DRINKING FROM THE CVE FIREHOSE

Or How To Ensure Your Open Source Product Survives the Onslaught of Publicly Known Security Vulnerabilities

Ryan Ware
Intel Corporation
WHAT IS A SECURITY VULNERABILITY?

No! Really! I’m Not Joking! What Is It?!?
This is your intended product designed but not implemented. It includes:

**Design**
- Architecture
- High Level Design
- Low Level Design
- Requirements
- Specifications
- Compliance

**Implementation**
- Source Code
- Object Code
- Libraries
- Executables
- Dependencies
- Environment

*Extra* functionality
IS IT SECURE?
IS IT COMPROMISED?
IS IT VULNERABLE?

2016 Vulnerabilities In 4 Common Components

- **Linux Kernel**
- **OpenSSL**
- **LibTiff**
- **ffmpeg**

294 Total CVEs In Just 4 Components!
How quickly can a known vulnerability be exploited?

* Hits from Google on 2/20/17
WHO ARE FINDING THE VULNERABILITIES?
NOT YOUR MOTHER'S HACKER
SECURITY HACKERS ECOSYSTEM

The World Today

National Interest

Personal Gain

Personal Fame

Curiosity

Fastest growing segment

Tools created by experts now used by less-skilled attackers and criminals

Author

Hobbyist Hacker

Expert

Specialist

Money

Vandal

Spy

Script-Kiddy
BUG BOUNTY PROGRAMS

• "A bug bounty program is a deal offered by many websites and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to exploits and vulnerabilities." – Wikipedia [1]

• First well known program created by Netscape

• Bug bounty programs have really taken off in the last few years

• Hundreds of bug bounty programs including major players such as Google, Facebook, Microsoft, Dell, and PayPal.
CHROMIUM BUG BOUNTIES [1]

- “Rewards for Qualifying bugs typically range from $500 to $100,000”
- Standing $100,000 reward for participants that can compromise Chromebook or Chromebox with device persistence in guest mode.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Sandbox Escape [5]</td>
<td>$15,000</td>
<td>$10,000</td>
<td>$2,000 - $5,000</td>
<td>$500</td>
</tr>
<tr>
<td>Renderer Remote Code Execution</td>
<td>$7,500</td>
<td>$5,000</td>
<td>$1,000 - $3,000</td>
<td>$500</td>
</tr>
<tr>
<td>Universal XSS (local bypass or equivalent)</td>
<td>$7,500</td>
<td>$5,000</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Information Leak</td>
<td>$4,000</td>
<td>$2,000</td>
<td>$0 - $1000</td>
<td>$0</td>
</tr>
<tr>
<td>Download Protection bypass [6]</td>
<td>N/A</td>
<td>$1,000</td>
<td>$0 - $500</td>
<td>$0</td>
</tr>
</tbody>
</table>
ZERODIUM Payout Ranges

LPE: Local Privilege Escalation
MTB: Mitigation Bypass
RCE: Remote Code Execution
RJB: Remote Jailbreak
SBX: Sandbox Escape
VME: Virtual Machine Escape

*All payout amounts are chosen at the discretion of ZERODIUM and are subject to change or cancellation without notice.*
OK. CAN WE GET BACK TO THE CVE THING?
WHAT IS A CVE?

- CVE = Common Vulnerabilities and Exposures
- Database of “all” publicly known software security vulnerabilities starting in 1999
- MITRE Corporation manages and maintains CVE on behalf of US National Cyber Security Division
- Currently 81,785 Vulnerabilities in Database
- 1,822 for 2017 so far
  - Average of 35 per day!
THE SILENT BUG FIX

• The CVE Database is Great...But...
  • Many companies do not publish CVEs for internally found security issues
  • Bug bounty programs don’t always publish CVEs for found issues
  • Many bugs that **may** have security implications are silently fixed by developers as functional bugs
GREAT INFO. HOW DOES THIS HELP ME?!!?
You must include an update mechanism of some type in your product!

If you don’t, the message to your customers is, “We don’t care about you.”

Make it easy for your customers to update

If it’s painless, they’ll do it more often

Make it completely transparent as long as you tell them what you’re doing

Many mechanisms available

Android OTA, swupd, SWUpdate, Mender, OSTree, even published repos
KEEPING TRACK OF CVES

CVE Details
The ultimate security vulnerability datasource

https://cvedetails.com

OpenSSL » OpenSSL : Vulnerability Statistics

Vulnerabilities (173)  CVSS Scores Report  Browse all versions  Possible matches for this product  Related Metasploit Modules

Related OVAL Definitions  :  Vulnerabilities (316)  Patches (348)  Inventory Definitions (1)  Compliance Definitions (0)

Vulnerability Feeds & Widgets

You can generate a custom RSS feed or an embedable vulnerability list widget or a json API call url.
(Feeds or widget will contain only vulnerabilities of this product)
Selected vulnerability types are OR'ed. If you don't select any criteria "all" CVE entries will be returned

- [ ] Vulnerabilities with exploits
- [ ] Cross Site Request Forgery
- [ ] Sql injection
- [ ] Memory corruption
- [ ] Gain information
- [ ] Code execution
- [ ] File inclusion
- [ ] Cross site scripting
- [ ] Http response splitting
- [ ] Denial of service

Order By: CVE id  CVSS score >= :

Log in or sign up for an account to create a custom feed or widget
KEEPING TRACK OF CVES (CONT)

- CVE-Check-Tool (https://github.com/ikeydoherty/cve-check-tool)
  - Created by Ikey Doherty
  - Will scan your source code for known CVEs
  - Used by Clear Linux
  - Not 100% perfect, but close
  - (Thank you for rewriting it in C!)
- Various Commercial Solutions
ATTACKABLE SURFACE AREA

• “The attack surface of a software environment is the sum of the different points (the ‘attack vectors’) where an unauthorized user (the ‘attacker’) can try to enter data to or extract data from an environment.” – Wikipedia

• Limit the attack surface by only including software your product requires.

• Anything beyond is just something you need to patch or a vector for an attacker.

Nothing more satisfying than being able to respond to a CVE by saying, “Doesn't affect me.”
OTHER IMPORTANT CONCEPTS

Least Privilege
- A huge danger phrase: “But I need to run as root.”
  - “But I’m special!”
- Software should run with the minimum privileges it needs to function

Defense in Depth
- Have multiple protections in place
OTHER IMPORTANT CONCEPTS

Code Reviews
• No one writes perfect code
• Beware code reviews submitted and accepted within minutes
• Use static code analysis as extra set of automated eyes

Validation
• Actually test that your product does what you intend
CONCLUSION

• What really constitutes a security bug vs. other bugs
• Questions that are danger signs for those unfamiliar with security
• How quickly vulnerabilities can start to be exploited
• What kinds of people find vulnerabilities and how bug bounty programs play into it
• What CVEs are and how to track them
• Various tools and techniques to help you survive

Ryan Ware – ryan.r.ware@intel.com
QUESTIONS?