IOT Web Vulnerability & Exploitation

OWASP-TOP-10

• IoT devices often have a web interface

• Manage and control the devices

• Often has different user levels which could lead to authorization flaws

• Vulnerable to typical web application security flaws

Firmware

#1. IP Camera

#2. Baby Monitor

#3. OR any other firmware which have web interface

Examples

IP Camera

Let's take example of IP Camera,

Suppose you hacked IP Camera, what will be the result ?

Answer:

Live Feed, anybody can see all home activity and broadcast real time images to other channel which will be very dangerous.

Other Vulnerability

• Command Injection

• CSRF

• XSS

• SQLi

- Information error message
- Others – XXE, SSRF, LFI, RFI, Serialization bugs, etc.
- Insufficient authorization and authentication checks
- Privacy issues
- Lack of secure communication channel
- Denial of service attacks
- Brute-force of username and password based attacks
- Business logic flaws

Recent vulnerabilities discovered

Source : https://www.rapid7.com/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf

CVE-2015-2886	Remote	R7-2015-11.1	Predictable Information Leak	iBaby M6
CVE-2015-2887	Local Net, Device	R7-2015-11.2	Backdoor Credentials	iBaby M3S
CVE-2015-2882	Local Net, Device	R7-2015-12.1	Backdoor Credentials	Philips In.Sight B120/37
CVE-2015-2883	Remote	R7-2015-12.2	Reflective, Stored XSS	Philips In.Sight B120/37
CVE-2015-2884	Remote	R7-2015-12.3	Direct Browsing	Philips In.Sight B120/37
CVE-2015-2888	Remote	R7-2015-13.1	Authentication Bypass	Summer Baby Zoom Wifi Monitor & Internet Viewing System
CVE-2015-2889	Remote	R7-2015-13.2	Privilege Escalation	Summer Baby Zoom Wifi Monitor & Internet Viewing System
CVE-2015-2885	Local Net, Device	R7-2015-14	Backdoor Credentials	Lens Peek-a-View
CVE-2015-2881	Local Net	R7-2015-15	Backdoor Credentials	Gynoii
CVE-2015-2880	Device	R7-2015-16	Backdoor Credentials	TRENDnet WiFi Baby Cam TV-IP743SIC

```
Thanks & Regards
Harshad Shah
Founder & CEO, Hacker Associate
```