hamoshwani / CVE-2022-38802

Last active 2 months ago

Code Revisions 2

Administrator can exploit XSS into local file read using PDF generator in Zkteco Biotime

CVE-2022-38802

```
Security Advisory

Topic:          Administrator can exploit XSS into local file read using PDF generator in Zkteco Biotime

Category:       Zkteco Biotime
Module:         webgui
Announced:      01-09-2022
Credits:        Ahmed Kameran From https://technobase.krd/ -- https://twitter.com/hamoshwani
CVE ID:         CVE-2022-38802
Affects:        BioTime - < 8.5.3  Build:20200816.447
Corrected:      BioTime - > 8.5.3  Build:20200816.447

1.   Background

BioTime 8.0 is a powerful web-based time and attendance management software that provides a stable connection to ZKTeco's
standalone push communication devices by Ethernet/Wi-Fi/GPRS/3G and working as a private cloud to
offer employee self-service by mobile application and web browser.

2.  Problem Description

A Cross-Site Scripting (XSS) vulnerabilities was found in
BioTime BioTime - < 8.5.3  Build:20200816.447 that could lead to local file read when you try to export injected payload using pdf
the pdf generator will simply execute the javascript code inside the injected payload that can lead to Local file read

Vulenrable models:

1- When reassigning an employee
Path:/personnel/resign/action/
Parameter: reason

2- When send private message
path:/iclock/privatemessage/action/
parameter:content

3-When adding manual log
path:/att/manuallog/action/
parameter:reason

4-When adding timetable
path:/att/timeinterval/action/
parameter:alias

5-When adding shift
path:/att/attshift/add/
parameter:alias
This got reflected when adding department schedule and employee schedule

6-Xss when adding leave,manuallog,overtime,training
same parameter (reason)

7-When adding holiday
path:/att/holiday/action/
parameter:alias

3. Impact

Due to the lack of proper encoding on the affected parameters susceptible to
XSS, arbitrary JavaScript could be executed by pdf generator's headless browser that could lead to local file read

4.   Solution

Users can upgrade to 8.5.4 or later.
Please find latest version from the Zkteco main website or they provide hardcopy of the software when you buy an Iface or any attendance de
You install versions higher than 8.5.3
```