NETTITUDE
AN LRQA COMPANY

Penetration Testing Technical Report

Prepared For: AKUVOX
Target: X915S
Author: Patrick Matthews
Date: 12 January 2024
Version: 2.0

Confidential Security Document

Contents

1 Document Distribution List

Nettitude	Name	Title
	Patrick Matthews	Security Consultant
	Dalton Wright	Security Consultant
	Fan Zhang	Account Manager
	Vanessa Santos	Security Consultant

Akuvox	Name	Title
	Jiajing Li	Product Assistant

2 Revision History

Version	Issue Date	Issued by	Comments
0.1	18 October 2023	Patrick Matthews	Initial Draft
0.2	27 October 2023	Dalton Wright	Quality Assurance
1.0	29 October 2023	Patrick Matthews	Final version
1.1	9 January 2024	Patrick Matthews	Initial Draft - Retest
1.2	12 January 2024	Vanessa Santos	Quality Assurance
2.0	12 January 2024	Patrick Matthews	Final version

3 Engagement Particulars

Background

This report serves as technical documentation for the recent penetration test performed for Akuvox by Nettitude. For a high-level assessment of the tested environment, please refer to the accompanying management report.

Engagement Activities and Rules

Nettitude was commissioned to conduct a remediation valuation engagement during the time period of 8 January to 9 January 2024 against the findings of the September/October 2023 engagement. The original testing engagement was conducted from 25 September to 18 October 2023.

All testing for both engagements was conducted from Nettitude US office, located in New York State.

Nettitude adhered to the following rules:

- Grey box physical device testing on a production device.
- OWASP IoT, Web and secure coding practices were to be thoroughly tested.
- No access was provided to the Smartplus cloud or mobile applications.
- Akuvox secondary configuration tools such as the IP Scanner were not utilized during this engagement.
- Verification that all public CVE's have been remediated.

Scope

Akuvox tasked Nettitude to perform a grey-box security assessment of the scope detailed in the following table:

Component	Description
X915S Smart Intercom	Firmware version - 2915.30.10.201 Hardware version – 2915.1.0.0

Testing Windows Observations and Constraints

The time frame provisioned for the completion of this retest engagement was adequate.

Original EngagementTesting Windows Observations and Constraints

The time frame provisioned for the completion of this engagement was adequate. The engagement consultant utilized the Smartplus and My Mobile key android applications to identify X915S device service end points.

No access was provided to the Smartplus cloud service so certain features related to that offering could not be fully dynamically tested, such as the Bluetooth feature. The engagement consultant did test all features based on dynamic and/or static source code review.

Findings Summary

Nettitude identified a total number of 5 findings during the engagement remain after remediation testing. The following table shows the categorization by severity:

0	0	0	2	3
Critical	High	Medium	Low	Info.

4 Findings

4.1 Physical Controls

Component	Description	CVSS	Severity	Ref.
X915S Hardware version 2915.1.0.0	Debugging Ports Enabled	6.4	Low	5.1
X915S Hardware version 2915.1.0.0	Lack of Security Screws	0.0	Informational	5.2
X915S Hardware version 2915.1.0.0	Lack of Smudge Attack Protections	0.0	Informational	5.3
X915S Hardware version 2915.1.0.0	Tamper Switch Weaknesses	0.0	Informational	5.4

4.2 Interface Controls

Component	Description	CVSS	Severity	Ref.
https://172.16.1.12/api/web/system/info	Insecure Direct Object Reference	3.7	Low	**Error! Reference source not found.**

4.3 Firmware

The downloaded firmware was encrypted and the ADB debug interface was disabled limiting the ability to access the devices APK's. The other debug ports did not provide a console to interact with the Android Operating System.

5 Analysis: Physical Controls

5.1 Low: Debugging Ports Enabled

CVSS 3.1	
Score:	3.0
Vector:	CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

5.1.1 Description of the Issue

Debugging ports allow threat actors to be able to easily interact with the firmware to conduct a range of attacks, including gaining a command session to download the unencrypted firmware running within memory.

Board ports such as the JTAG (Joint Test Action Group), SWD (serial Wire Debug), and UART (Universal Asynchronous Receiver-Transmitter) provide developers a means to interact with a device board. A JTAG port allows for modifying the memory, and CPU registry values; SWD and UART provide serial console access to interact with the running firmware.

The X915X device was found to have a number of debug ports available on the devices boards. A threat actor with physical access to the device can use these ports for interacting with the device.

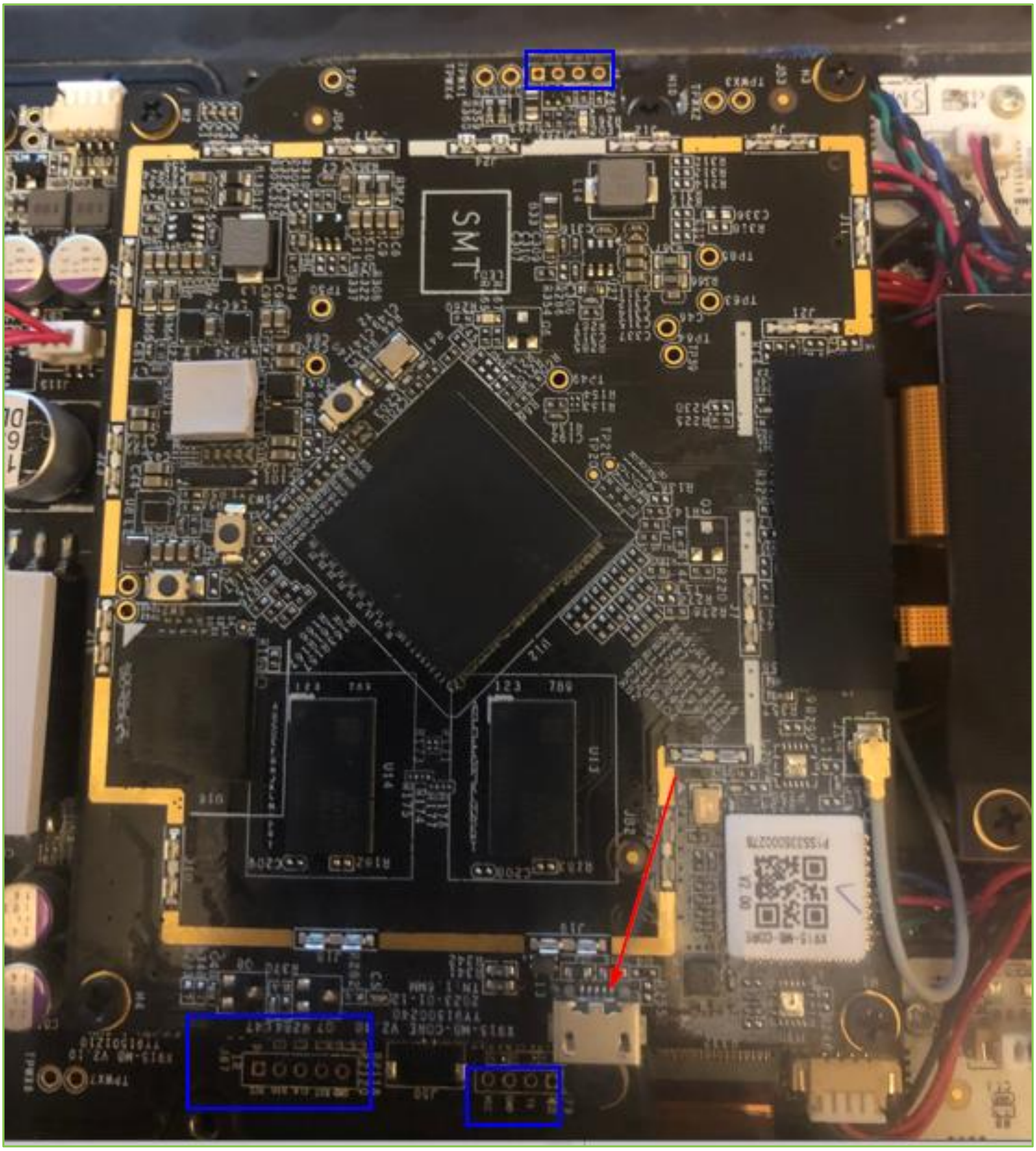
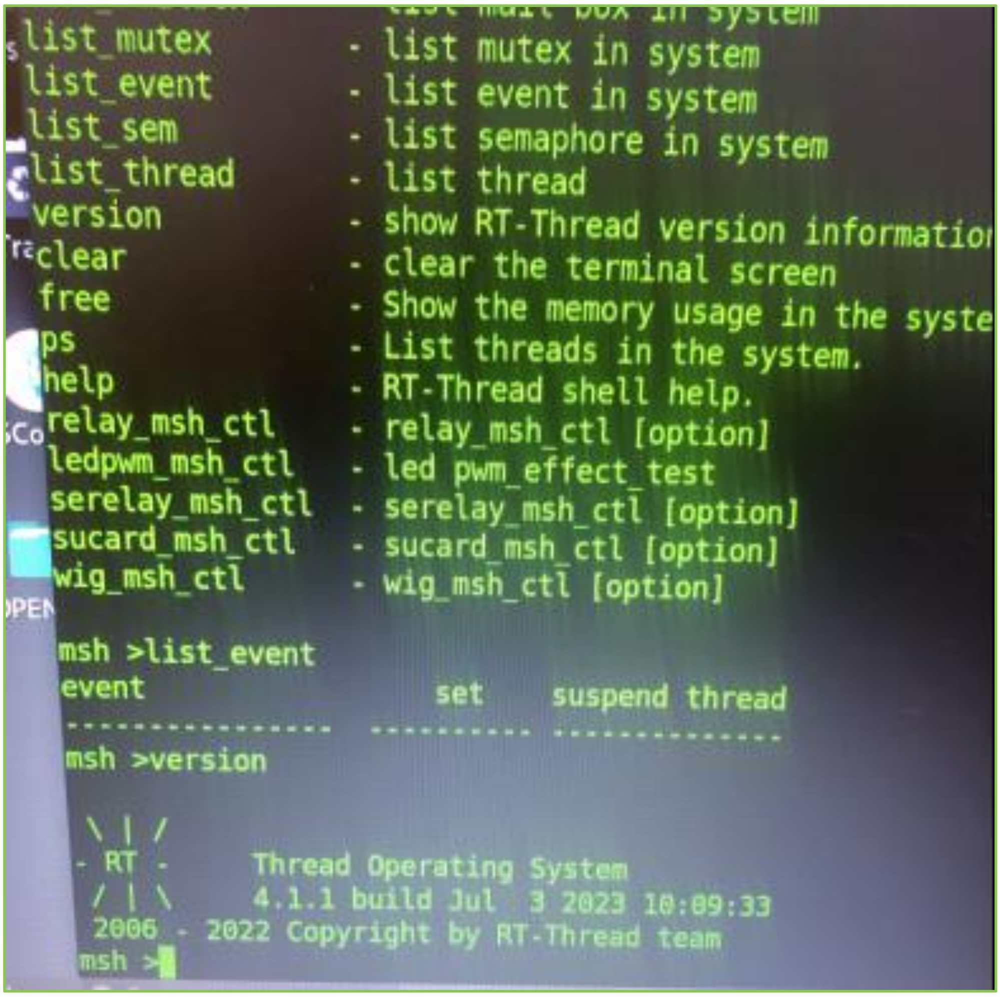


Figure 1 : Debug Interfaces



```
list_mutex         - list mutex in system
list_event         - list event in system
list_sem           - list semaphore in system
list_thread        - list thread
version            - show RT-Thread version informatio
clear              - clear the terminal screen
free               - Show the memory usage in the syste
ps                 - List threads in the system.
help               - RT-Thread shell help.
relay_msh_ctl      - relay_msh_ctl [option]
ledpwm_msh_ctl     - led pwm_effect_test
serelay_msh_ctl    - serelay_msh_ctl [option]
sucard_msh_ctl     - sucard_msh_ctl [option]
wig_msh_ctl        - wig_msh_ctl [option]

msh >list_event
event                   set    suspend thread
---------------    ---------- -------------
msh >version

 \ | /
- RT -     Thread Operating System
 / | \     4.1.1 build Jul  3 2023 10:09:33
 2006 - 2022 Copyright by RT-Thread team
msh >
```

Figure 2 : Access to Threat Operating System

The ADB port was found to be disabled. The remaining debug ports will require a manufacturing change were the ports are filled or circuits disabled.

5.1.2 Affected Components

- X915S Hardware version 2915.1.0.0

5.1.3 Nettitude Recommends

1. Disable board UART, I2C, and JTAG debug ports by filling connectors or disabling circuit.

5.2 Informational: Lack of Security Screws

CVSS 3.1	
Score:	0.0
Vector:	CVSS:3.1/AV:P/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N

5.2.1 Description of the Issue

OWASP top 10 IoT concerns – Lack of physical hardening. Physical security weaknesses are present when an attacker can disassemble a device to easily access the device and any data stored on that medium.

Security screws feature a special head that makes them harder to remove. Security screw heads are designed to be incompatible with standard slotted or Phillips screwdrivers. Some manufacturers have created custom screws that only their approved vendors can acquire them. Security screws have a number of purposes including discouraging tempering and making theft or misuse harder.

The X915S devices were found to only use standard Phillips head screws for the backing plate and back cover allowing for easy access to the device's debugger ports. The device does ship with two torx screws for mounting the device to the mounting box.

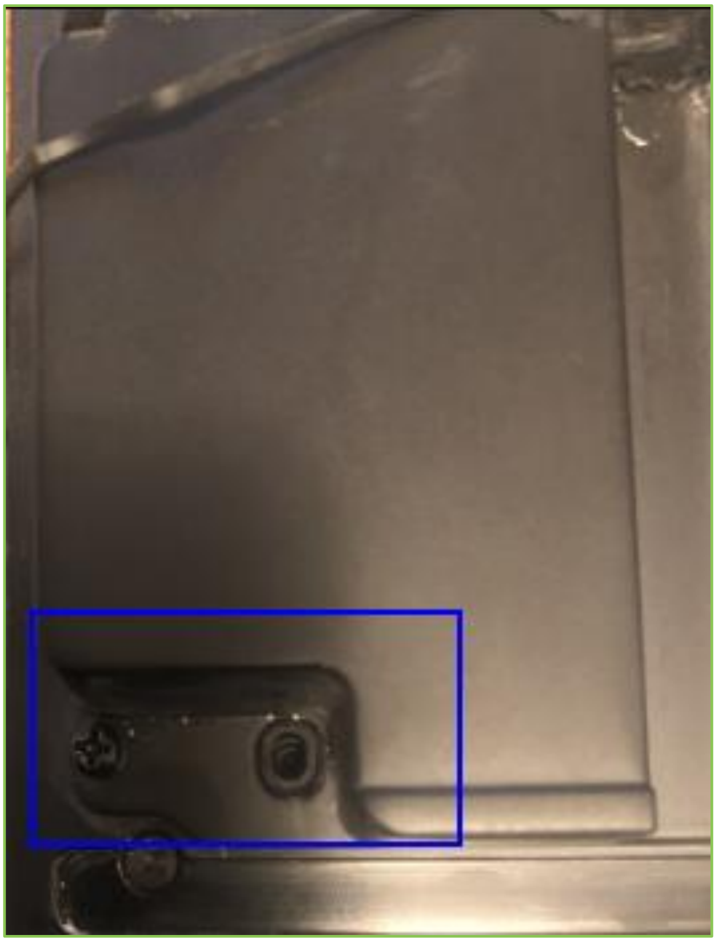


Figure 3 : Screw used to secure backplate

5.2.2 Affected Components

- X915S Hardware version 2915.1.0.0

5.2.3 Nettitude Recommends

1. Implement the use of security screws or sonically seal the device back plate.

5.2.4 Further Reading

- OWASP IoT Top 10 – https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10
- ISACA Security Issues in IoT – https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/security-issues-in-iot-challenges-and-countermeasures

5.3 Informational: Lack of Smudge Attack Protections

CVSS 3.1	
Score:	0.0
Vector:	CVSS:3.1/AV:P/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N

5.3.1 Description of the Issue

In 2020 the University of Pennsylvania introduced the concept of an information extraction attack against touchscreen devices that allows a threat actor to discern a password or access PIN called the smudge attack. This attack uses fingerprints or smudge marks on a touchscreen to figure out a 4-character numeric number by brute force guessing the PIN.

A threat actor with physical access to the device can coat the device’s keypad or screen with a matter that will allow them to see what numbers are pressed. Another version of this side channel attack is shoulder surfing or observing the device as a PIN is entered. This attack is very effective on devices that only have a keypad for entry and does not require a second form of identification.

While Android and Apple do not offer a random numeric keyboard natively with their operating systems, several open-source projects provide this functionality. The X915S devices were found not to use a random numeric keyboard for PIN access.

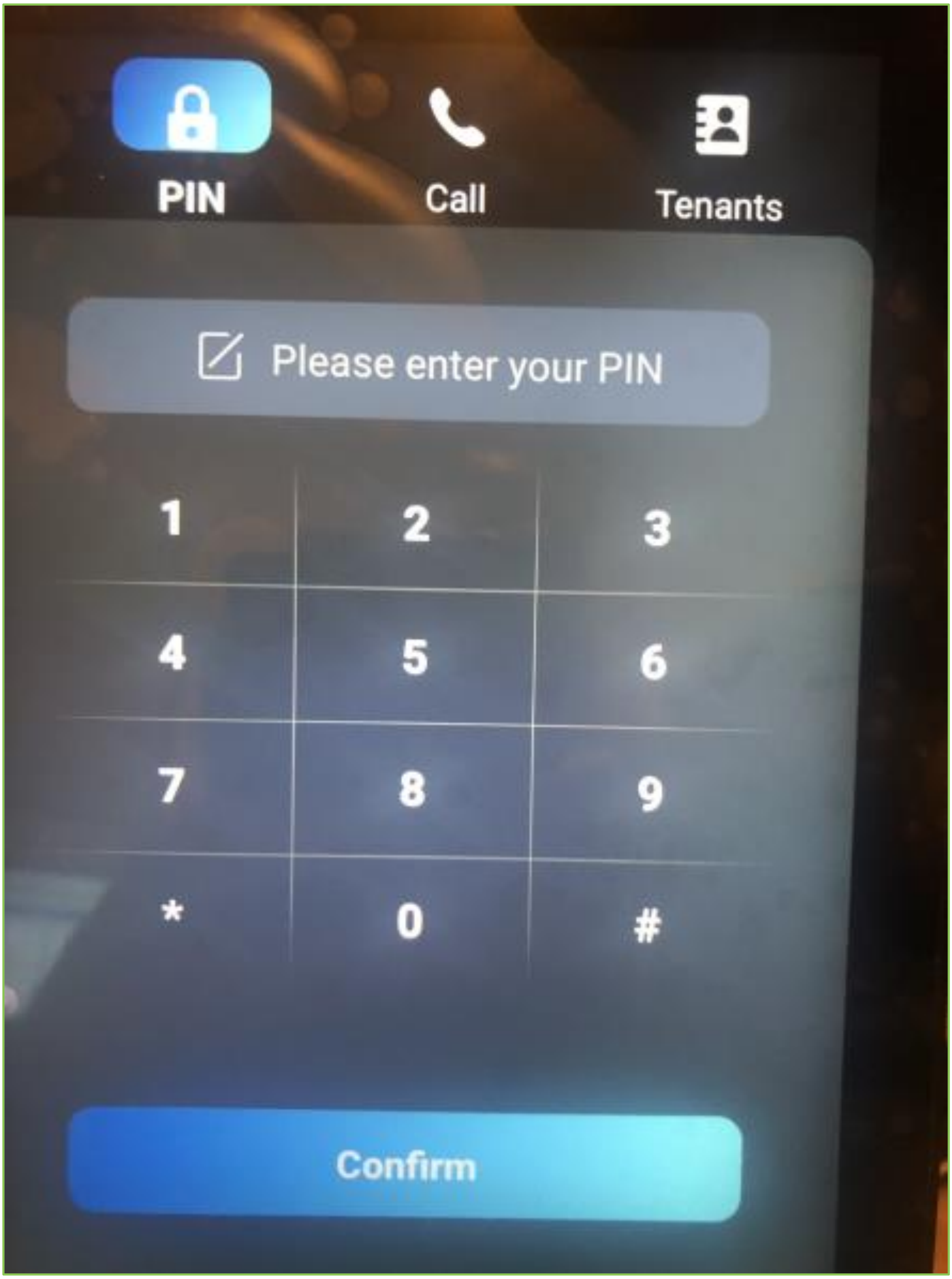


Figure 4 : PIN entry keyboard

5.3.2 Affected Components

- X915S Hardware version 2915.1.0.0

5.3.3 Nettitude Recommends

1. Implement a numeric keyboard for PIN entry that places the numbers in random order each time it is displayed.

5.3.4 Further Reading

- International Journal of Information and Computer Security – https://www.inderscience.com/offer.php?id=115345
- Homeland Security News Wire – Defending against Smudge Attacks – https://www.homelandsecuritynewswire.com/dr20210614-defending-against-smudge-attacks
- eweek - https://www.eweek.com/security/smartphone-security-vulnerable-to-touch-screen-smudges-researchers-report/

5.4 Informational: Tamper Switch Weaknesses

CVSS 3.1	
Score:	0.0
Vector:	CVSS:3.1/AV:P/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N

5.4.1 Description of the Issue

Tamper protection is a security feature designed to make a device or application resistant to unauthorized access or modification. Tamper protection is important in ensuring a product's quality and integrity and providing transparency and accountability.

The X915S device has a pressure tamper switch placed on the back of the device. The tamper switch can be enabled through the web interface or the device's configuration screen. Once activated the tamper switch causes the device to emit an alert sound unit the power is cut or the disarm code is entered. In reviewing the device's Phone code about the tamper switch and setting up an email account, it does not appear the X915X device sends out a special notification when the tamper switch is activated. This feature may be integrated into the cloud application.

The tamper switch 17ressuree was found to be very good where once depressed the alarm will activate with a few centimeters of movement. Given the placement of the tamper switch within a mounting box, it seems unlikely that a piece of material could be inserted to affect the activation of the tamper switch.

However, the tamper switch activation did not have a means to remain set between reboots nor was the device stopped from booting once the tamper switch was activated. This could allow a threat actor to reboot the device to turn off the alerting. Requiring the disarm code to be entered, for a device that had a tamper switch activated, will help protect against offline attacks where the unit is taken to access the device's configuration data.

Additionally, no alerting was detected to notify that the tamper switch was activated by relay activation (power reading) or at the host set in the FTP and Email notification parameters.

5.4.2 Affected Components

- X915S Hardware version 2915.1.0.0

5.4.3 Nettitude Recommends

- Implement automatic alerting logging on tamper switch activation.

- Disable device reboot, via software menus, on tamper switch activation.

5.4.4 Further Reading

- IoT times - https://iot.eetimes.com/tamper-resistant-elements-crucial-for-iot-security/
- IoT SAFE - https://www.gsma.com/iot/iot-safe/

  Tech Target - https://www.techtarget.com/iotagenda/tip/Dont-forget-IoT-physical-security-when-planning-protection

6 Analysis: Interface Controls

6.1 Low: Insecure Direct Object Reference

CVSS 3.1	
Score:	3.7
Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

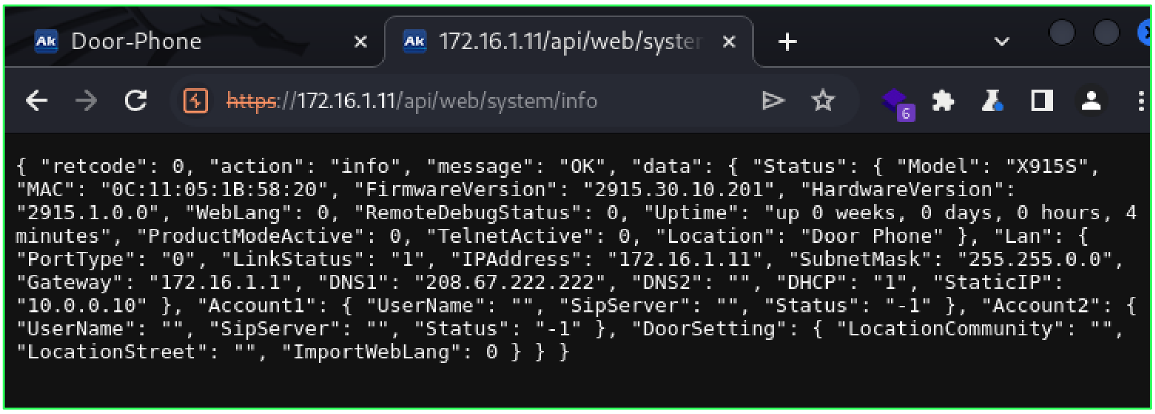
6.1.1 Description of the Issue

An insecure direct object reference vulnerability was found within the targeted application. This allowed for viewing information that was not intended for that user.

The application suffered from an access control issue that allows an anonymous user to access certain pages and/or function of the application that is not intended for that user. Insecure object reference usually occurs when an application provides access to objects or pages via user-supplied input.

A malicious user can make use of this issue to access certain records that he/she is not intended to view. In some more serious situations, it is also possible to update records based on the direct object reference in a specific request. The reason this is often accessible is that the application is not performing sufficient authorization checks for this page or object.

In this instance, the /api/web/system/info page is available to anonymous users allowing them to view certain information for further attacks. As seen below the page: /api/web/system/info provides anonymous threat actors with the MAC address, Firmware version, network information, and SIP details. All of which could assist in further attacks against the device or the company/residence that use the X915S device.



Door-Phone
172.16.1.11/api/web/syster
https://172.16.1.11/api/web/system/info

```
{ "retcode": 0, "action": "info", "message": "OK", "data": { "Status": { "Model": "X915S",
"MAC": "0C:11:05:1B:58:20", "FirmwareVersion": "2915.30.10.201", "HardwareVersion":
"2915.1.0.0", "WebLang": 0, "RemoteDebugStatus": 0, "Uptime": "up 0 weeks, 0 days, 0 hours, 4
minutes", "ProductModeActive": 0, "TelnetActive": 0, "Location": "Door Phone" }, "Lan": {
"PortType": "0", "LinkStatus": "1", "IPAddress": "172.16.1.11", "SubnetMask": "255.255.0.0",
"Gateway": "172.16.1.1", "DNS1": "208.67.222.222", "DNS2": "", "DHCP": "1", "StaticIP":
"10.0.0.10" }, "Account1": { "UserName": "", "SipServer": "", "Status": "-1" }, "Account2": {
"UserName": "", "SipServer": "", "Status": "-1" }, "DoorSetting": { "LocationCommunity": "",
"LocationStreet": "", "ImportWebLang": 0 } } }
```

Figure 5 : system info page

6.1.2 Affected Components

- https://172.16.1.12/api/web/system/info

6.1.3 Nettitude Recommends

1. Implement per user or session indirect object references with access reference map.
2. Carry out functional testing to ensure sufficient access controls on each role/group.
3. Avoid revealing private objects references to users, e.g. file names, internal URL's.

6.1.4 Further Reading

- OWSAP - https://owasp.org/Top10/A01_2021-Broken_Access_Control/

7 Appendix

7.1 Original Finding Physical Controls

Component	Description	CVSS	Severity	Status
X915S Hardware version 2915.1.0.0	Debugging Ports Enabled	6.4	Medium	Partly Remediated
X915S Hardware version 2915.1.0.0	Lack of Security Screws	5.9	Medium	Severity Change to Reflect Best Practice
X915S Hardware version 2915.1.0.0	Exposed Factory Reset Switch	4.2	Medium	Remediated
X915S Hardware version 2915.1.0.0	Lack of Smudge Attack Protections	2.4	Low	Severity Change to Reflect Best Practice
X915S Hardware version 2915.1.0.0	Tamper Switch Weaknesses	2.4	Low	Severity Change to Automatically Enabled

7.2 Original Finding Interface Controls

Component	Description	CVSS	Severity	Status
rtsp://device ip/live/ch00_0 http://device ip:8080/jpeg.cgi http://device ip:8080/picture.cgi http://device ip:8080/picture.jpg http://Device_IP/#/SurveillanceLiveStream	Basic Authentication over HTTP	8.7	High	Remediated
http://X915_Device_IP/	Browser Based Policy Control	8.1	High	Remediated
http://X915_Device_IP/ http://X915_Device_IP/api/ http://X915_Device_IP/fcgi/	Cleartext Submission of Passwords	7.5	High	Remediated
rtsp://device ip/live/ch00_0 http://device ip:8080/jpeg.cgi http://device ip:8080/picture.cgi http://device ip:8080/picture.jpg http://Device_IP/#/SurveillanceLiveStream	No Account Lockout on Certain End Points	6.5	Medium	Remediated
http://X915_Device_IP/	Weak Password Policy	6.5	Medium	Remediated
Refer to finding	Session Token in URL	5.9	Medium	Remediated
http://Device_IP/api/web/login	Account Lockout Bypass	4.3	Medium	Remediated

http://X915S_Device_IP/api/web/set https://172.16.1.12/api/web/system/info	Insufficient Access Control	4.3	Medium	Remediated
https://172.16.1.12/api/web/system/info	Insecure Direct Object Reference	3.7	Low	Not Remediated

7.3 Original Finding Firmware

Component	Description	CVSS	Severity	Status
com/akuvox/phone/defined/BleDefined.java com/akuvox/phone/mvvm/model/VerticalCallModel.java com/akuvox/phone/mvvm/model/VerticalTopModel.java com/akuvox/phone/utils/StringBaseTools.java	Hardcoded Credentials	7.7	Medium	Remediated
https://Device_IP/api/web/contact/set https://Device_IP/api/web/group/set https://172.16.1.13/api/web/contact/import	SQL Injection	6.5	Medium	Remediated
2915.30.10.4	Outdated Component - Busybox	5.6	Medium	Remediated
com/akuvox/phone/database/face/ImportDBHelper.java	Lack of Parameterized SQL Statements	4.7	Medium	Remediated
X915X	Lack of App Allowlist	4,7	Medium	Remediated
com/example/ftreadid/HS3DES.java env.sh rundemo.sh saveCfg.sh	Legacy / Unused Code in Production	2.9	Low	Remediated

/app/factory/DOOR/Setting.conf	Cleartext Password in Legacy File	0.0	Informational	Remediated
Refer to finding	Missing Binary Shared Library Protections	0.0	Informational	Remediated
Refer to finding	No Obfuscation APKS	0.0	Informational	Remediated

7.4 Vulnerability Severity Methodology

We use CVSS (Common Vulnerability Scoring System) version 3.1 to determine the severity of vulnerabilities we report. This is a widely used system which allows us to report in a consistent and actionable manner. The score ranges from 0 – 10, with higher numbers representing higher severity vulnerabilities.

Multiple factors contribute to the final CVSS score of each vulnerability. We determine a series of exploitability and impact metrics, which combine to create a base score. Depending on the level of information we have about the vulnerability and the environment it exists in, we may opt to apply some modifiers to that base score, leading to an altered final score.

The following table shows how each quantitative score is associated with a qualitative rating ranging from critical down to informational.

Severity Rating	CVSS Score	Typical Vulnerability Characteristics
CRITICAL	9.0 – 10.0	Exploitation is likely to be easy and repeatable. It is also likely to result in significant system access. There is potential for significant business impact.
HIGH	7.0 – 8.9	Exploitation is likely to be difficult and require specific user interactions or attack timing. Following exploitation, elevated system access is likely. Business impact is likely to be meaningful.
MEDIUM	4.0 – 6.9	Exploitation is difficult due for reasons such as complexity, location requirements, specific user interactions, etc. Successful exploitation is likely to lead to normal or limited system access. Business impact is likely to be low.
LOW	0.1 – 3.9	Exploitation is unlikely and resultant system access is low. Business impact is negligible. This may be more useful in tandem with one or more other vulnerabilities rather than a standalone one.

INFORMATIONAL	0.0	No vulnerability exists, but this is still a noteworthy finding. This may have the potential to evolve a vulnerability in future. It may represent an opportunity for improvement.

CVSS scores are calculated based on one or more of the following three metric groups: base metrics, temporal metrics, and environmental metrics. These are described in more detail below.

7.4.1 Base Metrics

The base score represents the intrinsic characteristics of each vulnerability, which remain the same over time and across all environments. The base score is comprised broadly of two metrics; the exploitability of a vulnerability and the impact it may have.

The exploitability elements reflect the ease with which the vulnerability can be exploited. Not all vulnerabilities are equally exploitable. For example, some may require specific user interactions or attack positioning, while others may be exploitable from anywhere in the world with no dependencies. The impact elements describe the immediate consequences of successful exploitation, in terms of confidentiality, integrity, and availability.

7.4.2 Temporal Metrics

The temporal metrics modify the severity of each vulnerability based on factors that change over time, such as the availability and maturity of exploit code, software patches, etc. Temporal metrics are included in our CVSS calculation when we have sufficient information to include them.

7.4.3 Environmental Metrics

Environmental Metrics modify the base score based on factors which are unique to the relevant environment, for example the existence of mitigating factors and the risk requirements of the environment. Environmental metrics are rarely included in our CVSS calculations due to insufficient information about these factors in most engagements.

7.5 Penetration Testing Methodology

Nettitude has a series of approaches for conducting Penetration Tests.

7.5.1 Black Box Testing

In a Black Box test, the client does not provide Nettitude with any information about their infrastructure. For internal tests the customer may provide no more than a network point for the tester to connect in to. For external tests, this may simply be a URL or even just the company name that is in scope for assessment.

Nettitude is tasked with testing the environment as if they were an attacker with no information about the infrastructure or application logic that they are testing. Black Box tests tend to take longer to commission than White Box tests and may identify less exposures and vulnerabilities than those of White Box tests.

7.5.2 White Box Testing

In a White Box test, clients provide Nettitude with information about the applications and infrastructure prior to the commencement of the testing engagement. Usernames and Passwords are provided to Nettitude's testing team as part of the engagement, and the client may provide Nettitude's consultants with access to source code. In this type of testing engagement, Nettitude works closely with the client to perform the assessment. These types of tests tend to gain deeper understanding of the application and infrastructure logic, and may generate highly comprehensive test results.

7.5.3 Grey Box Testing

A Grey Box test is a blend of Black Box testing techniques and White Box testing techniques. In Grey Box testing, clients provide Nettitude with snippets of information to help with the testing procedures. This results in a highly focused test.

Nettitude Penetration Testing Services

www.nettitude.com/penetration-testing/

NETTITUDE

AN LRQA COMPANY

UK Head Office
Jephson Court, Tancred
Close, Leamington Spa,
CV31 3RZ

Americas
50 Broad Street,
Suite 403, New York,
NY 10004

Asia Pacific
18 Cross Street,
#02-101, Suite S2039,
Singapore 048423

Europe
Leof. Siggrou 348
Kallithea, Athens, 176 74
+30 210 300 4935

Follow Us

solutions@nettitude.com
www.nettitude.com