FaceSentry Access Control System 6.4.8 Reflected Cross Site Scripting

2019.07.02

Credit: **LiquidWorm (https://cxsecurity.com/author/LiquidWorm/1/)**

Risk: **Low**

Local: **No**

Remote: **Yes**

CVE: **N/A**

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

FaceSentry Access Control System 6.4.8 Reflected Cross-Site Scripting

Vendor: iWT Ltd.
Product web page: http://www.iwt.com.hk
Affected version: Firmware 6.4.8 build 264 (Algorithm A16)
Firmware 5.7.2 build 568 (Algorithm A14)
Firmware 5.7.0 build 539 (Algorithm A14)

Summary: FaceSentry 5AN is a revolutionary smart identity management appliance that offers entry via biometric face identification, contactless smart card, staff ID, or QR-code. The QR-code upgrade allows you to share an eKey with guests while you're away from your Office and monitor all activity via the web administration tool. Powered by standard PoE (Power over Ethernet), FaceSEntry 5AN can be installed in minutes with only 6 screws. FaceSentry 5AN is a true enterprise grade access control or time-and-attendance appliance.

Desc: FaceSentry is vulnerable to multiple cross-site scripting vulnerabilities. This issue is due to the application's failure to properly sanitize user-supplied input thru the 'msg' parameter

```
(GET) in pluginInstall.php script. An attacker may leverage any
of the cross-site scripting issues to have arbitrary script code
executed in the browser of an unsuspecting user in the context
of the affected site. This may facilitate the theft of cookie-base
d
authentication credentials, phishing, as well as other attacks.

Tested on: Linux 4.14.18-sunxi (armv7l) Ubuntu 16.04.4 LTS (Xenial
Xerus)
           Linux 3.4.113-sun8i (armv7l)
           PHP/7.0.30-0ubuntu0.16.04.1
           PHP/7.0.22-0ubuntu0.16.04.1
           lighttpd/1.4.35
           Armbian 5.38
           Sunxi Linux (sun8i generation)
           Orange Pi PC +


Vulnerability discovered by Gjoko 'LiquidWorm' Krstic
                            @zeroscience


Advisory ID: ZSL-2019-5527
Advisory URL: https://www.zeroscience.mk/en/vulnerabilities/ZSL-20
19-5527.php


28.05.2019

--

http://192.168.11.1/pluginInstall.php?msg=%22%3E%3Cmarquee%3Etesti
ngus%3C/marquee%3E
http://192.168.11.1/pluginInstall.php?msg=Reflected</div><script>c
onfirm('XSS.')</script>
```

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2019070017)

Post

Vote for this issue: 0 0

50% 50%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)