Example PoC: Vulnerable Cordova SDKs

Smartphone with Smart Home Security app installed

1. Smartphone user visits malicious page in the browser
2. Malicious Webpage
3. Loading screen changed

Cordova Version 3.6.4
CVE-2015-1835

Example PoC: Default or Misconfigured Whitelist

Credentials sent to attacker. Now attacker can control the connected devices and FB.

Example PoC: Unsafe APIs

alarmName = XSS
PAYLOAD;
$("div-container").html(alarmName);

jQuery API html() being used to display alarm name

Future Work

- Develop proof-of-concept exploits for the remaining security issues
- Demonstrate on real-world IoT device

References


Work supported in part by National Science Foundation Grant No. 1566321