Payatu

Payatu case study

Hardware Security Assessment of a 4G Dongle for a Giant Telecom Company

Payatu Security Consulting Pvt. Ltd.

Project Overview

A 7-decade-old UK-based telecommunications company that deals in consumer electronics and IoT devices, gauged that the devices they were making needed to be assessed for their cyber resilience, given the market's exposure to cyber-attacks.

In recent times, there have been several incidents of infiltration to larger networks via IoT devices, and there is a dire need to set up their cybersecurity ecosystem.

One of the most holistic and proactive approaches is to assess the security posture of these devices and their corresponding applications. It helps in identifying all the gaps and missing controls in the ecosystem.

For larger organizations like this one, it is critical to detect all vulnerabilities in the products developed and rolled out to mass consumers. In case these vulnerabilities go undetected, it can lead to major cyber events ruining the credibility of the company along with draining out monetary resources.

So, the client decided to have Payatu onboard for testing the 4G dongle on IoT and its web application.

Let's take a look!

Scope

The scope of the project covered performing security assessments on

The objective of the assessment was to check

01 If any hardware debug ports are open

02 If any memory extraction is possible

03 If proper access control is implemented across teams

04 If proper authorization & authentication system is implemented

05 If the user input is properly escaped

Process

1. **Initial Recon -** During the initial phase of the assessment, comprehensive data gathering took place to compile all available information about the device. This entailed conducting an FCC ID search, gathering relevant device-specific details from online sources, and examining the radio protocols employed by the device.

2. **External Inspection of the Device -** During this phase, pertinent external details of the device were collected, including but not limited to the functional attributes of physical buttons, their intended purpose, the availability of external interfaces such as Ethernet and USB, the specific type of screws employed in the device's construction, and the presence or absence of tamper protection mechanisms.

   - **Firmware Assessment -** The firmware running in the device was assessed to find vulnerabilities like hardcoded credentials, insecure communication protocols, usage of outdated libraries or components, or improper input validation.

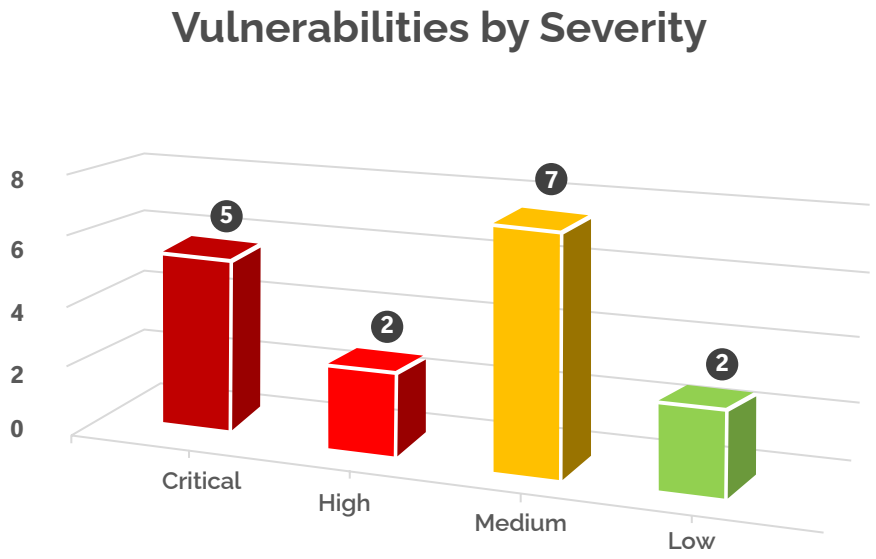
   - **Hardware Assessment -** During the hardware assessment, a meticulous examination of the device's internal components was performed to ascertain the precise details of the utilized chips and microcontrollers. Extensive testing of the device motherboard was conducted, encompassing the scanning and utilization of various debug ports such as UART and JTAG. Furthermore, robust methodologies for firmware extraction from the device were rigorously tested and employed.

   - **Protocol Assessment -** As part of the protocol assessment, a thorough evaluation was conducted, encompassing the analysis of communication channels, protocol implementation, and the potential vulnerabilities to MITM attacks and DoS attacks.

3. **Reporting and Documentation -** Documented all findings, including vulnerabilities discovered, exploitation techniques used, and their potential impact. Provided clear and actionable recommendations for remediation.

4. **Validation and Retesting -** Collaborated with the device owner to validate remediation efforts and conducted retesting to ensure vulnerabilities have been effectively addressed.

Findings



Challenges

01 The entire project was pretty time sensitive and needed to be completed in crunched timelines

02 Lack of proper documentation can lead to miscommunication and elevation of time taken to complete tasks at hand

03 The scope of the project was stretched towards the end

Recommendations

1. Always use authentication to accept any request to the device
2. Use random CSRF tokens to validate each request
3. Restrict the SMS payload length to server acceptable constraints
4. Always make sure the JTAG pins are not exposed on the PCB
5. If in case, they are exposed then the JTAG port must be disabled
6. Use an encrypted/heavily compressed firmware
7. Always use updated libraries and binaries
8. Ensure authentication is required before deleting directories
9. Ensure authentication is required before checking for the existence of files
10. Validate the type of file being uploaded against a whitelist
11. Ensure authentication is required before creating directories
12. Do not disable any debug message in the UART port
13. Disable the UART Port completely

14 Do not disable shell/root access in the UART port

15 Remove the NV binary from the device

16 Filter out the user input data before preparing the final system command to be executed by the server

17 Escape and encode all the possible special characters that can break a particular command

18 Create the file limited to the SD card path only

About Payatu

Payatu is a Research-powered cybersecurity services and training company specialized in IoT, Embedded Web, Mobile, Cloud, & Infrastructure security assessments with a proven track record of securing software, hardware and infrastructure for customers across 20+ countries.

Critical Infrastructure Assessment

There are various security threats focusing on Critical Infrastructures like Oil and Gas, Chemical Plants, Pharmaceuticals, Electrical Grids, Manufacturing Plants, Transportation systems etc. and can significantly impact your production operations. With Payatu's OT security expertise you can get a thorough ICS Maturity, Risk and Compliance Assessment done to protect your, critical infrastructure. pipeline to increase the visibility of security threats.

Product Security

Save time while still delivering a secure end-product with Payatu. Make sure that each component maintains a uniform level of security so that all the components "fit" together in your mega-product.

Mobile Security Testing

Detect complex vulnerabilities & security loopholes. Guard your mobile application and user's data against cyberattacks, by having Payatu test the security of your mobile application.

Cloud Security Assessment

As long as cloud servers live on, the need to protect them will not diminish. Both cloud providers and users have a shared responsibility to secure the information stored in their cloud. Payatu's expertise in cloud protection helps you with the same. Its layered security review enables you to mitigate this by building scalable and secure applications & identifying potential vulnerabilities in your cloud environment.

Code Review

Payatu's Secure Code Review includes inspecting, scanning and evaluating source code for defects and weaknesses. It includes the best secure coding practices that apply security consideration and defend the software from attacks.

Red Team Assessment

Red Team Assessment is a goal-directed, multidimensional & malicious threat emulation. Payatu uses offensive tactics, techniques, and procedures to access an organization's crown jewels and test its readiness to detect and withstand a targeted attack.

DevSecOps Consulting

DevSecOps is DevOps done the right way. With security compromises and data breaches happening left, right & center, making security an integral part of the development workflow is more important than ever. With Payatu, you get an insight to security measures that can be taken in integration with the CI/CD pipeline to increase the visibility of security threats.

Web Security Testing

Internet attackers are everywhere. Sometimes they are evident. Many times, they are undetectable. Their motive is to attack web applications every day, stealing personal information and user data. With Payatu, you can spot complex vulnerabilities that are easy to miss and guard your website and user's data against cyberattacks.

IoT Security Testing

IoT product security assessment is a complete security audit of embedded systems, network services, applications and firmware. Payatu uses its expertise in this domain to detect complex vulnerabilities & security loopholes to guard your IoT products against cyberattacks.

CTI

The area of expertise in the wide arena of cybersecurity that is focused on collecting and analyzing the existing and potential threats is known as Cyber Threat Intelligence or CTI. Clients can benefit from Payatu's CTI by getting - social media monitoring, repository monitoring, darkweb monitoring, mobile app monitoring, domain monitoring, and document sharing platform monitoring done for their brand.

More Services Offered by Payatu

- AI/ML Security Audit
- Trainings

More Products Offered by Payatu

- EXPLIoT
- CloudFuzz

Payatu

Payatu Security Consulting Pvt. Ltd.

www.payatu.com

info@payatu.io

+91 20 41207726