FaceSentry Access Control System 6.4.8 Remote Root Exploit

Title: FaceSentry Access Control System 6.4.8 Remote Root Exploit
Advisory ID: ZSL-2019-5525
Type: Local/Remote
Impact: System Access
Risk: (5/5)
Release Date: 30.06.2019

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.

Description

FaceSentry suffers from an authenticated OS command injection vulnerability using default credentials. This can be exploited to inject and execute arbitrary shell commands as the root user via the 'strInIP' POST parameter in pingTest PHP script.

```
/pingTest.php:
--------------
if (!isAuth('TestTools','R')){
echo "No Permission";
include("footer.php");
exit;
}

if(isset($_POST["strInIP"])){
$strInIP = $_POST["strInIP"];
}else{
$strInIP = "";
}

$strOperationResult = "";
if ($strInIP != ""){

$out = array();
exec("sudo ping -c 4 $strInIP",$out);
$result = "";
foreach($out as $line){
$result = $result.$line."<br>";
}
```

Vendor

iWT Ltd. - 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)

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 +

Vendor Status

[28.05.2019] Vulnerability discovered.
[29.05.2019] Vendor contacted.
[12.06.2019] No response from the vendor.
[13.06.2019] Vendor contacted.
[27.06.2019] No response from the vendor.
[28.06.2019] Vendor contacted.
[29.06.2019] No response from the vendor.
[30.06.2019] Public security advisory released.

PoC

biometac.py

Credits

Vulnerability discovered by Gjoko Krstic - <gjoko@zeroscience.mk>

References

[1] https://www.exploit-db.com/exploits/47066
[2] https://packetstormsecurity.com/files/153490
[3] https://cxsecurity.com/issue/WLB-2019070014

[4] https://exchange.xforce.ibmcloud.com/vulnerabilities/163187
[5] https://github.com/zeroscience/advisory/blob/master/ZSL-2019-5525
[6] https://raw.githubusercontent.com/zeroscience/advisory/master/ZSL-2019-5525
[7] https://cve.mitre.org/cgi-bin/cvename.cgi?name=2020-21999
[8] https://nvd.nist.gov/vuln/detail/CVE-2020-21999
[9] https://security-tracker.debian.org/tracker/CVE-2020-21999
[10] https://www.tenable.com/cve/CVE-2020-21999
[11] https://cve.report/CVE-2020-21999

Changelog

[30.06.2019] - Initial release
[04.07.2019] - Added reference [1], [2], [3], [4], [5] and [6]
[19.06.2021] - Added reference [7], [8], [9], [10] and [11]

Contact

Zero Science Lab

Web: http://www.zeroscience.mk
e-mail: lab@zeroscience.mk

- **Rete mirabilia**
- **We Suggest**
- **Profiles**
- Site Meter