IOT SECURITY ASSESSMENT

The Node

Prepared for ACME Manufacturing, Inc.

By Samuel LaTourette

Executive Summary

ACME Manufacturing engaged our team to assess the security of their IoT device, "The Node," prior to facility-wide deployment.

Our assessment targeted the STM32F103C8T6 microcontroller and associated interfaces, focusing on physical attack vectors accessible to personnel with device access.

Findings: Four critical vulnerabilities were identified that expose sensitive data through debug interfaces, weak cryptography, and unencrypted communications.

4

VULNERABILITIES FOUND

100%

PHYSICAL ACCESS REQUIRED

Tools Used:

FT232RL USB-to-Serial Adapter
ST-Link V2 Debugger

UART Debug Shell Exposure

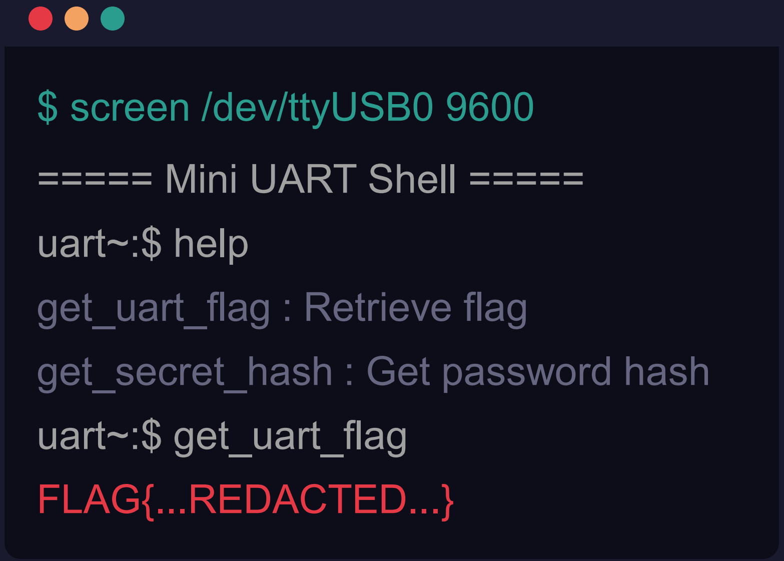
ISSUE

Exposed debug shell on USART2 interface accessible to anyone with physical access to the device.

METHOD

Connected FT232RL to PA2 (TX) and PA3 (RX). Used screen command at 9600 baud. Discovered help menu with get_uart_flag command.

Impact: Full shell access allows extraction of sensitive data and system manipulation.



```
$ screen /dev/ttyUSB0 9600
===== Mini UART Shell =====
uart~:$ help
get_uart_flag : Retrieve flag
get_secret_hash : Get password hash
uart~:$ get_uart_flag
FLAG{...REDACTED...}
```

Weak Password Hashing

ISSUE

Password hash exposed via debug shell using deprecated SHA-1 algorithm with no salt.

METHOD

Retrieved hash via get_secret_hash command. Identified as SHA-1 (40 hex characters). Cracked instantly using CrackStation.

Impact: Weak hashing enables rapid password recovery, granting access to protected functionality.

EXPOSED HASH (SHA-1)

```
37c3bb681afc98e2df6f48d1576071add74b1ad2
```

↓

CRACKED PASSWORD

MARQUETTE

Cracked in < 1 second via rainbow table

✗ No Salt

✗ SHA-1

✗ Dictionary Word

Internal Flash Memory Dump

ISSUE

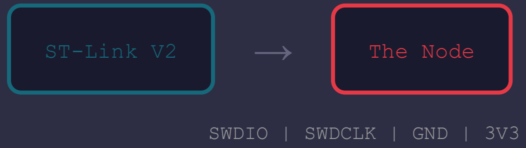
SWD debug interface enabled with no read-out protection. Sensitive data stored in plaintext.

METHOD

Connected ST-Link V2 to SWD header. Used OpenOCD to halt CPU. Dumped 64KB flash from 0x08000000. Searched with strings/grep.

Impact: Complete firmware extraction, credential theft, and intellectual property exposure.

SWD CONNECTION



OpenOCD Output

```
> dump_image flash.bin 0x08000000
0x10000
dumped 65536 bytes
$ strings flash.bin | grep FLAG
FLAG{CONSIDER_ME_DEBUGGED}
```

Unencrypted Data Stream

ISSUE

Sensitive data continuously broadcast in plaintext over USART3 interface (PB10).

METHOD

Reviewed datasheet for additional interfaces. Identified USART3 on PB10 (TX). Connected FT232 RXD to listen. Captured continuous plaintext stream.

Impact: Passive eavesdropping reveals all inter-device communications without detection.

LIVE - Intercepted Data Stream

```
FLAG{DOUBLE_THE_UART_DOUBLE_THE_FUN}
FLAG{DOUBLE_THE_UART_DOUBLE_THE_FUN}
FLAG{DOUBLE_THE_UART_DOUBLE_THE_FUN} ...
```

9600
BAUD RATE

24/7
BROADCAST

0
ENCRYPTION

Recommendations

UART

Disable Debug Interfaces

Remove debug shell in production. Require authentication. Implement secure boot.

PASSWORD

Strengthen Cryptography

Use bcrypt or Argon2. Enforce strong passwords. Never expose hashes.

FLASH MEMORY

Enable Protection

Enable RDP Level 1/2. Disable SWD/JTAG. Encrypt stored data.

DATA STREAM

Encrypt Communications

Use TLS/AES encryption. Request-response only. Authenticate devices.

Conclusion

Our assessment revealed **four critical vulnerabilities** exploitable through physical access alone.

The Node currently lacks fundamental security controls required for production deployment. With contract employees having device access, these vulnerabilities pose significant risk to ACME's sensitive operational data.

Recommendation: Implement all suggested mitigations before production deployment. These changes are essential to protect critical business data.