x-amz-security-token,Signature=3a44d4c21fd0418873d137f5c837949b14962f7b4858c30390a08939a96b9665
Content-Type: video/MP2T
Content-Length: 1460572
Connection: close

G`f
```

Intercepted logging request:

```
POST /bulk/61391be8-d772-47c3-ae83-75618406854a@41058/tag/KUNA_VJW01,V1C441908132,30080473,master/ HTTP/1.1
Host: logs-01.loggly.com
Accept: */*
Content-Type: text/plain
Content-Length: 7302
Expect: 100-continue
Connection: close

{"timestamp":"2021-08-13T14:50:38.449256-0300","id":422,"severity":"info","facility":1,"appName":"kuna_img_control","j":{"fn":
"_daynight_mode_detect","t":"avg-gain:19 raw-gain:19"}}
{"timestamp":"2021-08-13T14:50:48.096214-0300","id":423,"severity":"info","facility":1,"appName":"kunamonitor","j":{"fn":"kunad
b_notify_wait","t":"DB key DB_BUTTON_STATE was updated, calling handlers"}}
{"timestamp":"2021-08-13T14:50:48.096256-0300","id":424,"severity":"info","facility":1,"appName":"kunaimage","j":{"fn":"kunadb_
notify_wait","t":"DB key DB_BUTTON_STATE was updated, calling handlers"}}
{"timestamp":"2021-08-13T14:50:48.255446-0300","id":425,"severity":"info","facility":1,"appName":"kunarest","j":{"fn":"kunarest
_handle_params_patch","j":{"patch_data": {"prerecorded_msg": 3}}}}
{"timestamp":"2021-08-13T14:50:48.258319-0300","id":426,"severity":"info","facility":1,"appName":"kunaaudio","j":{"fn":"kunadb_
notify_wait","t":"DB key DB_PRERECORDED_MESSAGE was updated, calling handlers"}}
{"timestamp":"2021-08-13T14:50:48.262746-0300","id":427,"severity":"info","facility":1,"appName":"kunarest","j":{"fn":"kunarest
_handle_params_get","j":{"get_data": { "play": "none", "volume": 59 },}}}
{"timestamp":"2021-08-13T14:50:48.545591-0300","id":428,"severity":"error","facility":1,"appName":"kunamonitor","j":{"fn":"_sys
tem_monitor_signal_main","t":"sigwait failed with errno=4"}}
{"timestamp":"2021-08-13T14:50:48.568889-0300","id":429,"severity":"error","facility":1,"appName":"kunamonitor","j":{"fn":"_sys
tem_monitor_signal_main","t":"sigwait failed with errno=4"}}
```

d. Information sent in logs:

Even though the logs could be intercepted, they do not contain sensitive information that could be useful to an attacker. Most of the messages pertain to the functioning of the camera. The surrounding Wi-Fi networks and their MAC addresses are transmitted, as well as the name of the current network.

The password for the current network is not transmitted.

f. Firmware update:

The user can manually force the check for a firmware update, but the device will also periodically check for a new version of the firmware.

If a new version is available, the camera will request the firmware and its signature from update.kunasystems.com. The request can be intercepted with a man-in-the-middle attack, but the firmware is signed. This means that any modifications to the binary will result in a signature mismatch. The binary will be discarded in this case. An attacker can't forge the signature, as it requires the private certificate corresponding to the public key used to check the signature.

2. Local network:

No ports can be accessed on the local interface because of *iptables* rules that drop any incoming connection. CVE-2019-14899 was tested in order to hijack the VPN connection, but the camera is not vulnerable.

3. Setup:

At first, the Kuna application connects to the camera using Bluetooth. To initiate the setup, the device sends back the surrounding Wi-Fi networks, its serial number, common name and a nonce. The app sends the serial number together with the common name and the nonce to server.kunasystems.com. The server then replies with a token (the SHA1 hash of the nonce + secret) that will be sent to the camera along with the Wi-Fi credentials.

The Bluetooth connection can be established at any time to change the Wi-Fi network, but only the camera owner can initiate it. This is enforced by the secret known only by the camera and the server. If an attacker wishes to change the network, they would need either the secret to create the token, or the token provided from the server. The secret is unknown, and the server sends the token to the owner only.

4. Application – cloud communication:

The requests that control the camera, manage the account, or ask for a recording are sent to server.kunasystems.com. They must contain a token that is received at login. To modify the camera's settings, the user requires its serial number. An attacker who knows the serial number cannot modify settings, as ownership is validated.

To access a recording, the user receives a pre-signed URL that leads to the file in an AWS bucket.

For live streaming, a WebSocket Secure connection is made to video.kunasystems.com. The first request contains the authentication token in the following format:

```
wss://video.kunasystems.com:443/ws/rtsp/proxy?authtoken=<token>
```

After the connection is established, a custom protocol is used to set up a proxy between the application and the camera. First, the serial number of the camera - as well as the token - must be provided for authentication. After that, RTSP messages will be routed through this connection and the camera starts sending the video stream.

5. Hardware access:

The pins for a UART serial connection are exposed on the camera. The boot process can be observed on this connection, and at the end of it a password protected console is provided. The password for the root user is the secret mentioned earlier, and it's unknown.

Serial login prompt:

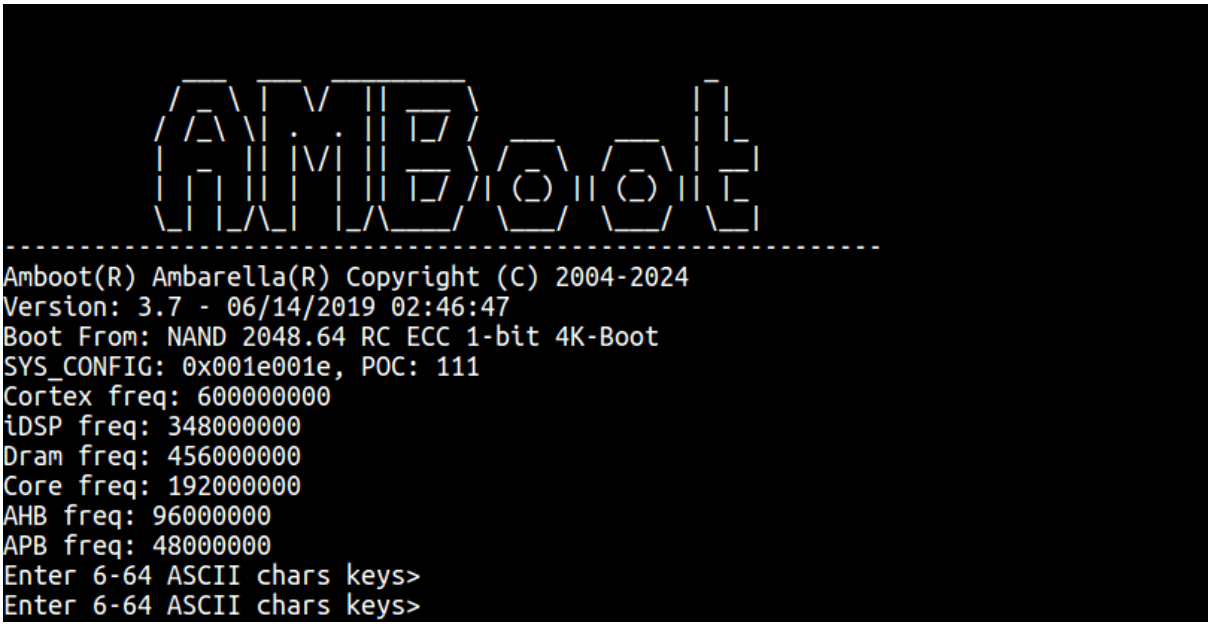
```
  : values=3
count : 20[    9.447064] buf : reg-value:0x02:0x81
[    9.450882] pData = reg-value:0x02:0x81
[    9.454922] [SKL_POWER]skylight_power_chage_regs 175 [    9.460026] 20 reg-value:0x02:0x
81
[    9.460026]


Welcome to Kuna
Kuna login: crond[557]: crond (busybox 1.24.1) started, log level 8
```

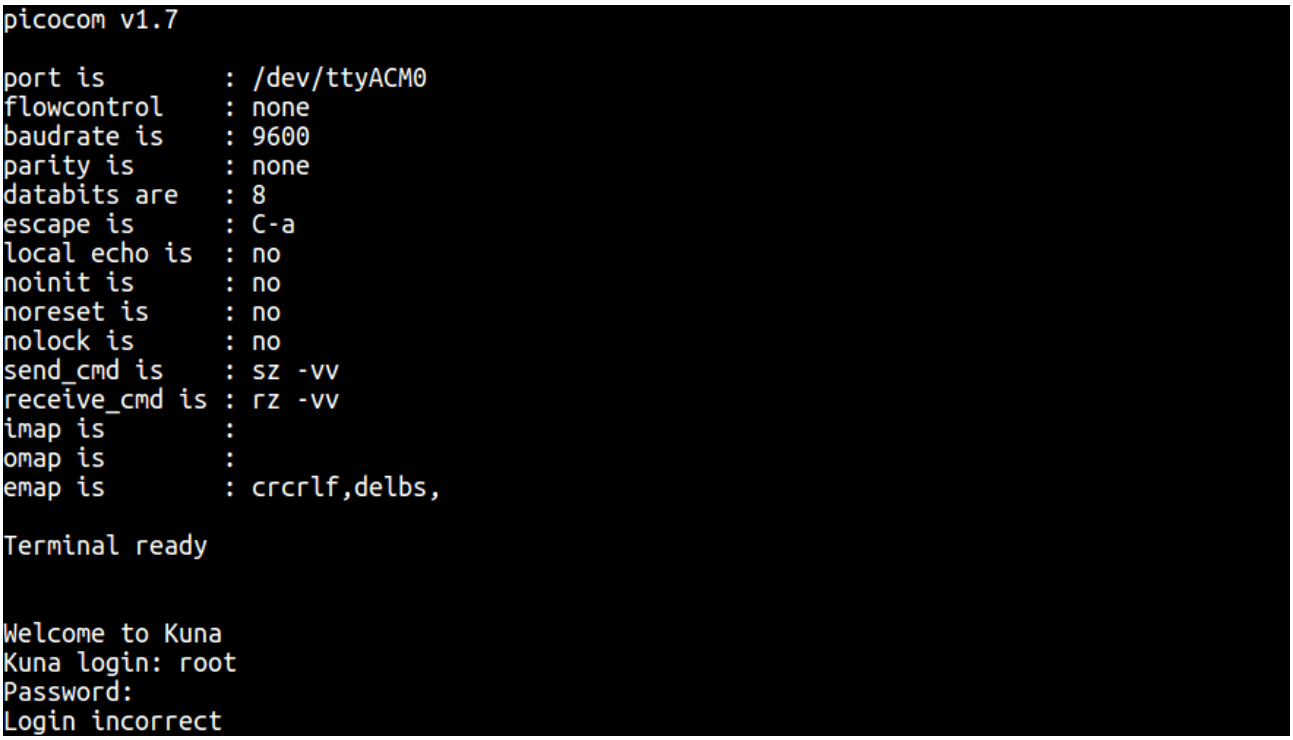
The boot process can be interrupted by shorting the TX and RX pins. The Ambarella bootloader will ask for a password to access its console, but this password is unknown.

The UART connection is also accessible over USB, but it also requires the password for the root user.

Amboot login prompt:



USB serial login prompt:



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-WhitepaperMDBcreat5659-en_EN
09/13/21September 13, 2021 3:31 pm09/13/21