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

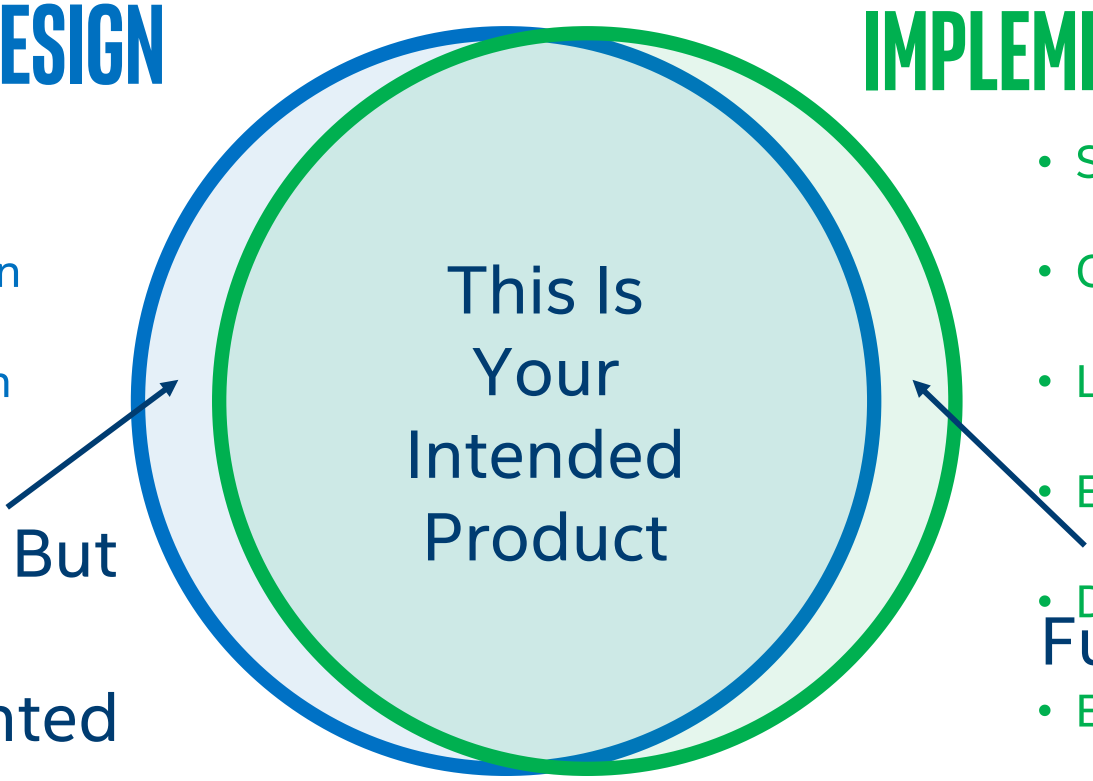
Spadowski's

WHAT IS A SECURITY VULNERABILITY?

No! Really! I'm Not Joking! What Is It?!?

DESIGN

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



This Is Your Intended Product

Designed But Not Implemented

“Extra” Functionality

IMPLEMENTATION

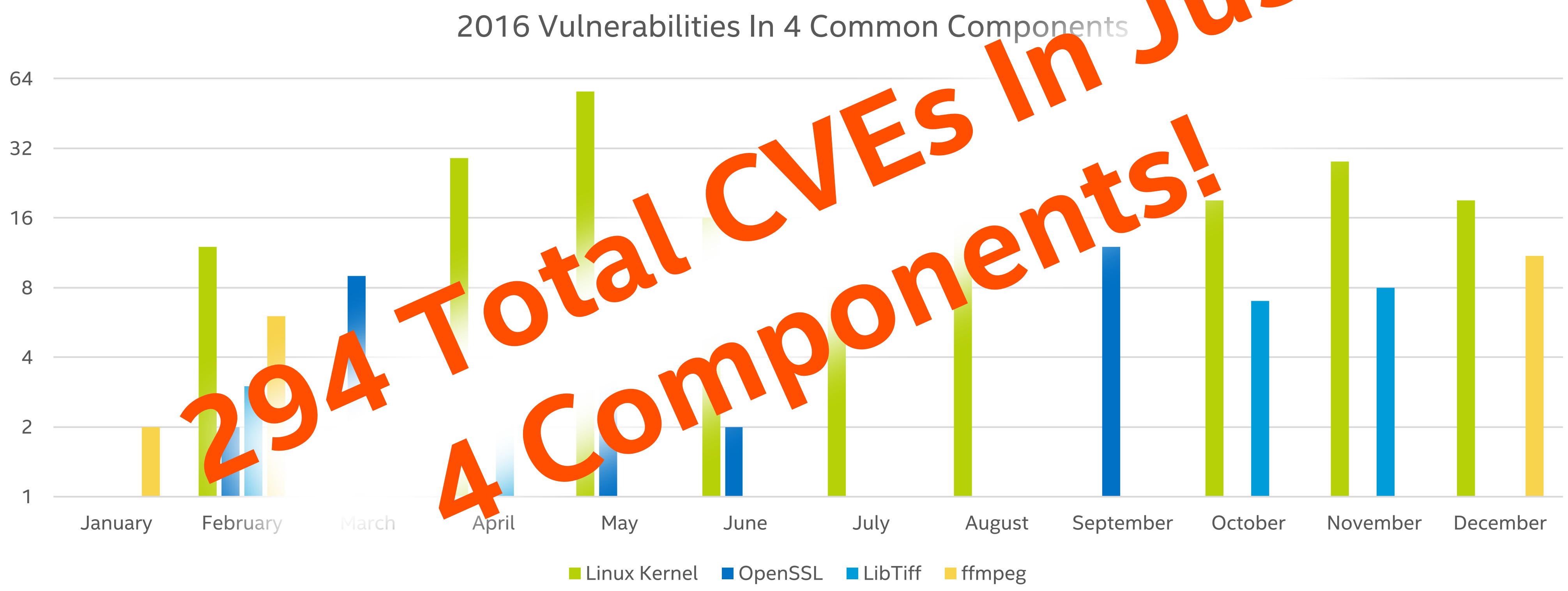
- Source Code
- Object Code
- Libraries
- Executables
- Dependencies
- Environment

IS IT SECURE?

LIVE
MAKE GIFS AT GIFS OM
BLOGGIF
7:40:20 PM
MAKE GIFS AT GIFSOUP.COM

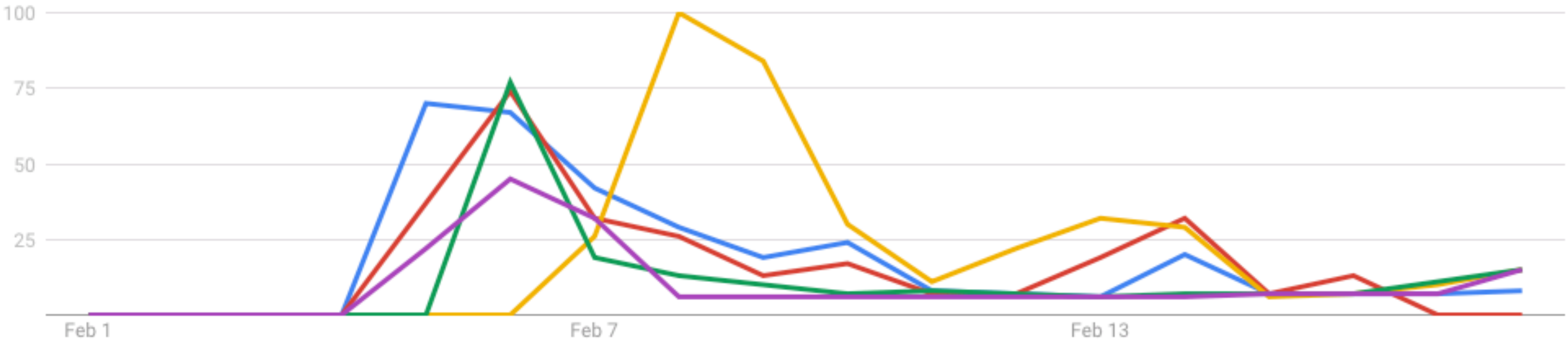
IS IT COMPROMISED?

IS IT VULNERABLE?



294 Total CVEs In Just 4 Components!

HOW QUICKLY CAN A KNOWN VULNERABILITY BE EXPLOITED?



- "Hacked By MuhmadEmad"
- 923k hits

- "Hacked By SA3D HaCk3D"
- 628k hits

- "by w4l3XzY3"
- 368k hits

- "Hacked By Imam"
- 241k hits

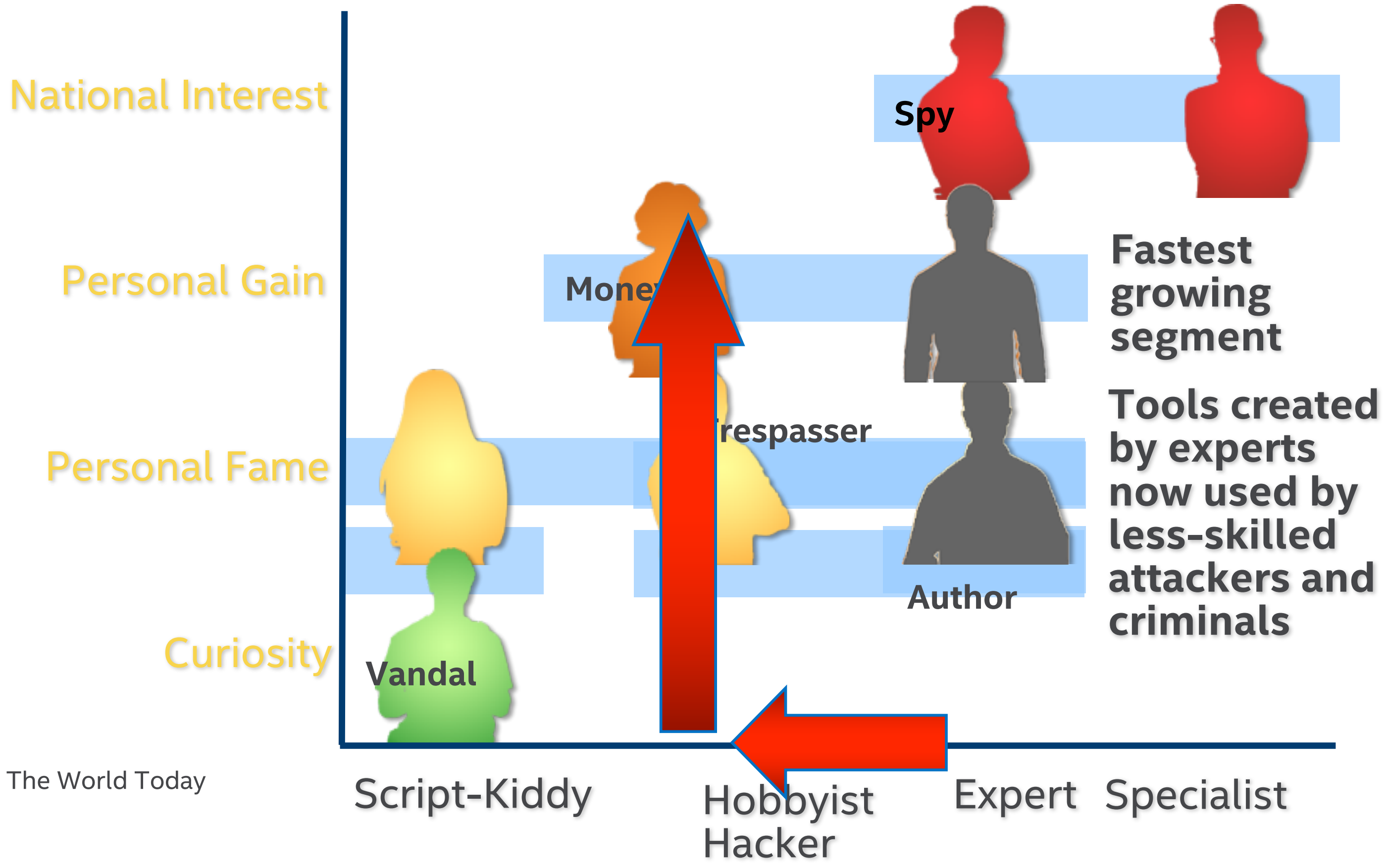
- "Hacked By BALA SNIPER"
- 169k hits

* Hits from Google on 2/20/17

WHO ARE FINDING THE VULNERABILITIES?

NOT YOUR MOTHER'S HACKER

SECURITY HACKERS ECOSYSTEM



Fastest growing segment

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

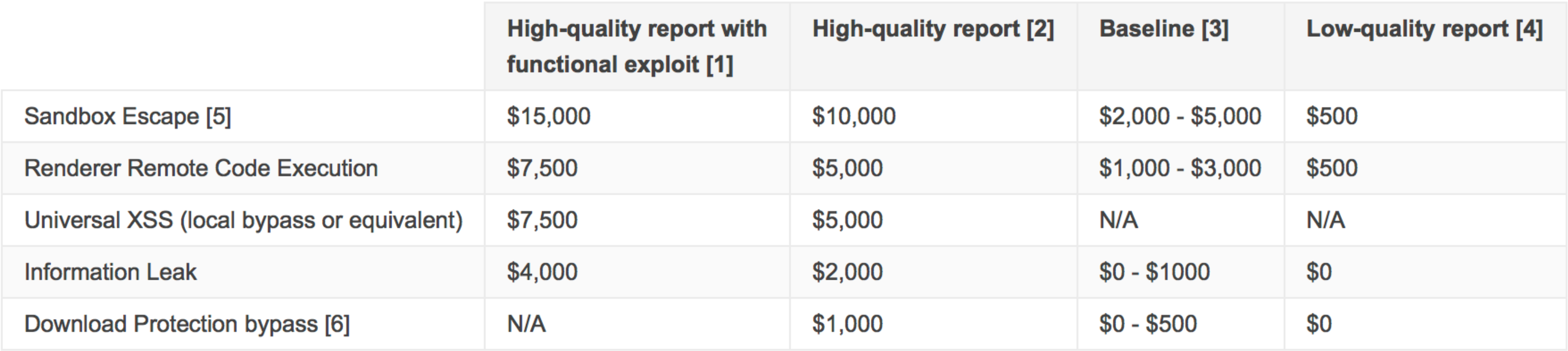
The World Today

BUG BOUNTY PROGRAMS

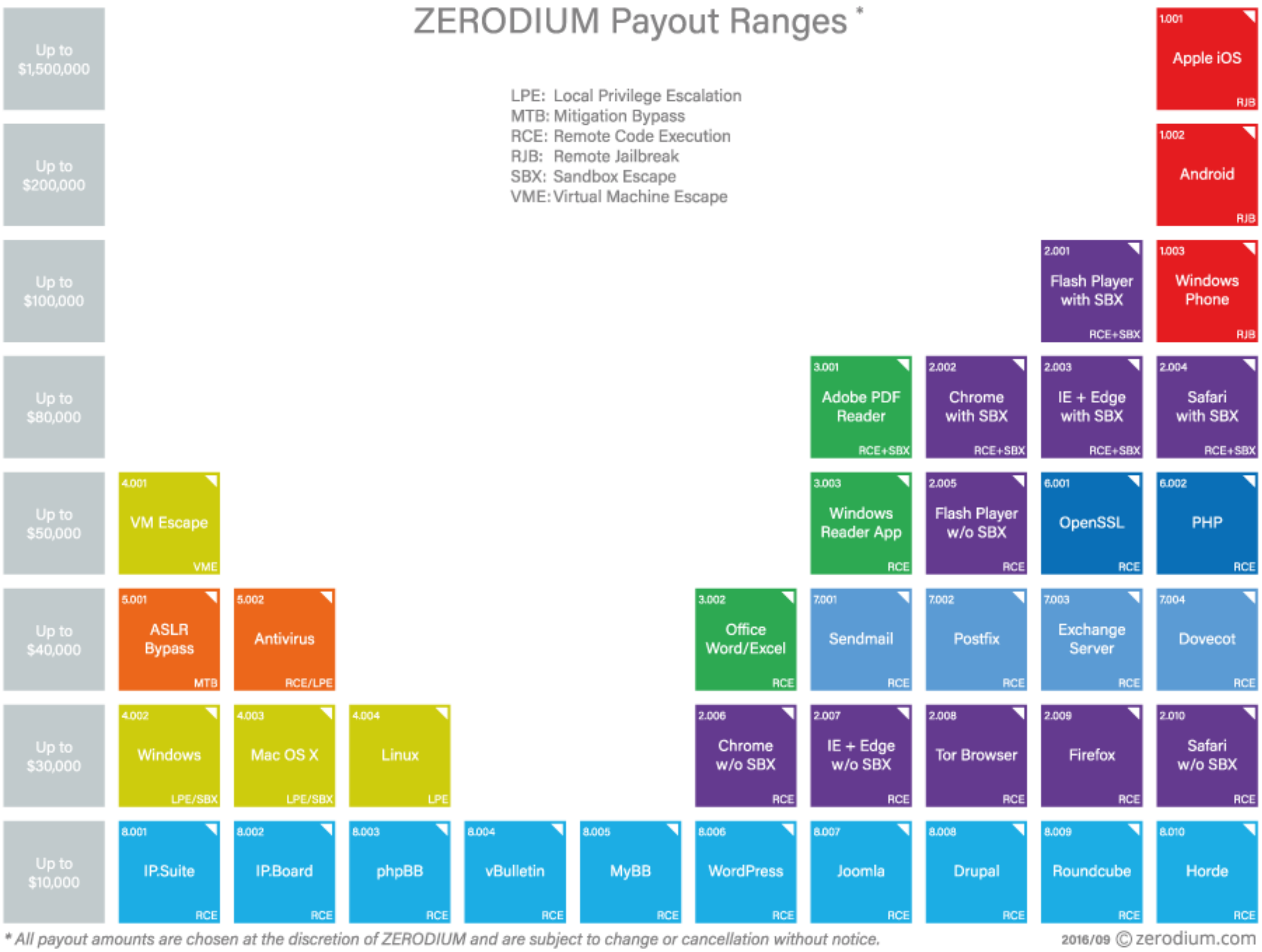
- ”A bug bounty program is a deal offered by many websites and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to exploits and vulnerabilities.” – Wikipedia [1]
- First well known program created by Netscape
- Bug bounty 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.



	High-quality report with functional exploit [1]	High-quality report [2]	Baseline [3]	Low-quality report [4]
Sandbox Escape [5]	$15,000	$10,000	$2,000 - $5,000	$500
Renderer Remote Code Execution	$7,500	$5,000	$1,000 - $3,000	$500
Universal XSS (local bypass or equivalent)	$7,500	$5,000	N/A	N/A
Information Leak	$4,000	$2,000	$0 - $1000	$0
Download Protection bypass [6]	N/A	$1,000	$0 - $500	$0



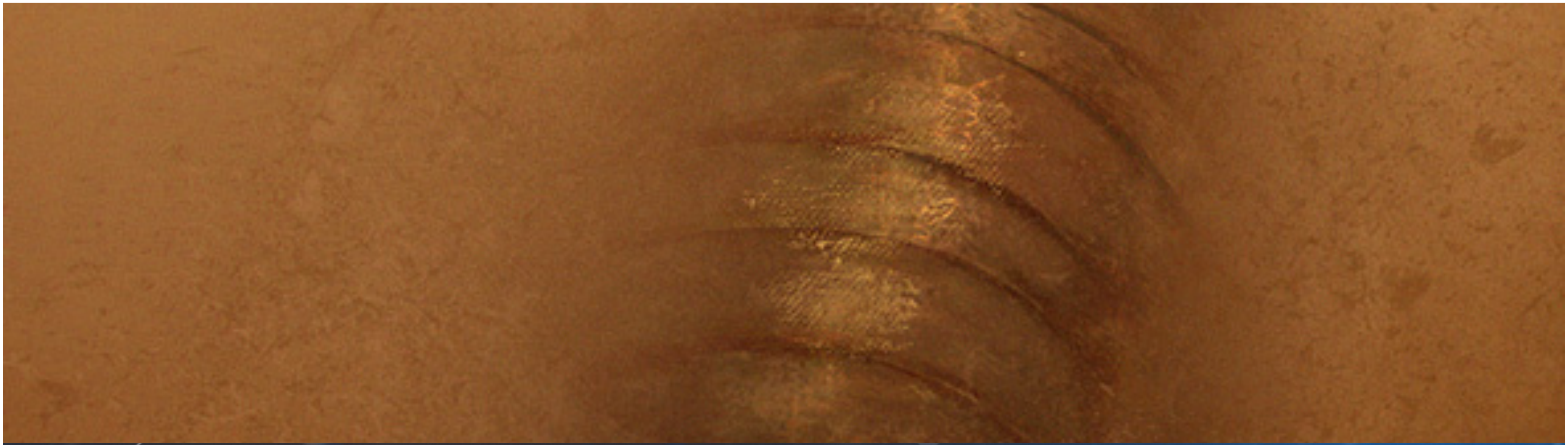
ZERODIUM Payout Ranges *

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

Up to $1,500,000										1.001 Apple iOS RJB
Up to $200,000										1.002 Android RJB
Up to $100,000									2.001 Flash Player with SBX RCE+SBX	1.003 Windows Phone RJB
Up to $80,000							3.001 Adobe PDF Reader RCE+SBX	2.002 Chrome with SBX RCE+SBX	2.003 IE + Edge with SBX RCE+SBX	2.004 Safari with SBX RCE+SBX
Up to $50,000	4.001 VM Escape VME						3.003 Windows Reader App RCE	2.005 Flash Player w/o SBX RCE	6.001 OpenSSL RCE	6.002 PHP RCE
Up to $40,000	5.001 ASLR Bypass MTB	5.002 Antivirus RCE/LPE				3.002 Office Word/Excel RCE	7.001 Sendmail RCE	7.002 Postfix RCE	7.003 Exchange Server RCE	7.004 Dovecot RCE
Up to $30,000	4.002 Windows LPE/SBX	4.003 Mac OS X LPE/SBX	4.004 Linux LPE			2.006 Chrome w/o SBX RCE	2.007 IE + Edge w/o SBX RCE	2.008 Tor Browser RCE	2.009 Firefox RCE	2.010 Safari w/o SBX RCE
Up to $10,000	8.001 IP.Suite RCE	8.002 IP.Board RCE	8.003 phpBB RCE	8.004 vBulletin RCE	8.005 MyBB RCE	8.006 WordPress RCE	8.007 Joomla RCE	8.008 Drupal RCE	8.009 Roundcube RCE	8.010 Horde RCE

* *All payout amounts are chosen at the discretion of ZERODIUM and are subject to change or cancellation without notice.*

2016/09 © zerodium.com

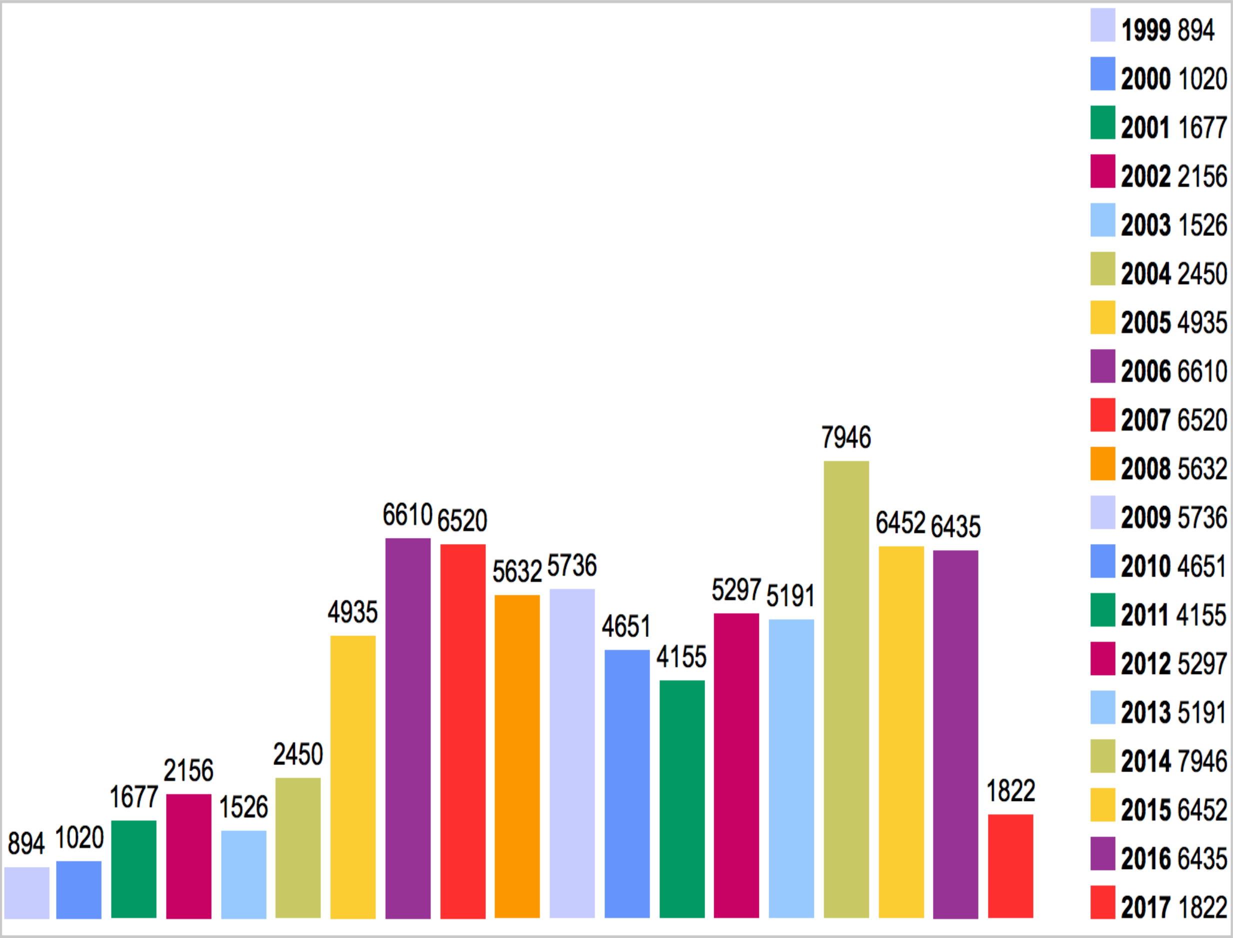


OK. CAN WE GET BACK TO THE CVE THING?

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!

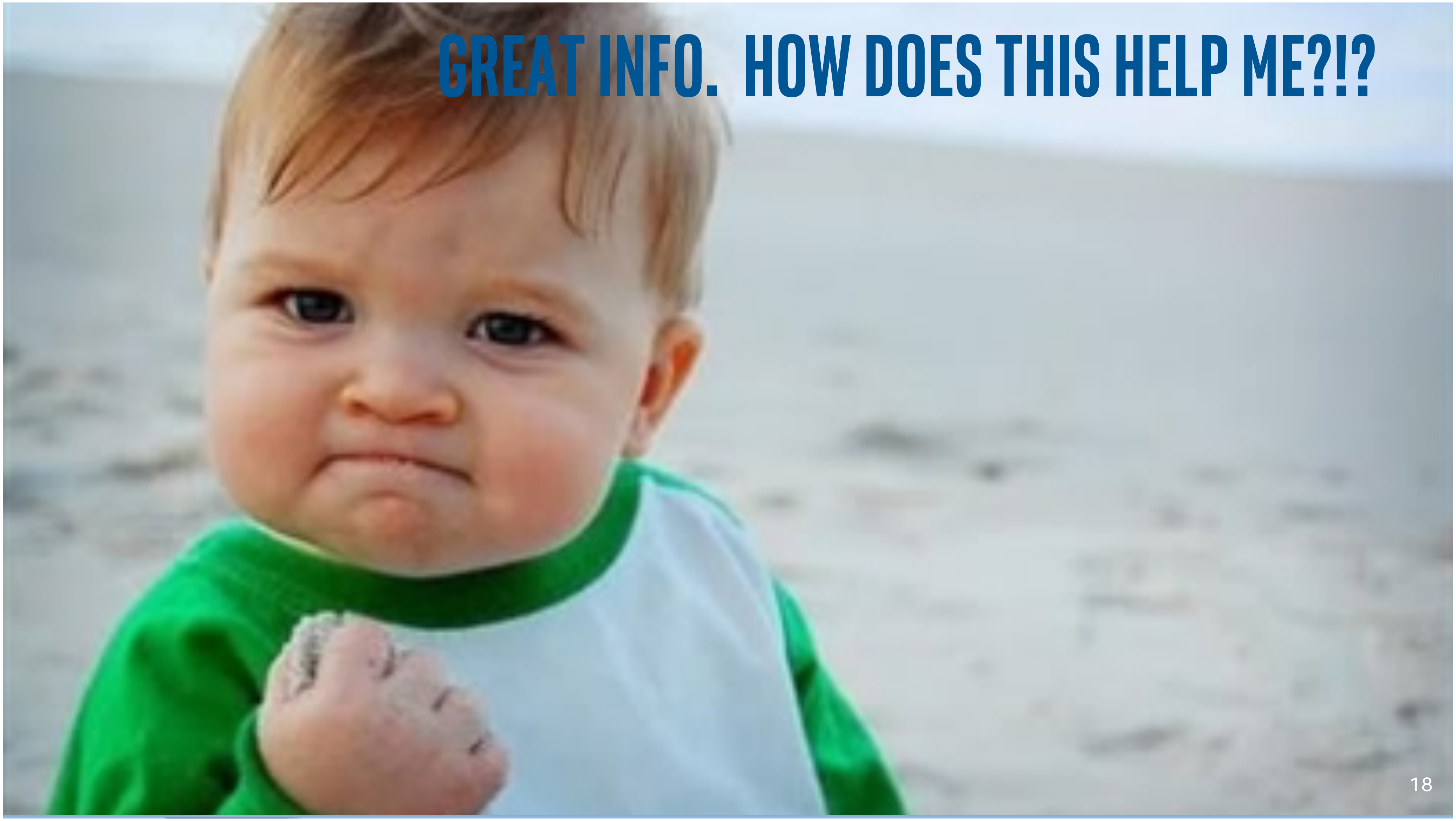
Vulnerabilities By Year



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?!?



SURVIVABILITY

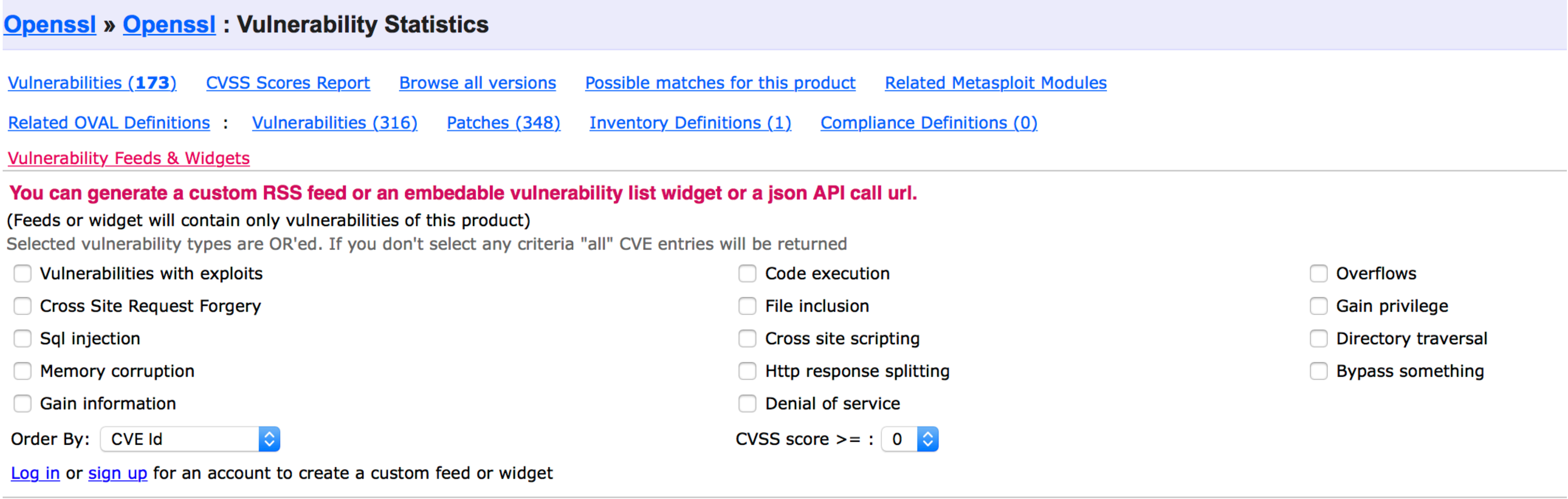
- You **must** include an update mechanism of some type in your product!
  - If you don’t, the message to your customers is, “We don’t care about you.”
- Make it **easy** for your customers to update
  - If it’s painless, they’ll do it more often
  - Make it completely transparent as long as you tell 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

☐ Overflows
☐ Gain privilege
☐ Directory traversal
☐ Bypass something

Order By: CVE Id

CVSS score >= : 0

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?