Security Level:

TLP:WHITE

Advanced Use of Bug Bounty Programs to Improve Vulnerability Response

2022 TF-CSIRT Meeting & FIRST Regional Symposium Europe

TTE Lab Germany

Version: V1.0 (2022-03-02)

BUILDING A BETTER CONNECTED WORLD

Huawei Technologies Duesseldorf GmbH

HUAWEI EUROPEAN RESEARCH CENTER

Introduction

Key driver: how to make best use of vulnerability reports to improve the security posture ***even more***

Plan

- Vulnerability handling and bug bounty at Huawei
- Acting on a high profile / novel vulnerability
- Example of Vulnerability Research techniques

Your speaker:

François Ambrosini

Role: Responsible Disclosure and Vulnerability Management Evangelist

Email: francois.ambrosini@huawei.com

LinkedIn: https://www.linkedin.com/in/fambrosini

HUAWEI PSIRT Is the Safeguard to Reduce the Risk of Customer Network

In 2011, Huawei released the Statement on Establishing a Global Cyber Security Assurance System approved by Huawei's CEO, Mr. Ren Zhengfei. The Statement says that "Taking on an open, transparent and sincere attitude, Huawei is willing to work with all governments, customers and partners through various channels to jointly cope with cyber security threats and challenges from cyber security." It is under this principle that Huawei PSIRT carry out the work of vulnerability response.

PSIRT Core Values

1. Responses to all security vulnerabilities and promotes the product line to reduce and minimize vulnerability effect
2. Investigates all possible affected products, and avoid the same vulnerability recurrence on live network, through new version or product has been deployed

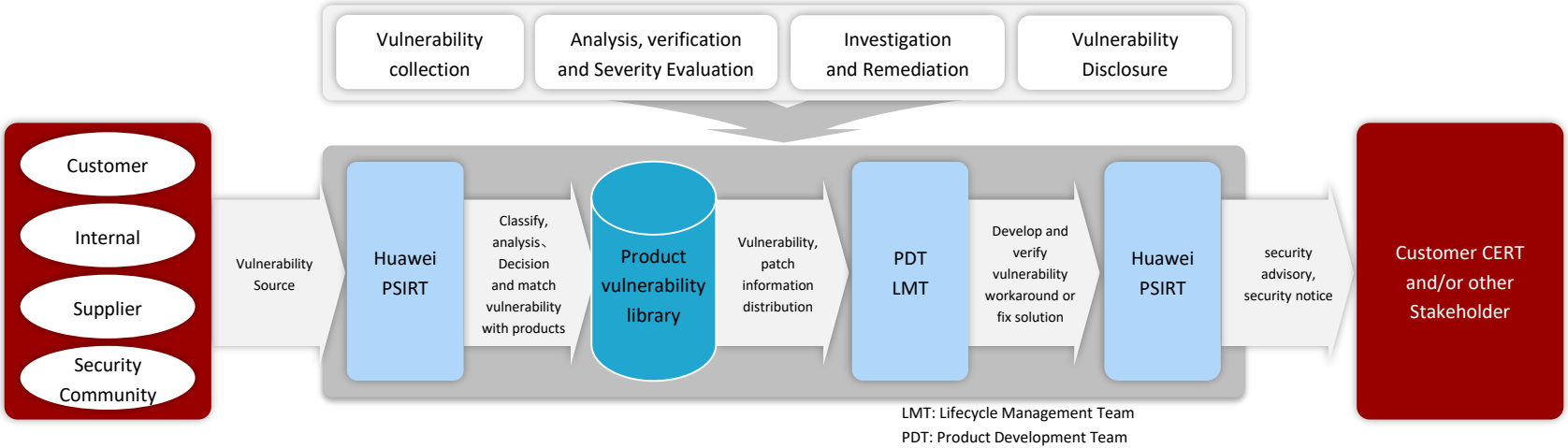
Product Security Vulnerability Response Process

Vulnerability Collection	Analysis, verification and Severity Evaluation	Investigation and Remediation	Disclosure
• Proactively monitor vulnerability • Timely response the report vulnerability • Monitor industrial trend	• Reproduce vulnerability • Vulnerability evaluation	• Instruction of investigation • Technique support to product line	• Release Security Advisory • Version management of Security Advisory

- Product security vulnerability response process has been insert into IPD
- PSIRT enforces product line to improve product security through case learning and training

PSIRT: Product Security Incident Response Team IPD: Integrated Product Development

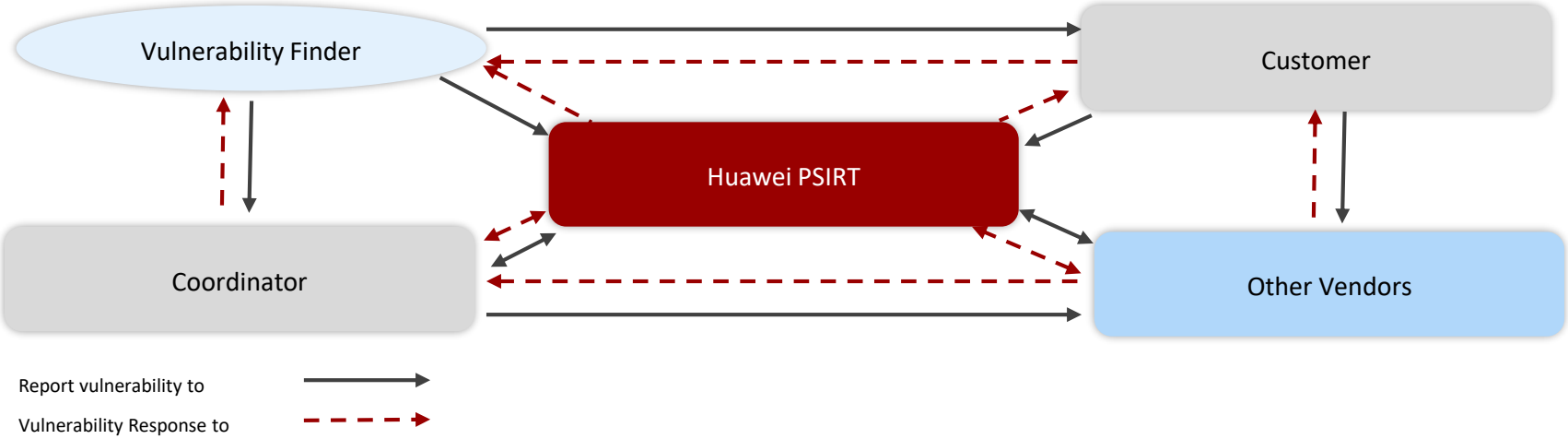
We are enhancing our vulnerability management and disclosure policies and procedures to match best practice and cater for the new Business Groups



- Learn from the industry's vulnerability management best practices: CVSS, CPE, CVRF, ISO/IEC 29147, ISO/IEC 30111 etc.
- PSIRT response to the vulnerability of the self-development, open source and third-party components, speed up response to the vulnerabilities which are already in the wild

We adopt responsible disclosure principle for vendors, CERT organizations and security researchers. We coordinate the resolution of the product vulnerability

Trustworthiness + Transparency + Mitigation + Improvement

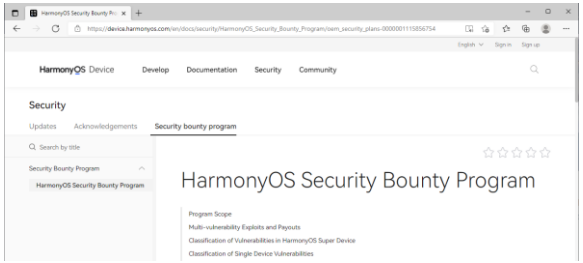


- Responsible disclosure implies that the vulnerability finder and vendor work together diligently to produce a timely resolution to reduce user's risks associated with the vulnerability

Why bug bounty programs?

Leverage to power of the crowd and access top talent

- Huawei runs both public and private, invitation-only, bug bounty programs
- We follow industry practice: define clear rules for researchers to look for vulnerabilities in a vendor‘s products or services and get rewarded on success.



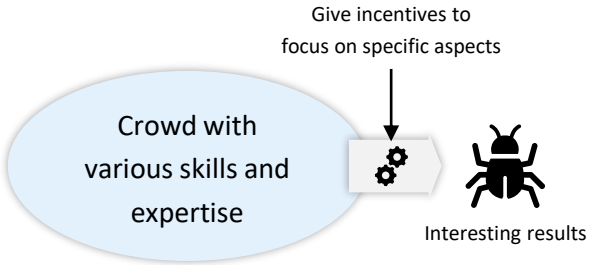
https://device.harmonyos.com/en/docs/security/HarmonyOS_Security_Bounty_Program/oem_security_plans-0000001115856754

The reward-based approach allows to steer the vulnerability research effort

- Opportunity for ad-hoc access to external talents with required expertise
- Focus on specific aspects of a system or on specific security threats – scoping has stronger effect when there is an incentive

Allows to achieve higher goals

- Outsider’s look complement internal security effort
- Vendor‘s promise (possibly with the help of a trusted platform) gives confidence to vulnerability researchers that they can embark on a „hacking journey“
- Established trust between vendors and researchers allows vendors to share assets in confidence



Let´s act!

What to do when a high profile or innovative vulnerability is found

Vulnerability reported

Remediation

Vulnerability end-to-end handling process

Learning

What can be learned from the vulnerability report? Improvements in Secure Development Lifecycle in terms of prevention…

- Prevent similar bugs from happening again (e.g. documentation, ready-to-use solutions based on best practices, etc.)
- Kill the vulnerability class (e.g. prevent null pointer dereference)
- Introduce exploit mitigations (e.g. ASLR)

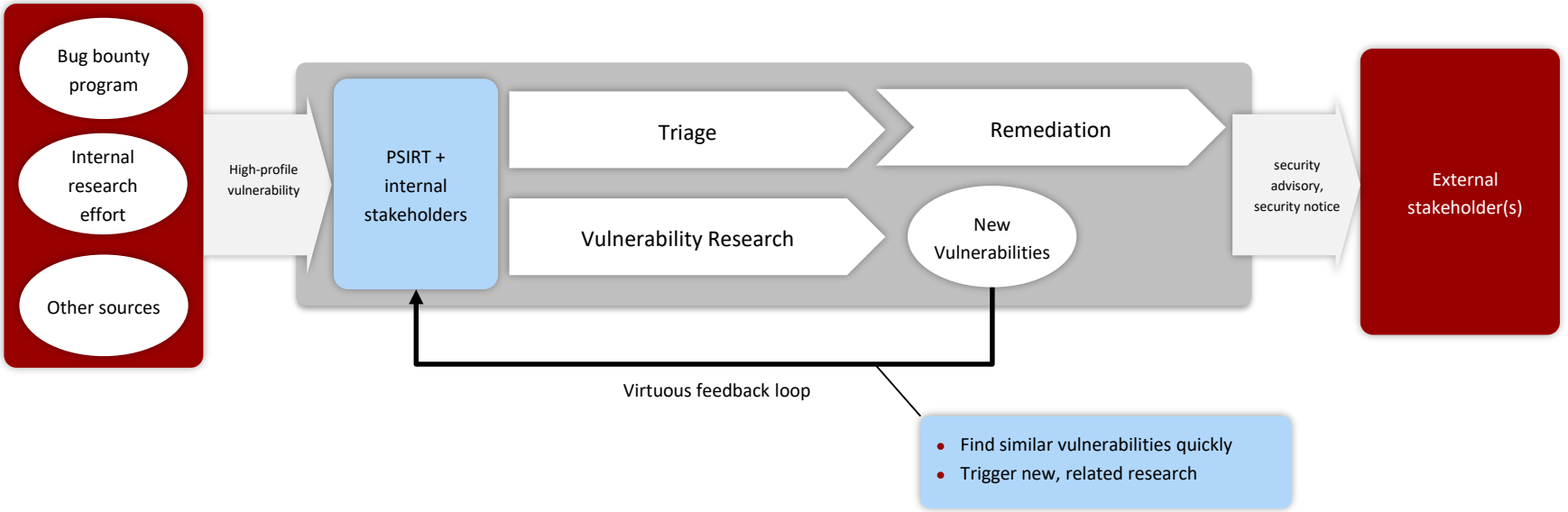
… and detection

- Expand automated security review of products

What about **right now**?

- Do „variations“ of this vulnerability currently exist in the code, in other codebases or other products?

Finding variations



Vulnerability Research

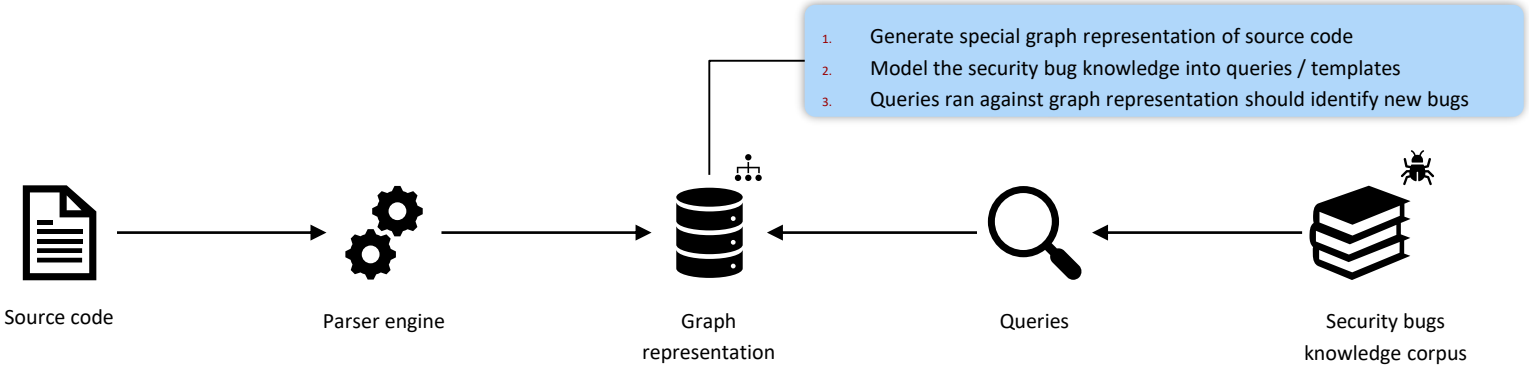
Definition: A process used to find flaws in software and hardware, that could lead to security issues.

In our context we want it informed, i.e. we start from the knowledge gained from a vulnerability report. Three methods will be presented:

- Variant analysis
- Fuzzing
- Manual code review

Variant Analysis

Definition: the process of using known vulnerabilities as a starting point to find similar problems in the code. Relies on modelling.

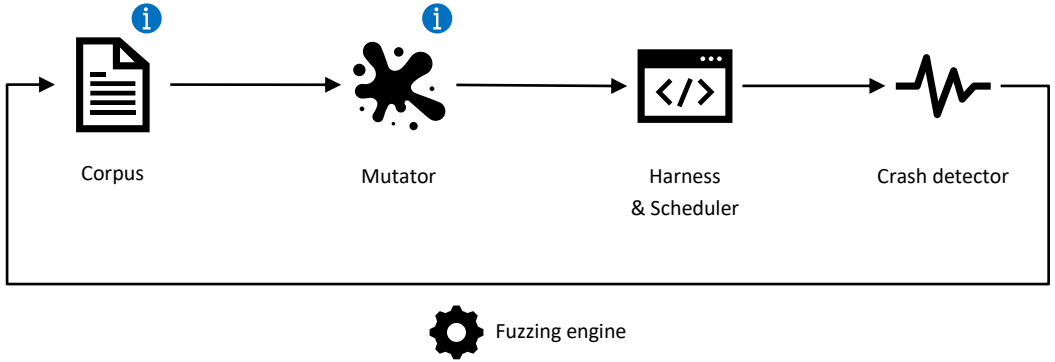


Tooling:

Coccinelle (INRIA et al.)	Joern (Shiftleft)	Weggli (Google Project Zero)
CodeQL (GitHub / Semmle)	SemGrep (r2c)	

Fuzzing

Definition: Dynamic software testing methodology that aims to find bugs by feeding the Software Under Test with (random) data and observe its behavior.



The *corpus* and the *mutator* are key components that can be configured according the information gained from a previous vulnerability report

Fuzzer types & examples:

- Format and grammar
  - Peach
  - Sully
  - Codenomicons
- Feedback-driven
  - AFL
  - LibFuzzer
- Sanitizers
  - ASAN
  - UBSAN

Manual code review

Manual code review

- Learning and get out of comfort zone
- Imagination
  - Think like an attacker / bad actor
- Curiosity
  - What actually happens if I just do this?
  - Has anyone tried to apply $topic to $asset?
  - What does this novel vulnerability tell us about the system?

Combined with right incentives for teams

Overcome research bias, innovate and find new types of vulnerabilities

vs.

Automation

- Very useful: speeds up the finding of vulnerabilites based on known problems
- Shortcommings
  - Requires learning the problem in the first place
  - Lacks many aspects of imagination

Combined with wrong Key Performance Indicators

Vunerability Research bias

Key takeaways & Community feedback

- A vendor‘s vulnerability handling processes can be enhanced with a feedback loop to maximaly leverage knowledge gained from reports
- Existing techniques in vulnerability research can be reused for this purpose
- Dedicated efforts such as bug bounty programs and funded research are key to find relevant (high-profile & innovative) vulnerabilities
- We are keen to get feedback from the Community on feasibility / experience

JOIN US IN

BUILDING A BETTER CONNECTED WORLD

THANK YOU

HUAWEI EUROPEAN RESEARCH CENTER

Security Level:

TLP:WHITE

Thanks

TTE Lab Germany

Version: V1.0 (2022-03-02)

BUILDING A BETTER CONNECTED WORLD

Huawei Technologies Duesseldorf GmbH

HUAWEI EUROPEAN RESEARCH CENTER