ZKTeco BioTime Missing Authentication

Posted Nov 5, 2022 • Updated Nov 7, 2022
By Dimitri Lesy
1 min read

Product	ZKTeco BioTime
Vendor	ZKTeco Co., Ltd
Tested Versions	8.5.4 - 8.5.5 (Build:20221013.1414beta)
Fixed Version	Unresolved
Vulnerability Type	Improper Access Control
CVSSv3.1 Severity	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CWE Reference	CWE-306
CVE Reference	CVE-2022-30515

Summary

During a recent penetration test, I stumbled upon an instance of the ZKTeco BioTime web application. This application was linked to a time punch clock taking pictures of employees. The management can then analyse these pictures through the web application or an app.

Through some directory fuzzing, I discovered the world-readable directories `/files/photo` and `/files/biophoto`. These directories contained the aforementioned pictures, which were viewable without authenticating to the web app. Since the filename structure used in the web application was incremental, brute-forcing all images present was trivial.

Proof of Concept

0:00 / 0:22

Remediation

The vendor failed to respond to any communication, leaving the vulnerability present in a default installation. It is recommended to implement access restrictions to prevent access to this data.

Disclosure Timeline

February 2022	Vulnerability Discovered

2022-05-16	Second contact attempt
2022-11-05	Vulnerability Published

References

1. MITRE CVE Reference
2. ZKTeco Middle East Website

Security Advisories

zkteco biotime authentication

Share:

Further Reading

May 16, 2022

Tangro BWF Multiple Vulnerabilties

Product Tangro BWF Vendor tangro software components GmbH (Heidelberg, Germany) Tested Version 1.17.5 Fixed Version ...

May 4, 2022

Installing EndeavourOS (Parallels, M1)

In this guide I will briefly go through the installation of EndeavourOS in Parallels Desktop on an M1 MacBook. I will be using an ArchBoot ISO t…

OLDER
Tangro BWF Multiple Vulnerabilties

NEWER
-