



RESEARCH
HARDEN
SECURE
A SAFER TOMORROW

BRIDGING TRUST TO ROOT: OFFENSIVE RESEARCH INTO INDUSTRIAL COUPLERS



Omkar Mali

SECURITY RESEARCHER | HARDWARE & OT SECURITY



INDUSTRIAL SECURITY
FOR A RESILIENT TOMORROW

ABOUT ME

PEOPLE
TECHNOLOGY
A SAFER TOMORROW



SAME CURIOSITY.
DIFFERENT BATTLEFIELDS.



Independent Hardware Security Researcher
Exploring hardware, firmware and real-world systems.



Former IBM X-Force Red Team Member
Hands-on experience in offensive security and red teaming.



International Conference Speaker and Trainer
Sharing research, conducting workshops and training globally.



Passionate About UAV, IoT, Automotive & Firmware Security
From drones to vehicles, from silicon to systems.



Part-time Gamer
Because even hackers need a respawn.



Love Snipers
Patience, precision and the thrill of the perfect shot.

CURRENTLY PLAYING



“EXPLORE
BREAK
LEARN
BUILD A SAFER TOMORROW

SECURING
CRITICAL SYSTEMS
FOR A SUSTAINABLE FUTURE

WHY THIS RESEARCH MATTERS?



RENEWABLE ENERGY ADOPTION IS RAPIDLY INCREASING

Especially in developing nations, driven by sustainability goals and energy demand.



CHINESE-MANUFACTURED COUPLERS ARE COST-EFFECTIVE

Widely available and deployed across renewable energy infrastructure due to affordability and accessibility.



HOWEVER, ACCELERATED DIGITIZATION INTRODUCES NEW RISKS

Increased connectivity, remote management, and protocol integration expand the attack surface.



OUR RESEARCH INVESTIGATES REAL-WORLD VULNERABILITIES

We analyze security weaknesses in couplers through hands-on testing and real-world scenarios.



FOCUS AREAS: DATA PRIVACY, OPERATIONAL SECURITY, AND NATIONAL INFRASTRUCTURE THREATS

Ensuring a more secure and resilient renewable energy ecosystem.

RESEARCH | SECURITY | RESILIENT INFRASTRUCTURE

SECURING
CRITICAL SYSTEMS
FOR A SUSTAINABLE
TOMORROW

CLEANER
ENERGY
STRONGER
TOMORROW



PEOPLE
TECHNOLOGY
A SAFER TOMORROW

WHAT IS A COUPLER?

A SMALL DEVICE. A CRITICAL ROLE.



DEFINITION

A device that connects two systems, enabling communication between different protocols or standards.



IN CONTEXT

In renewable energy, couplers facilitate communication between field devices and control systems.



IMPORTANCE

Ensure seamless data flow and operational control across the energy infrastructure.

PEOPLE
TECHNOLOGY
A SAFER TOMORROW

CONNECTING
SYSTEMS
POWERING
A CLEANER TOMORROW



SECURING
CRITICAL SYSTEMS
FOR A SUSTAINABLE FUTURE

RESEARCH | SECURITY | RESILIENT INFRASTRUCTURE

HOUSEHOLD SOLAR PHOTOVOLTAIC ENERGY

CLEAN ENERGY. CONNECTED SYSTEMS. NEW ATTACK SURFACES.

In the application of household photovoltaic energy storage, a gateway device can upload the data collected by energy conversion equipment such as the inverter and energy storage system (e.g., battery pack) to a monitoring center, so that users can conveniently and flexibly monitor and manage the operation of the photovoltaic system in real time.



Solar Panels

Generate DC electricity from sunlight.



Inverter

Converts DC to AC and communicates system data.



Energy Storage

Battery packs store excess energy for later use.



Monitoring

Real-time data collection and remote monitoring.

SUSTAINABLE ENERGY | CONNECTED INFRASTRUCTURE | HIGHER RESILIENCE

PEOPLE
TECHNOLOGY
A SAFER TOMORROW



CLEANER HOMES
STRONGER TOMORROW

MEDICAL DEVICE DATA TRANSMISSION SOLUTION

CONNECTED CARE. REAL-TIME INSIGHTS. BETTER OUTCOMES.

The medical equipment transmits the collected data to the cloud server in real time through Wi-Fi network. Users can quickly complete the collection, storage and analysis of important data.



Real-Time Data Transmission

Continuous and reliable data upload over Wi-Fi.



Secure & Private Cloud

Encrypted data transmission and secure storage.



Centralized Monitoring

Access and analyze data from anywhere, anytime.



Improved Patient Care

Faster insights for better diagnosis and response.



Remote control center

Private Cloud
(Internet)



Router

WiFi



IoT Gateway

RS232/485



Patient Monitor



Infusion Pump



Imaging Device

Medical Devices

HEALTHIER PEOPLE | SMARTER SYSTEMS | A SAFER TOMORROW



CONNECTED MEDICAL DEVICES
FOR A HEALTHIER TOMORROW

PEOPLE
TECHNOLOGY
A SAFER TOMORROW

COMMON VULNERABILITIES

TYPICAL SECURITY ISSUES FOUND IN INDUSTRIAL COUPLERS / PROTOCOL GATEWAYS

PEOPLE
TECHNOLOGY
A SAFER TOMORROW



WEAK / DEFAULT CREDENTIALS

Factory credentials, weak passwords or lack of account management.



EXPOSED MANAGEMENT INTERFACES

HTTP/HTTPS, SSH, Telnet or proprietary admin services accessible over the network.



INSECURE PROTOCOL TRANSLATION

Insufficient validation when bridging different protocols (e.g., Modbus, IEC 104, DNP3, proprietary).



UNENCRYPTED COMMUNICATIONS

Sensitive data transmitted without encryption, making it susceptible to eavesdropping or manipulation.



FIRMWARE VULNERABILITIES

Outdated firmware, known CVEs, or insecure third-party components.



INSECURE FIRMWARE UPDATES

Missing signature verification, integrity checks or secure update mechanisms.



DEBUG INTERFACES EXPOSED

UART, JTAG, SWD, SPI or other test points accessible physically.



SENSITIVE DATA EXPOSURE

Credentials, cryptographic keys, configuration files or other secrets stored in plaintext.



MISSING INPUT VALIDATION

Malformed or unexpected messages can cause crashes, memory corruption or unexpected behavior.



DENIAL OF SERVICE

Resource exhaustion or crafted traffic can disrupt communications and operational control.



INSUFFICIENT ACCESS CONTROL

Lack of role-based access, excessive privileges or insecure default configuration (unnecessary services/ports enabled).



SECURITY BY DESIGN IS CRITICAL.

HARDEN, MONITOR AND REGULARLY ASSESS INDUSTRIAL COUPLERS TO PREVENT MISUSE AND ENSURE RESILIENT OPERATIONS.

FROM ACCESS TO IMPACT

A TYPICAL ATTACK PATH AGAINST AN INDUSTRIAL COUPLER / PROTOCOL GATEWAY

SECURING
CRITICAL SYSTEMS
FOR A SUSTAINABLE
FUTURE

1 INITIAL ACCESS



- Exploit weak/default credentials
- Abuse exposed management services (HTTP/HTTPS/SSH)
- Gain network or physical access

2 Foothold



- Access device configuration
- Extract sensitive data (credentials, keys)
- Identify internal interfaces and protocols
- Establish persistent access (if possible)

3 LATERAL MOVEMENT



- Pivot between protocols (e.g. Modbus, IEC 104, DNP3)
- Interact with connected field devices
- Abuse trust between IT and OT networks
- Map and enumerate downstream systems

4 MANIPULATION



- Send crafted messages or commands
- Modify configuration or setpoints
- Execute unauthorized operations
- Disable safety or monitoring functions

5 IMPACT



- Disrupt operations (Denial of Service)
- Cause unsafe behavior
- Manipulate process data
- Loss of visibility and control



REAL-WORLD IMPACT

Compromise of a coupler can lead to operational disruption, safety risks, data manipulation, and impact on critical infrastructure.

SAME
CURIOSITY.
STRONGER
SYSTEMS.

COUPLER CONFIGURATION PROCESS

CONNECT
MONITOR
CONTROL
A SAFER TOMORROW

SIMPLE SETUP. SECURE CONNECTION. REMOTE MONITORING.

1 SET UP THE CONNECTION

- Connect one end of an Ethernet cable to the device and the other end to your laptop.
- Alternatively, use a Serial-to-USB cable to connect the device to your laptop (or keyboard hub).



2 CONFIGURE IP ADDRESS

- Open your computer's network settings and manually set the wired (Ethernet) IP address to **10.10.100.100**.



3 CONNECT TO WI-FI

- Connect your computer to the Wi-Fi network named **"COUPLE-AP"**.
- Once connected, open a web browser and go to **10.10.100.254**.
- Log in to the device's configuration page using (**Username/Password: admin/admin**).



READY FOR CONFIGURATION

Access the web interface at **10.10.100.254** and log in with **admin/admin** to manage the device settings.

MONITOR
MANAGE
SECURE
DEPLOY

NETWORK SCANNING

DISCOVER. ENUMERATE. UNDERSTAND. ANALYZE.

After analyzing the firmware, I powered up the device and connected it to my laptop using both Ethernet and Serial to USB cables. I set the Ethernet IP on my computer to **10.10.100.100** and accessed the device at **10.10.100.254**.

I used **Nmap**, a powerful network scanner, to discover which ports and services were active on the device.

Command

```
$ nmap -sC -sV -A -p- 10.10.100.254
```



Identify Open Ports

Discovered active services running on the device.



Service Enumeration

Helps understand the device's attack surface.



Potential Entry Points

Open services such as Telnet may allow further analysis and exploitation.



```
$ nmap -sC -sV -A -p- 10.10.100.254
```

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-26 13:27:54
Nmap scan report for 10.10.100.254
Host is up (0.0026s latency).
Not shown: 65531 closed tcp ports (conn-refused)
```

PORT	STATE	SERVICE	VERSION
23/tcp	open	telnet	?

```
|_fingerprint-strings:
```

```
DNSStatusRequestTCP, DNSVersionBindReqTCP, JavaRMI, Kerberos, LANDesk-RC,
LDAPBindReq, NCP, NULL, NotesRPC, RPCCheck, SMBProgNeg, SSLSessionReq,
TLSSessionReq, TerminalServer, TerminalServerCookie, WMSRequest, X11Probe,
afp, giop, ms-sql-s, oracle-tns, tn3270:
```

```
Login as:
```

```
FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, LDAPSearchReq,
RTSPRequest:
```

```
Login as:Invalid User Name
```

```
Login as:Invalid User Name
```

```
Login as:
```

```
Help, LPDString:
```

```
Login as:Invalid User Name
```

```
Login as:
```

```
SIPOptions:
```

```
Login as:Invalid User Name
```

```
Login as:Invalid User Name
```

```
Login as:Invalid User Name
```

```
Login as:Invalid User Name
```

```
Login as:
```

```
80/tcp open rtsp
```

```
|_rtsp-methods: ERROR: Script execution failed (use -d to debug)
```

```
|_http-auth:_
```



KEY TAKEAWAY

Network scanning helps identify exposed services and potential entry points for further security analysis.

RECON
ANALYZE
ASSESS
SECURE

TELNET ACCESS

REMOTE ACCESS. CONFIGURE. CONTROL.

I used the previously extracted credentials from the firmware and attempted to log in to the Telnet service. I wasn't sure if they would work, but they did, successfully giving me access to the device.

I initiated the Telnet session using the Netcat (nc) command:

Command `$ nc 10.10.100.254 23`

(**Note:** The credentials shown in the picture are the old working login details. They were valid before I reset the device configuration during the Telnet Exploitation.)

While exploring the device through the web interface, I noticed that I could **view and modify the profile settings**. These profiles define how the device handles network, serial, and protocol configurations.

By editing these values—such as IP addresses, ports, and serial communication parameters—I was able to **change the behavior** of the device without needing any special permissions or extra steps.



Remote Device Access

Successfully logged in to the Telnet service using extracted credentials.



Modify Configurations

Able to view and change profile settings such as IP, ports, and serial parameters.



Potential Impact

Unauthorized access allows full control, which can disrupt or redirect data.

```
$ nc 10.10.100.254 23
Login as:admin
Password:admin
CMD>?
cfg          net          os          mft
CMD>14:D4:24:8E:92:0F 200011 0 0 1 3 -59/0 /42 HTMIX 20M 7 0 0 300 65 0
MaxCap:HTMIX 20M 7 1 0 , 1447, 100%
```

```
CFG>set SYS_ADMPPASS1 Test123
Change Done

CFG>
CFG>prof show
#PROFILE
#VER_2_1
SYS_ADMPPASS=admin
SYS_ADMPPASS1=Test123
SYS_DAYLITE=0
SYS_DOMAIN=USR-WIFI232-AP
SYS_IDLET=0
SYS_NAME=USR-WIFI232-AP
SYS_RM_EN=1
SYS_RM_IP=0.0.0.0
SYS_RM_PORT=80
SYS_TZONE=45
```



KEY TAKEAWAY

Telnet access with default or weak credentials allows attackers to modify device profiles and change its behavior without restrictions.

RECON
ANALYZE
ASSESS
SECURE

PEOPLE
TECHNOLOGY
A SAFER TOMORROW

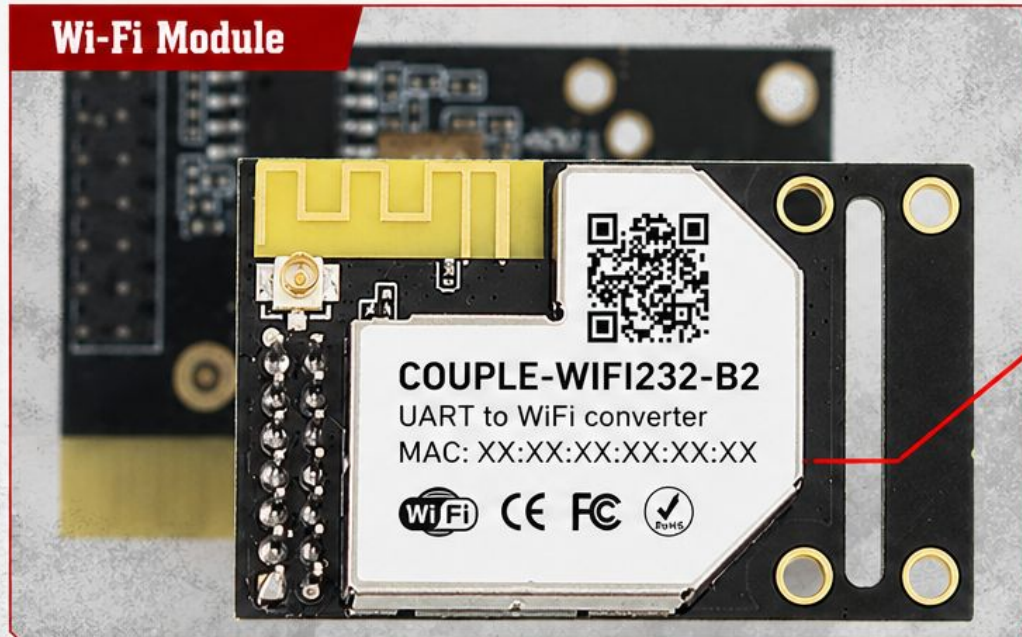
PHYSICAL INSPECTION AND HARDWARE SETUP

PEOPLE
TECHNOLOGY
A SAFER TOMORROW

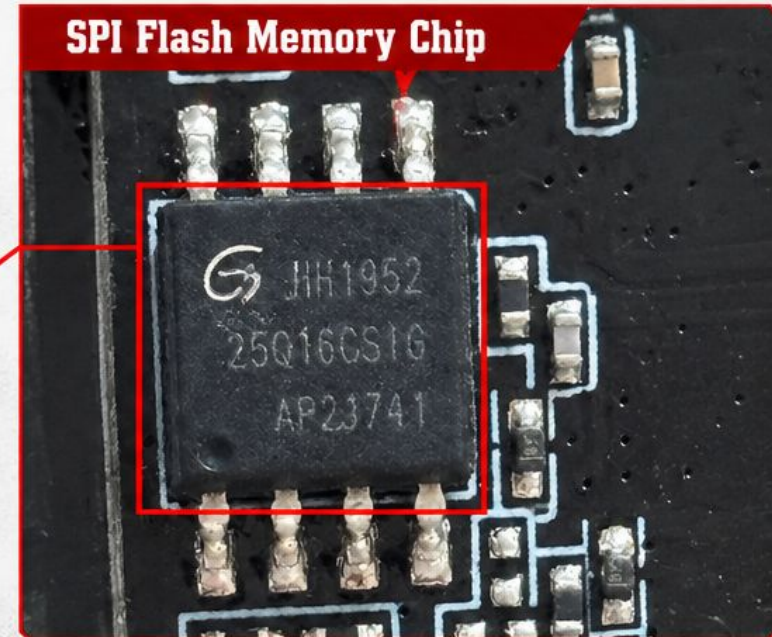
HARDWARE INSIGHTS. FIRMWARE ACCESS. SECURITY RESEARCH.

The process started by carefully opening the device casing to inspect the internal components. I located a small module labeled “**COUPLE-WIFI232-B2**”, and underneath it, I identified a memory chip labeled “**25Q16CSIG**”, which I later confirmed via online datasheets to be a **SPI flash memory chip**. This type of chip stores the firmware (software that runs the device).

Wi-Fi Module



SPI Flash Memory Chip



KEY TAKEAWAY

The **COUPLE-WIFI232-B2** module uses a **25Q16CSIG** SPI flash memory chip to store its firmware, making it a potential target for firmware extraction and analysis.

ANALYZE
REVERSE
UNDERSTAND
SECURE

FIRMWARE EXTRACTION

PEOPLE
TECHNOLOGY
A SAFER TOMORROW

READ. ACCESS. EXTRACT.

To read the contents of the SPI flash memory chip, I used a **CH341A USB programmer** along with **test clips** to connect directly to the chip pins. With the help of a **CH341A programmer** and **testing clips**, I was able to extract the firmware using a tool called **Flashrom**.

Command `$ flashrom -p ch341a_spi -r backup.bin`

This created a backup file (**backup.bin**) of the firmware stored on the flash chip.



CH341A Programmer



25Q16CSIG (SPI Flash)

```
$ flashrom -p ch341a_spi -r backup.bin

flashrom v1.2 on Linux 6.8.0 (x86_64)
Using clock_gettime for delay loops (clk_id: 1, resolution: 1ns).
Found Generic SPI flash chip "25Q16CSIG" (2048 kB, SPI) on ch341a_spi.
Reading flash... done.
Wrote 2097152 bytes to file "backup.bin".
Verification... OK.

$ ls -lh backup.bin

-rw-r--r-- 1 user user 2.0M May 26 13:27 backup.bin
```

FIRMWARE ANALYSIS

Once I had the firmware, I used **Binwalk**, a tool for analyzing and extracting embedded file systems from the binary firmware. I was specifically looking for file systems like **SquashFS**, which is commonly used in Linux-based embedded devices.

After running Binwalk, I also used the **strings** command to extract readable text from the firmware binary.

Command `$ binwalk -Me backup.bin`

Command `$ strings backup.bin | less`

```
$ binwalk -Me backup.bin
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
75232        0x125E0      U-Boot version string, "U-Boot 1.1.3 (Apr 22 2016 - 08:43:56)"
327680       0x50000      uImage header, header size: 64 bytes, header CRC: 0xEAB61D5D,
created: 2019-09-12 02:39:26, image size: 824272 bytes, Data Address:
0x80500000, Entry Point: 0x80500000, data CRC: 0xC577DC27,
OS: Linux, CPU: MIPS, image type: Standalone Program, compression type: none

337024       0x52480      LZMA compressed data, dictionary size: 8388608 bytes,
uncompressed size: 2352640 bytes

1376256      0x150000     Squashfs filesystem, little endian, version 4.0, compression: xz,
size: 713924 bytes, 486 inodes, blocksize:131072 bytes, created: 2016-12-05

$ strings backup.bin | grep -i admin
admin
/etc/passwd admin
web/admin/login
user=admin
admin:admin
```



KEY TAKEAWAY

Extracted and analyzed the firmware to identify file systems, configuration data, and hardcoded credentials.

ANALYZE
REVERSE
UNDERSTAND
SECURE

MOXA NPORT W2150A / W2250A SERIES

PEOPLE
TECHNOLOGY
A SAFER TOMORROW

SECURITY RESEARCH • REAL IMPACT • STRONGER OT SECURITY

01 FINDING

Proprietary Integrity Mechanism — No Cryptographic Digital Signature

Finding F-01: Proprietary Integrity Mechanism — No Cryptographic Digital Signature

Severity	CRITICAL
CWE Classification	CWE-347: Improper Verification of Cryptographic Signature
CVSS v3.1 Score	9.0
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Affected Component	Firmware update mechanism - integrity field at header offset 0x28-0x37
Description	The firmware image relies on a 16-byte proprietary integrity field at header offset 0x28 rather than a standard cryptographic digital signature. This field does not match any standard hash of the payload (MD5, SHA-1, SHA-256) or of the full file, indicating it is either a proprietary CRC, a keyed HMAC with a static manufacturer key, or a truncated custom hash. The firmware update process on the device validates only this 16-byte field before applying the update. An attacker who reverse-engineers this algorithm from the device bootloader (via JTAG/UART extraction) can calculate a valid integrity value for any arbitrary malicious firmware image and flash it to the device. There is no Secure Boot chain of trust, no RSA/ECDSA signature, and no per-partition signing visible in the image structure.
Evidence	<pre> Stored field (0x28-0x37): 875e39084a5bb9d8d4d45d62208d189 MD5 (full file): 47af5331b22a161c20529ff52d735a4 [MISMATCH] MD5 (payload only): 147fb58ebebada4dc5329142bf98965a [MISMATCH] MD5 (header 0x00-0x27): 53128c6d66ba434c44537f0215cfd248 [MISMATCH] SHA-1 (full file): 3c0fc00ebodce506080978660f464055b5822e4acb680 SHA-256 (full file): 9e33179aa15d410ac910315506c57108Sac038897e0ddbed7d6115ee586cfbce Segment count: 0x01 (monolithic - no per-partition signatures) Secure Boot chain: Not present in image structure </pre>
Impact	An attacker who obtains the encryption key (via hardware extraction of any single device) can: (1) decrypt the firmware payload, (2) modify binaries or inject malicious code, (3) re-encrypt, (4) compute a valid forged integrity value, and (5) distribute the malicious image to every device of this model worldwide. This enables persistent remote code execution, credential theft, and the transformation of deployed industrial devices into persistent access points.

02 VENDOR ACKNOWLEDGEMENT

Moxa PSIRT acknowledged the research and agreed to include the researcher in the security advisory.



Moxa PSIRT <PSIRT@moxa.com>

to me ▾

Dear Omkar Mali,

Thank you for your confirmation and for agreeing to be acknowledged in the security advisory.

We sincerely appreciate your support and contribution in helping us identify this omission.

We are currently updating the security advisory, and we will notify you once the revision has been completed.

Thank you again for your valuable assistance.

Sincerely,

The Product Security Incident Response Team

03 ADVISORY UPDATE

Moxa PSIRT later confirmed the security advisory has been updated.



Moxa PSIRT <PSIRT@moxa.com>

to me, Moxa ▾

Dear Omkar Mali,

The security advisory has been updated: <https://www.moxa.com/en/support/product-support/security-advisory/mpsa-233328-nport-s000-series-firmware-improper-validation-of-integrity-check-vulnerability>.

Please feel free to let us know if you have any questions. Thank you!

Sincerely,

The Product Security Incident Response Team

Moxa PSIRT, Part of the CVE Numbering Authority (CNA) Program

04 REVISION HISTORY

The updated advisory includes acknowledgement to the researcher in the revision history.

Revision History:

VERSION	DESCRIPTION	RELEASE DATE
1.0	First Release	Oct 3, 2023
1.1	Update affected versions to "All firmware versions." in Affected Products section	Oct 20, 2023
1.2	Add NPort W2150A/W2250A Series in Affected Products section. Add acknowledgement to Omkar Mali.	June 18, 2026

05 SECURITY IMPACT

- Firmware integrity relies on a proprietary 16-byte field without a standard cryptographic digital signature.
- No Secure Boot chain of trust, no RSA/ECDSA signature, and no per-partition signing.
- An attacker with the encryption key could potentially modify and re-sign firmware images for the device.
- May lead to persistent remote code execution, credential theft, and long-term compromise of deployed devices.



KEY TAKEAWAY

This case highlights the importance of independent security research and responsible disclosure. The vendor acknowledged the finding and updated the advisory, with the researcher credited in the revision history.

RESEARCH
DISCLOSURE
COLLABORATION
A SAFER TOMORROW

VULNERABILITY OVERVIEW

AFFECTED FUNCTIONS • IMPACT • TECHNICAL DETAIL

PEOPLE
TECHNOLOGY
A SAFER TOMORROW

SECURE
INDUSTRIAL
SYSTEMS
STRONGER
TOMORROW

#	AFFECTED FUNCTION	IMPACT	TECHNICAL DETAIL
01	<code>[REDACTED]()</code>	 RCE Remote Code Execution	Heap buffer overflow when <code>[REDACTED]</code> . <code>[REDACTED]</code> allows arbitrary code execution. CVSS 9.8 (Critical).
02	<code>[REDACTED]()</code>	 RCE Remote Code Execution	Heap buffer overflow in <code>[REDACTED]</code> . Boundary checking failure enables remote code execution. CVSS 9.8 (Critical).
03	<code>[REDACTED]()</code>	 DoS Denial of Service	Heap buffer overflow <code>[REDACTED]</code> . <code>[REDACTED]</code> trigger crash without service recovery. CVSS 7.5 (High).



KEY TAKEAWAY

Memory-safety flaws in the affected functions can lead to remote code execution or denial of service, highlighting the importance of secure coding practices and robust input validation.

RESEARCH
ANALYZE
VALIDATE
SECURE

SECURITY ADVISORY

PUBLIC VALIDATION. CVSS. REAL WORLD IMPACT.

PEOPLE
TECHNOLOGY
A SAFER TOMORROW

SECURE
INDUSTRIAL
SYSTEMS
STRONGER
TOMORROW



METRICS

CVSS Version	3.1
Base Score	9.8
Base Severity	CRITICAL
Vector String	CVSS:3.1/AV:N/AC:L /PR:N/UI:N/S:U/C:H/ I:H/A:H



PUBLIC ADVISORY

The vulnerability received public ICS advisory recognition with a **CRITICAL** severity rating and a CVSS v3.1 score of **9.8**.



CISA ADVISORY



America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search



Topics ▾ Spotlight Resources & Tools ▾ News & Events ▾ Careers ▾ About ▾

[Home](#) / [News & Events](#) / [ICS Advisories](#) / Jinan USR IOT Technology Limited (PUSR) USR-W610 RS232/485 to Wi-Fi/Ethernet Converter

SHARE: [f](#) [x](#) [in](#) [e](#)

ICS ADVISORY

Jinan USR IOT Technology Limited (PUSR) USR-W610 RS232/485 to Wi-Fi/Ethernet Converter

Release Date: May 28, 2026

Alert Code: ICSA-26-148-02

RELATED TOPICS: [INDUSTRIAL CONTROL SYSTEM VULNERABILITIES](#) , [INDUSTRIAL CONTROL SYSTEMS](#)

[View CSAF](#)

Summary

Successful exploitation of this vulnerability could result in an attacker gaining administrator access to the device.



KEY TAKEAWAY

Independent research was validated through public ICS advisory publication, with the issue rated **CRITICAL** and capable of leading to administrator access.

RESEARCH
ANALYZE
VALIDATE
SECURE

TOOLS USED

PEOPLE
TECHNOLOGY
A SAFER TOMORROW

RESEARCH • EXTRACTION • ANALYSIS • VALIDATION

01



CH341A PROGRAMMER

Flash dumping

Used to read the contents of SPI flash memory from the target device.

02



FLASHROM

SPI communication

Used for interacting with SPI flash chips and reading the firmware.

03



BINWALK

Firmware unpacking

Used to analyze firmware images and identify embedded files and file systems.

04



STRINGS

ASCII extraction

Used to extract readable strings from firmware binaries for analysis.

05



NMAP

Network scanning

Used to discover open ports, services, and network information on the target device.

06



TELNET

Remote shell

Used to access the device remotely and interact with the command shell.

07



CONFIGURATION TOOL

Device setup

Used for initial device setup, configuration, and analysis of device parameters.



KEY TAKEAWAY

A layered hardware to network workflow enabled systematic firmware analysis, service enumeration, and security validation.

RECON
ANALYZE
ASSESS
SECURE

SECURITY IMPLICATIONS

PEOPLE
TECHNOLOGY
A SAFER TOMORROW

HARDWARE • FIRMWARE • REMOTE ACCESS • DATA EXPOSURE

The device had several security vulnerabilities that could allow an attacker to gain unauthorized access, extract sensitive information, and fully control the device.

01 HARDCODED CREDENTIALS

Plaintext credentials found in firmware

```
$ strings firmware.bin | grep -i pass
admin
admin123
root
rootpass
user
user123
http://192.168.1.1
telnetd
login:
password:
/etc/passwd
/etc/shadow
CONFIG_PASSWORD=
DEFAULT_PASS=admin123
WIFI_PASS=12345678
```

The firmware contains hardcoded plaintext credentials that can be extracted using static analysis tools.

02 UNENCRYPTED FIRMWARE

Firmware can be easily extracted and analyzed

```
$ binwalk firmware.bin
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	uImage header, header size: 64 bytes,
4096	0x1000	LZMA compressed data, properties: 0x5D
131072	0x20000	Squashfs filesystem, little endian, version 4.0, compression:xz, size: 6543360 bytes
7208960	0x6E0000	JFFS2 filesystem, little endian

```
$ |
```

The firmware is not encrypted or obfuscated, allowing an attacker to extract and analyze the filesystem, configuration files, and sensitive data.

03 TELNET SERVICE WITH ROOT ACCESS

Remote shell access with administrative privileges

```
$ nc 10.10.100.254 23

Login as: root
Password: *****

# id
uid=0(root) gid=0(root)

# uname -a
Linux 3.10.14 #1 SMP ... armv7l

#
```

The device exposes a Telnet service that allows root level access, providing full administrative control over the system.



KEY TAKEAWAY

Hardcoded credentials, unencrypted firmware, and exposed administrative services can lead to full device compromise. These issues allow attackers to extract sensitive data, modify the device, and gain persistent control.



DATA EXPOSURE
Sensitive information
can be extracted



FULL CONTROL
Administrative
access achieved



PERSISTENT RISK
Allows long term
device compromise

RECOMMENDATIONS

MITIGATE. STRENGTHEN. STAY SECURE.

PEOPLE
TECHNOLOGY
A SAFER TOMORROW



01 DISABLE **TELNET** BY DEFAULT

Disable or remove the Telnet service by default to prevent unauthorized remote access.



02 ENFORCE **CREDENTIAL CHANGE** ON FIRST LOGIN

Require users to change default credentials during the first login to prevent the use of hardcoded or factory credentials.



03 ENCRYPT **CONFIGURATION STORAGE**

Encrypt sensitive configuration data stored on the device to protect it from unauthorized extraction.



04 IMPLEMENT **FIRMWARE SIGNING** AND VALIDATION

Use cryptographic signing and validation mechanisms to ensure only trusted and untampered firmware is executed.



KEY TAKEAWAY

Implementing these recommendations will significantly reduce the attack surface and improve the overall security posture of the device.

RECON
ANALYZE
ASSESS
SECURE

PEOPLE
TECHNOLOGY
A SAFER TOMORROW

THANK YOU

FOR YOUR TIME AND SUPPORT



LET'S STAY CONNECTED