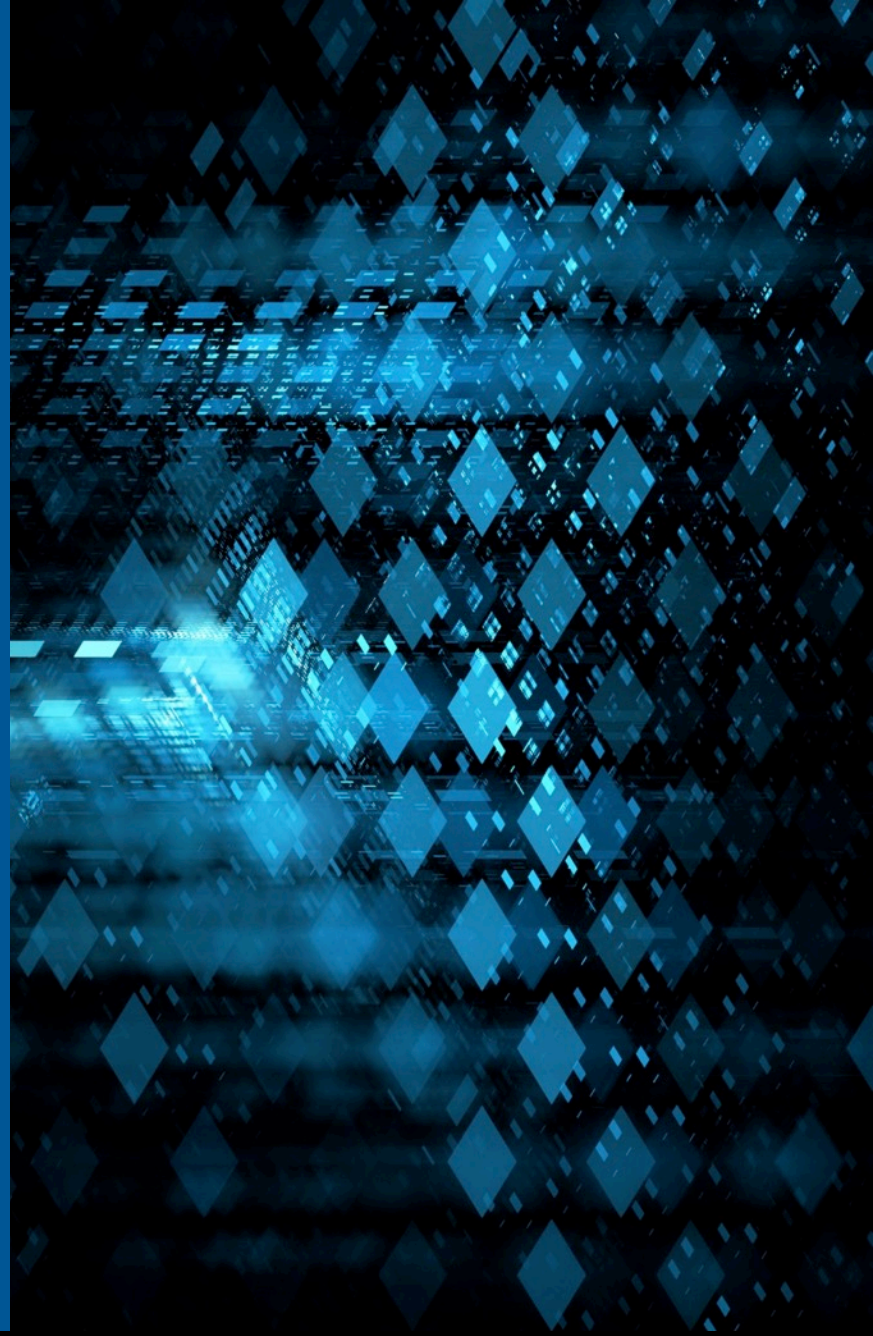
Framework for Embedded Device Vulnerability Analysis

Madison Oliver

Kyle O'Meara

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213



© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Copyright 2017 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM17-0752

Software Engineering Institute/CERT Coordination Center (CERT/CC)

- Carnegie Mellon -> SEI -> CERT -> Threat Analysis Directive -> Vulnerability Analysis Team -> Attack Modeling

- Madison Oliver

- Kyle O’Meara

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Agenda

- Introduction
- Motivation
- Framework
- Results
- Future Work
- Conclusion

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Introduction

- Embedded devices are becoming more ubiquitous and accessible
- Vulnerability research process regarding embedded devices does not currently exist
- Our framework is a concrete, scientific process that can be followed to thoroughly complete research at a macro-level

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Motivation

- Creating comparable and thorough results
- Ensure that every component of the device is at least minimally tested throughout the research process

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Framework

- Embedded Device List Curation
- Information Gathering
- Firmware Analysis
- Web Application Analysis
- Mobile Application Analysis
- Hardware Analysis
- Vulnerability Analysis

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Framework

- Embedded Device List Curation
- Information Gathering
- Firmware Analysis
- Web Application Analysis
- Mobile Application Analysis
- Hardware Analysis
- Vulnerability Analysis

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Embedded Device List Curation

- This step only needs to be completed if the researcher doesn't have a specific device to test
- Develop a list of common embedded devices
- Key considerations:
  1. Access to the physical device
     - Physical access to the device allows for more complete results
  2. Access to the firmware in any capacity
     - This is necessary to have comprehensive results
     - Also consider:
       - Number of firmware versions
       - Availability of this firmware
       - If the firmware is still being maintained

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Framework

- Embedded Device List Curation
- Information Gathering
- Firmware Analysis
- Web Application Analysis
- Mobile Application Analysis
- Hardware Analysis
- Vulnerability Analysis

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Information Gathering

- Collecting information about past and present vulnerabilities and exploits
  - In regards to the specific device, similar devices, and the vendor
- Three steps:
  1. Identifying any vulnerabilities, past or present, that have been associated with the vendor and vendor devices that are similar to the chosen device
  2. Identify vulnerabilities across similar devices, as these vulnerabilities may be applicable in the chosen device
  3. Identify exploits
     - There are multiple Internet resources, such as Exploit-DB and VirusTotal, that can be used to discover exploits for the vulnerabilities found

© 2017 Carnegie Mellon University
"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Framework

- Embedded Device List Curation
- Information Gathering
- Firmware Analysis
- Web Application Analysis
- Mobile Application Analysis
- Hardware Analysis
- Vulnerability Analysis

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Firmware Analysis

- Analyze the contents of the firmware image
- Tools used:
  1. Binwalk – open source tool for analyzing firmware images
     - Used to:
       - Analyze, reverse engineer, and extract firmware images
       - Review the contents, determine, and extract the file system
  2. TROMMEL – custom developed for this project
     - Available on GitHub
     - Searches files and directories to identify indicators of vulnerabilities
       - Indicators include SSH and SLS key files, IP addresses, URLs, email addresses, shell scripts, web server and other specific binaries, config files, database files, shared object libraries, web app scripting variables, and Android APK file permissions
     - vFeed – open source - correlated vulnerability and threat intelligence database wrapper
       - Integrated to take TROMMEL results and searches the CVE database, Exploit-DB, and Metasploit

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Framework

- Embedded Device List Curation
- Information Gathering
- Firmware Analysis
- Web Application Analysis
- Mobile Application Analysis
- Hardware Analysis
- Vulnerability Analysis

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Web Application Analysis

- Most embedded devices contain some sort of web application interface
  - Typically used to access administrative features
- Many open source tools can be used for testing
  - Most common on web application scanners
    - Typically test for most general web app vulnerabilities
- Tools used:
  - Both are freely available, easy to use, and worked in our environment
  1. OWASP ZAP
     - Uses a proxy to intercept website requests and uses this to actively and passively scan for vulnerabilities
  2. Nikto
     - Searches for potentially malicious files, checks versions, and looks for specific issues relating to the versions used

© 2017 Carnegie Mellon University
"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Framework

- Embedded Device List Curation
- Information Gathering
- Firmware Analysis
- Web Application Analysis
- Mobile Application Analysis
- Hardware Analysis
- Vulnerability Analysis

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Mobile Application Analysis

- Specifically analyzed Android mobile applications
- Tools used:
  1. Apktool
     - Used to decode the Android Package Kit (APK) files
  2. TROMMEL
     - Searches files and directories to identify indicators of vulnerabilities
       - Same techniques that was used during the Firmware Analysis section

© 2017 Carnegie Mellon University
"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Framework

- Embedded Device List Curation
- Information Gathering
- Firmware Analysis
- Web Application Analysis
- Mobile Application Analysis
- Hardware Analysis
- Vulnerability Analysis

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Hardware Analysis

- Five steps:
  1. Identify all markings on the physical case of the device
  2. Identify the components internal to the device located on printed circuit board
  3. Dump the flash memory, and extract and analyze the contents of the firmware image
  4. Extract the contents of the flash memory component
  5. Compare the contents extracted from the flash memory component to relative firmware gathered during the Embedded Device List Curation and Identification phase of the framework

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Framework

- Embedded Device List Curation
- Information Gathering
- Firmware Analysis
- Web Application Analysis
- Mobile Application Analysis
- Hardware Analysis
- Vulnerability Analysis

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Vulnerability Analysis – Research and Testing

- Two steps:
  1. Review the firmware updates for patches – typically found in release notes
     - This is to determine if and when the vulnerabilities previously found were fixed
  2. Test the actual exploits against the device
     - Gathered during the Information Gathering section
       - Test all of them, including the ones in similar devices from the same vendor
     - Researchers should take caution when downloading exploits and review the exploit code before testing it against the chosen device

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Vulnerability Analysis - Disclosure

- Depends on the vendor
  - Ideally the vendor will have a disclosure process or portal outlined on their website that the researcher should follow
- If this doesn't exist, the researcher can follow The CERT Guide to Coordinated Vulnerability Disclosure

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Results

- We applied this framework to a D-Link DCS-935L HD Wi-Fi Camera

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Results

- Embedded Device List Curation
- Information Gathering
- Firmware Analysis
- Web Application Analysis
- Mobile Application Analysis
- Hardware Analysis
- Vulnerability Analysis

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Embedded Device List Curation

- Compiled a list of nearly 300 different embedded devices
- Chose a D-Link camera because their firmware was readily available
  - There has been significant testing of their routers, but limited testing on their cameras
  - Five firmware versions were tested:
    - 1.04
    - 1.06
    - 1.08
    - 1.09
    - 1.10

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Results

- Embedded Device List Curation
- Information Gathering
- Firmware Analysis
- Web Application Analysis
- Mobile Application Analysis
- Hardware Analysis
- Vulnerability Analysis

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Information Gathering

- Generated a list of 16 different vulnerabilities with corresponding CVE's, VU#s, Metasploit modules, and Exploit-DB exploits
- **No** current vulnerabilities for DCS-935L
  - All the ones found are other cameras by the same vendor
- Vulnerabilities include:
  - Remote Code Execution
  - Unauthenticated Remote Access
  - Unrestricted Upload
  - Cross-site Scripting
  - Information Exposure
  - Denial of Service
  - Directory Traversal
  - Cross Site Request Forgery

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Results

- Embedded Device List Curation
- Information Gathering
- Firmware Analysis
- Web Application Analysis
- Mobile Application Analysis
- Hardware Analysis
- Vulnerability Analysis

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Firmware Analysis - Binwalk

- Identified a file system embedded in firmware v1.10.01 that was extracted for further analysis
  - v1.10.01 is the latest version on vendor website at the start of this paper
- Squashfs – compressed, read-only Linux file system common in embedded devices

```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
10264         0x2818          LZMA compressed data, properties: 0x5D, dictionary
1446946       0x161422        Squashfs filesystem, little endian, version 4.0, c
```


© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Firmware Analysis - TROMMEL

- TROMMEL found two files of interest and an outdated, vulnerable version of BusyBox (1.22.1) running on v1.10.01

Files of Interest
/root/etc/Wireless/wscd.conf
/root/etc/Wireless/RTL8192CD_static.dat

BusyBox Vulnerabilities
CVE-2016-2148
CVE-2016-2147
CVE-2014-9645

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Results

- Embedded Device List Curation
- Information Gathering
- Firmware Analysis
- Web Application Analysis
- Mobile Application Analysis
- Hardware Analysis
- Vulnerability Analysis

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Web Application Analysis – OWASP ZAP

- OWASP ZAP spidered the web pages and performed active scans against the interface
- Returned four different findings
  - Two of these findings are related to best practices
    - Web Browser XSS Protection Not Enabled
    - X-Content-Type-Options Header Missing
  - Two findings are vulnerabilities that have not been previously reported
    - We contacted the vendor and are following their vulnerability disclosure process

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Web Application Analysis - Nikto

- Confirmed most of our findings from OWASP ZAP
  - Did find one additional vulnerability – likely because it was given admin credentials and OWASP ZAP was not
- Output from authentication and unique result:
  - crossdomain.xml contains a full wildcard entry

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Results

- Embedded Device List Curation
- Information Gathering
- Firmware Analysis
- Web Application Analysis
- Mobile Application Analysis
- Hardware Analysis
- Vulnerability Analysis

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Mobile Application Analysis

- Downloaded the mydlink Lite application from the Google Play Store
- Decoded the APK using Apktool
- Ran TROMMEL on the decoded APK directory
  - Reviewed the indicators and verified that no vulnerabilities were identified

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Results

- Embedded Device List Curation
- Information Gathering
- Firmware Analysis
- Web Application Analysis
- Mobile Application Analysis
- Hardware Analysis
- Vulnerability Analysis

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Hardware Analysis – 1) Physical Case

- Goal: Identify all markings on the physical case of the device
- Case provided: Firmware Version, Hardware Version, MAC Address, Model, Model Number, mydlink Number, Part Number, QR Code, Regulatory Identification (ID) Numbers, Serial Number, Wi-Fi Password, and Wi-Fi SSID
- Any of this information can aid in analysis
  - Particularly, the Regulatory ID Numbers
    - Associated country regulatory databases can be searched for documents submitted by the vendor

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Hardware Analysis – 2) PCB

- Goal: Examine PCB to identify the flash component
- We identified six components of interest
  - Two RealTek, one Winbond, two Macronix, and one SkyWorks
- We identified the main flash memory component as one of the Macronix by reviewing datasheets

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Hardware Analysis – 3) Dump Flash Memory

- Goal: Dump memory from flash memory component
- More of an advanced process however setup and execution is straight forward
- Used BusPirate and flashrom to extract the firmware image from the Macronix flash memory
- The extracted the contents of the of the Macronix component were written to a binary file
  - We labeled this extracted firmware as v1.04 as this was the firmware version listed on the physical case of the DCS-935L

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Hardware Analysis – 4) Extract & Analyze Firmware Image

- Goal: Extract and analyze content from firmware image
- Same techniques that were used to analyze v1.10.01 during the Firmware Analysis section
- Extracted firmware from DCS-935L, v1.04, contained an out of date BusyBox version (v1.13.4)
- 6 CVEs were found to affect this BusyBox version:
  - CVE-2016-2148, CVE-2016-2147, CVE-2014-9645, CVE-2013-1813, CVE-2011-5325, and CVE-2011-2716
  - No Exploit-DB entries or Metasploit modules exist for these

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Hardware Analysis – 5) Compare Flash Memory

- Goal: Compare flash memory component firmware to firmware from vendor website
- Compared v1.04 and v1.04.06 (earliest on website) and v1.04 and v1.10.01
- Used the MD5 hash values of the respective extracted files
- Firmware v1.04 shared 4.3% of the files found in firmware v1.04.06 and 3.7% of the files found in v1.10.01
  - Demonstrates that the vendor is actually updating firmware
- Most common shared files were shared object library files
  - This could be a future concern if a vulnerability is found in a library file

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Results

- Embedded Device List Curation
- Information Gathering
- Firmware Analysis
- Web Application Analysis
- Mobile Application Analysis
- Hardware Analysis
- Vulnerability Analysis

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Vulnerability Analysis – Research and Testing

- Manually reviewed firmware updates for version 1.04 to version 1.10
  - Showed that two of the new vulnerabilities found had never been reported then patched
- Attempted known exploits against the devices
  - 16 different vulnerabilities, some with exploits, for many different model cameras, **not** including the camera being tested
  - Did not return any results
    - Meaning that 935L is either not vulnerable or the exploit does not translate exactly to a different

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Vulnerability Analysis - Disclosure

- Following the process outlined by the vendor to properly disclose the newly discovered vulnerabilities
- Found on the vendor's website

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Future Work

- Applying framework to other embedded devices
  - Including other D-Link cameras, different vendor cameras, and completely different types of devices
- Change our analysis environment as our current analysis was extremely limited because of our inability to completely setup the devices
- In the development to include future phases into the framework to include:
  - Radio frequency (RF) analysis
  - Advanced hardware analysis
  - Binary analysis of ARM and MIPS files

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Conclusion

- This framework was developed to create a universal, holistic, macro-level approach to embedded devices vulnerability analysis
- Goal was to create a methodology that researchers could follow to create more **comprehensive** and **actionable** results
- Tested on a class of embedded devices, Wi-Fi cameras, and found vulnerabilities that had not yet been published
- Developed an open source tool, TROMMEL, to aid researchers in embedded device vulnerability analysis
- We expect the framework to not only expand with our future work but as well as with evolution of the embedded device landscape

© 2017 Carnegie Mellon University

"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."

Contact Information

Presenter
Madison Oliver
Technical Intern
Email: mqoliver@sei.cmu.edu

Presenter
Kyle O'Meara
Sr. Member of the Technical Staff
Telephone: 412.268.2537
Email: komeara@cert.org

Paper
Link
Tool
Link

© 2017 Carnegie Mellon University
"[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution."