BUG BOUNTY BASED MEDICAL DEVICES

Presented By:
S.B Arunachalam – Salem College of Engineering and Technology - CSE

SYNOPSIS

- ❖ Introduction
- ❖ IOT based medical devices
- ❖ Threat landscape
- ❖ How
- ❖ Why
- ❖ Benefits
- ❖ Conclusion

INTRODUCTION

A bug bounty is a reward offered by organizations to ethical hackers or security researchers for finding and reporting security vulnerabilities in their software, websites, or applications. These vulnerabilities, also called bugs, could potentially be exploited by malicious actors to gain unauthorized access to data or systems.

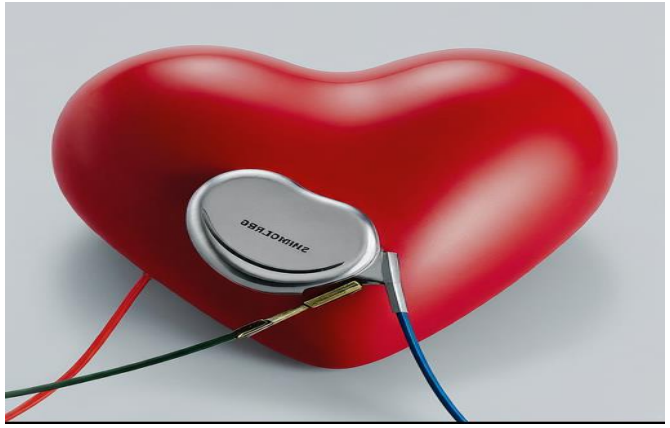
How Bug Bounties Work

1. **Organizations Set Up Programs:** Companies create bug bounty programs with guidelines outlining the types of vulnerabilities they're interested in and the rewards offered for finding them. These programs can be public (open to anyone) or private (by invitation only).
2. **Ethical Hackers Participate:** Security researchers and ethical hackers participating in the program test the organization's systems for vulnerabilities following the program's guidelines.
3. **Vulnerability Reporting:** If a vulnerability is found, the ethical hacker reports it to the organization according to a specific process. This report typically includes details on how the vulnerability was discovered and the potential impact it could have.
4. **Verification and Bounty Payment:** The organization verifies the reported vulnerability and assesses its severity. If the vulnerability is legitimate, the organization fixes it and rewards the ethical hacker according to the program's bounty schedule.

IOT BASED MEDICAL DEVICES

The Internet of Things (IoT) is revolutionizing the healthcare industry by creating a new wave of smart medical devices. These devices collect, transmit, and analyze patient data, allowing for remote monitoring, improved diagnostics, and personalized treatment plans. Here are some examples of medical devices based on IoT:

1. Remote Patient Monitoring (RPM) wearables
2. Smart inhalers
3. Insulin pumps
4. Smart pills
5. Cardiac rehabilitation devices



THREAT LANDSCAPE

- Medical devices are a growing target for cyberattacks.
- Hackers can exploit vulnerabilities to:
    - Steal patient data.
    - Disrupt device operation.
    - Change treatment parameters.
- Potential consequences:
    - Delayed or inaccurate treatment.
    - Serious patient harm or even death.

HOW?

- Bug bounty programs incentivize security researchers to find vulnerabilities.
- Researchers are paid for reporting valid vulnerabilities.
- Benefits:
    - Identify vulnerabilities before they are exploited by attackers.
    - Diverse range of expertise from the security researcher community.
    - Cost-effective compared to traditional security testing.
- Key considerations:
    - Scope: Clearly define the types of devices and data included in the program.
    - Rewards: Offer competitive rewards for high-impact vulnerabilities.
    - Communication: Establish clear communication channels with researchers.
    - Response: Have a defined process for triaging, validating, and fixing vulnerabilities.

WHY?

- Leverage the expertise of a global security researcher community
- Identify vulnerabilities before they are exploited by attackers
- Proactive approach to medical device security
- Complement traditional security testing methods
- Cost-effective way to improve device security

BENEFITS

- **Enhanced Security:** Bug bounties help organizations identify and fix vulnerabilities before they can be exploited by attackers.
- **Diverse Testing:** Bug bounty programs tap into the expertise of a wide range of security researchers, providing a broader perspective on potential security issues.
- **Cost-Effective:** Bug bounties can be a cost-effective way to improve security compared to hiring a large in-house security team.

CONCLUSION

- Bug bounties are a valuable tool for securing medical devices.
- By leveraging the expertise of the security researcher community, we can improve the safety and security of these life-saving technologies.