Introduction to vulnerability disclosure

Erik Silfversten, RAND Europe
20 January 2019

Introduction to vulnerability disclosure

1. What are vulnerabilities?
2. What is vulnerability disclosure?
3. Who is involved in vulnerability disclosure?
4. What are the different types of vulnerability disclosure?


enisa
Good Practice Guide on Vulnerability Disclosure
From challenges to recommendations
NOVEMBER 2015

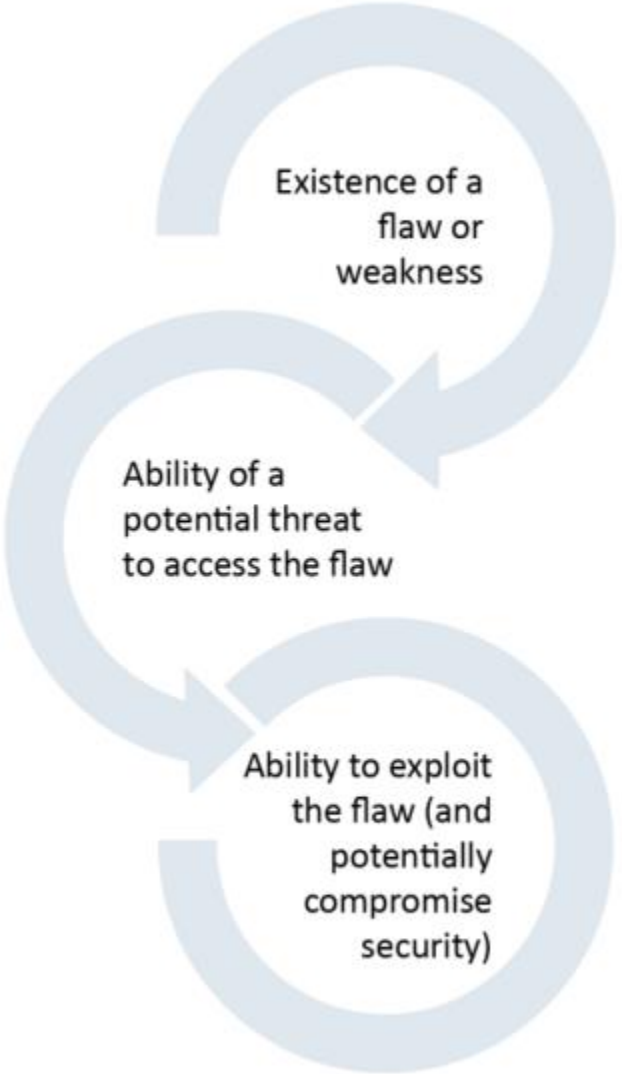

enisa
Economics of vulnerability disclosure
DECEMBER 2018

What are vulnerabilities?

A vulnerability is a weakness of software, hardware or online service that can be exploited or, more broadly, functional behaviour of a product or service that violates an implicit or explicit security policy.

ISO/IEC 29147:2018

Three characteristics of a vulnerability



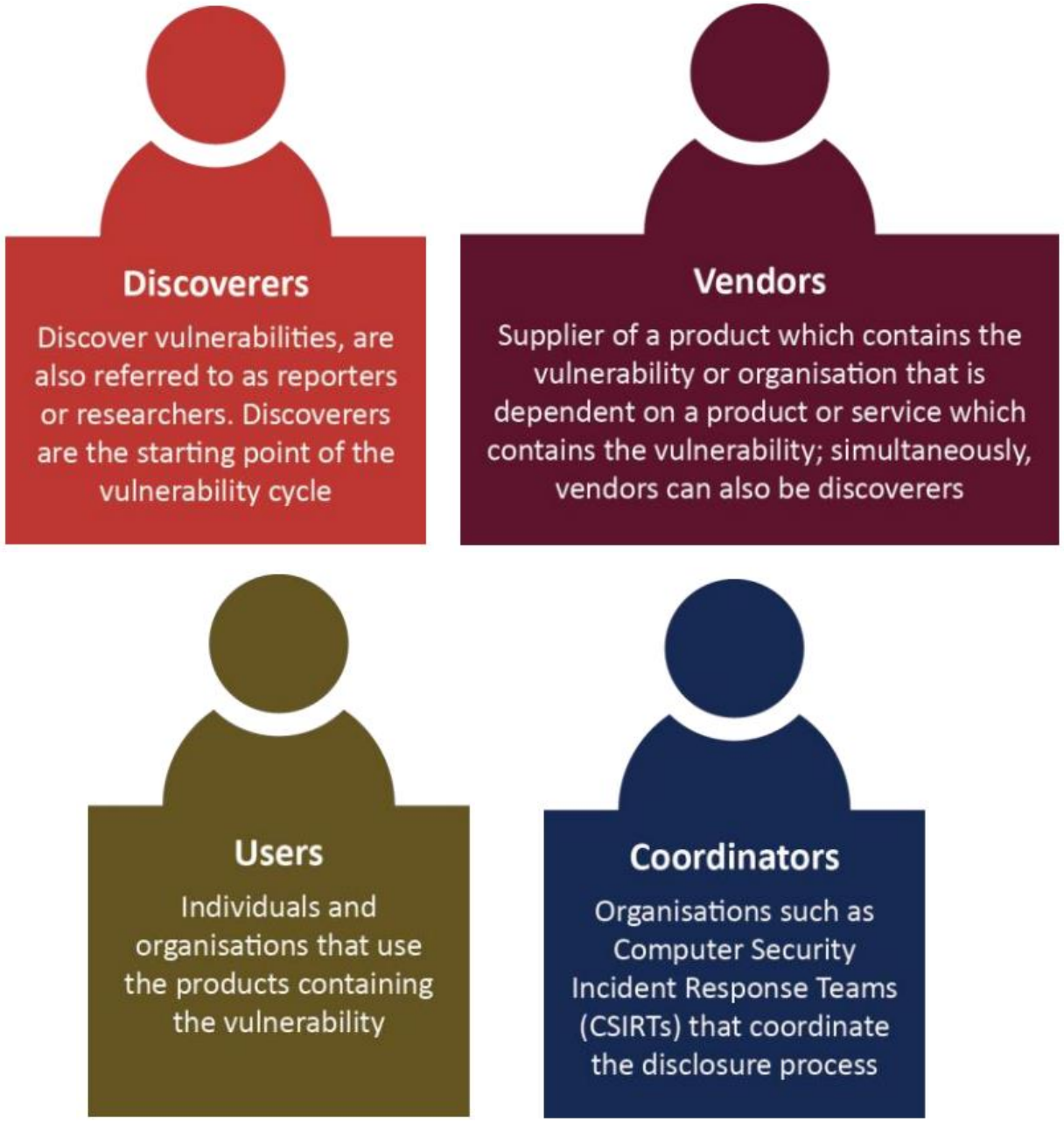
ENISA (2015)

What is vulnerability disclosure?

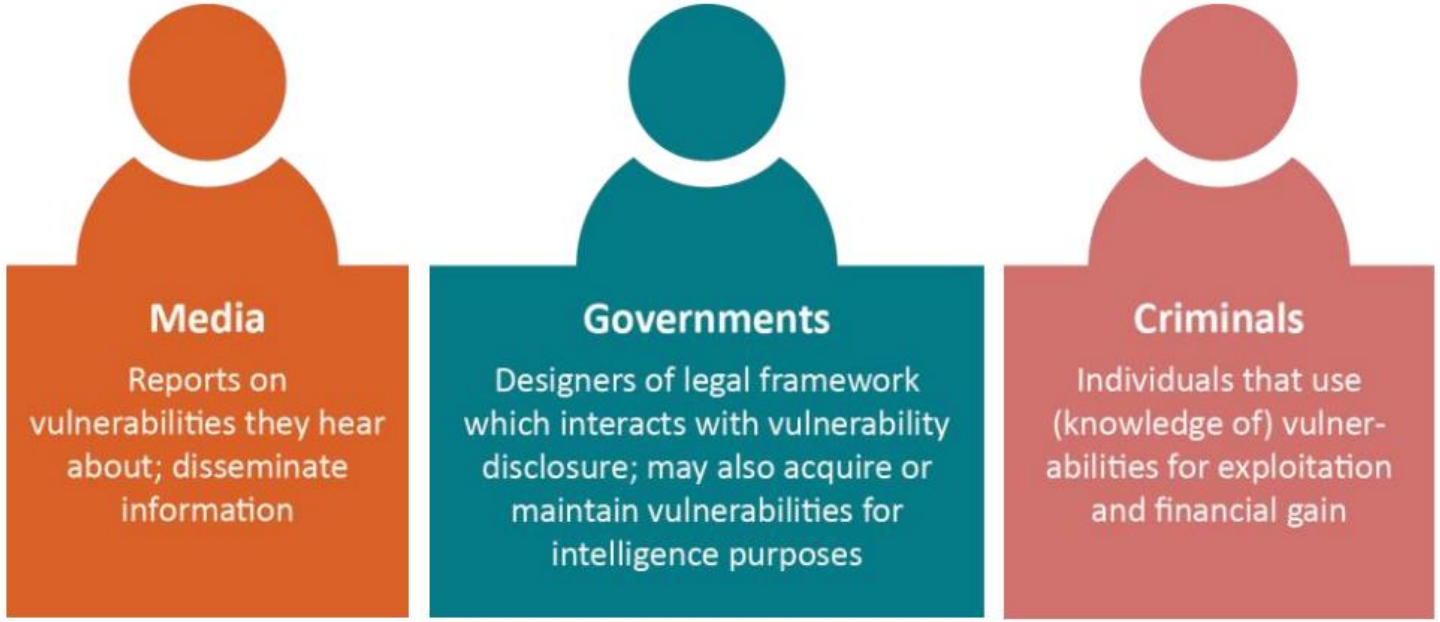
The act of initially providing vulnerability information to a party that was not believed to be previously aware. The overall disclosure process typically includes multiple disclosure events.

ISO/IEC 29147:2014

Who is involved in vulnerability disclosure?


Discoverers
Discover vulnerabilities, are also referred to as reporters or researchers. Discoverers are the starting point of the vulnerability cycle
Vendors
Supplier of a product which contains the vulnerability or organisation that is dependent on a product or service which contains the vulnerability; simultaneously, vendors can also be discoverers
Users
Individuals and organisations that use the products containing the vulnerability
Coordinators
Organisations such as Computer Security Incident Response Teams (CSIRTs) that coordinate the disclosure process

ENISA (2015)


Media
Reports on vulnerabilities they hear about; disseminate information
Governments
Designers of legal framework which interacts with vulnerability disclosure; may also acquire or maintain vulnerabilities for intelligence purposes
Criminals
Individuals that use (knowledge of) vulner-abilities for exploitation and financial gain

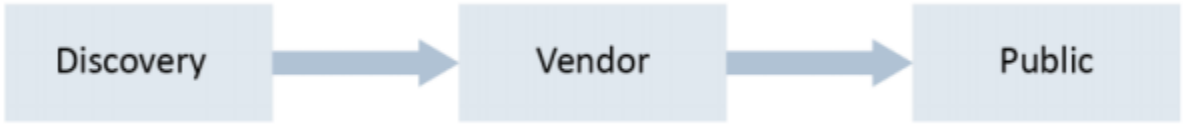
ENISA (2015)

Different types of disclosure

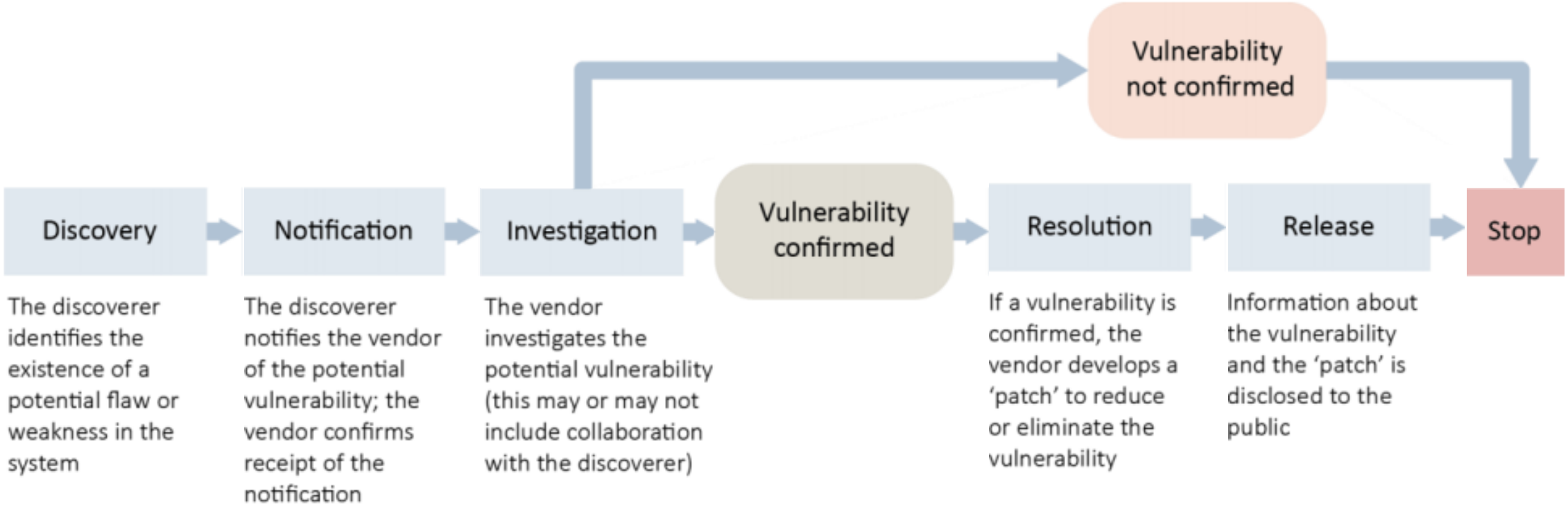
Non-disclosure

Full disclosure

Responsible disclosure

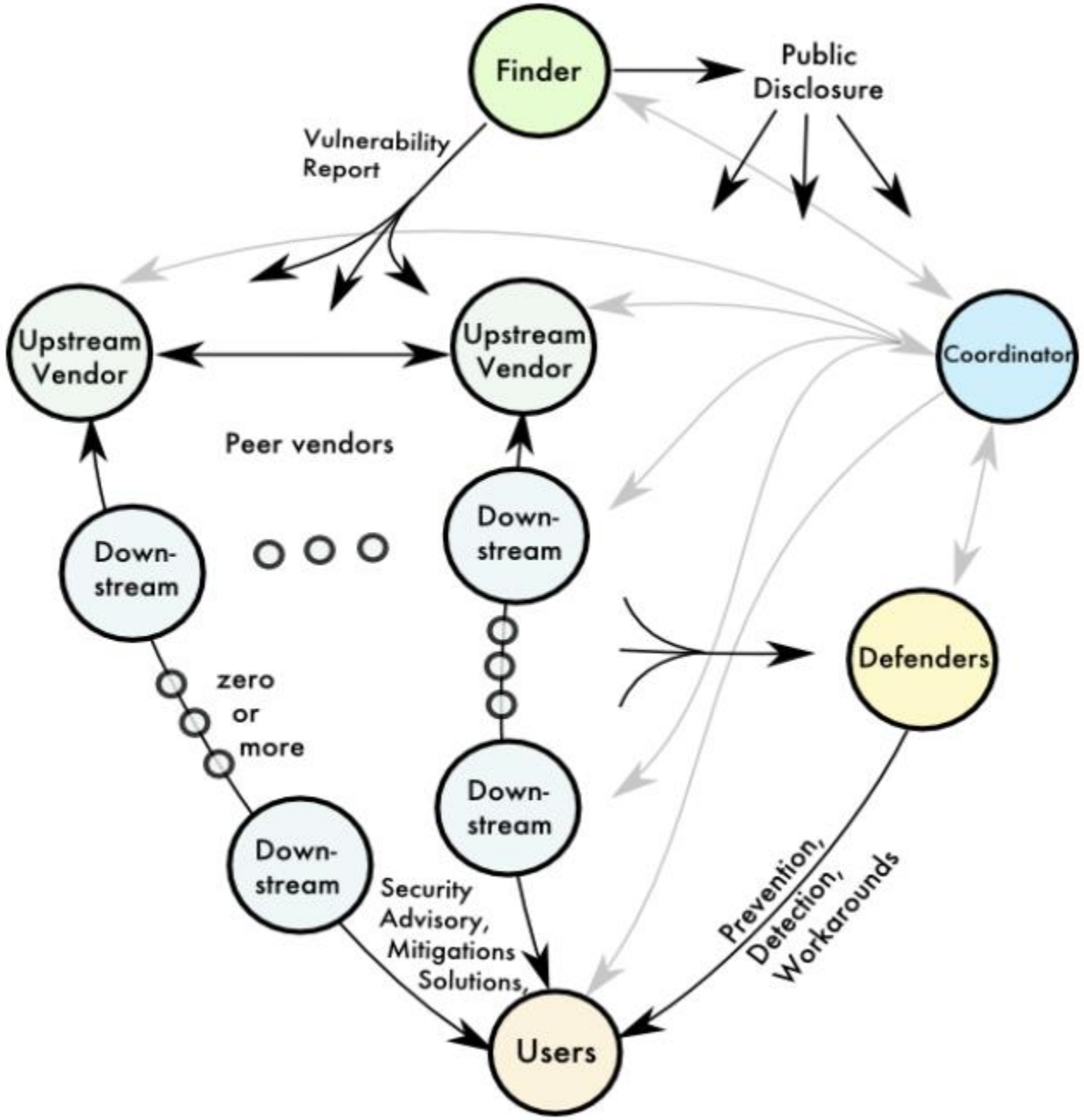


Simplified responsible disclosure process



ENISA (2015)

However, things are not always as simple



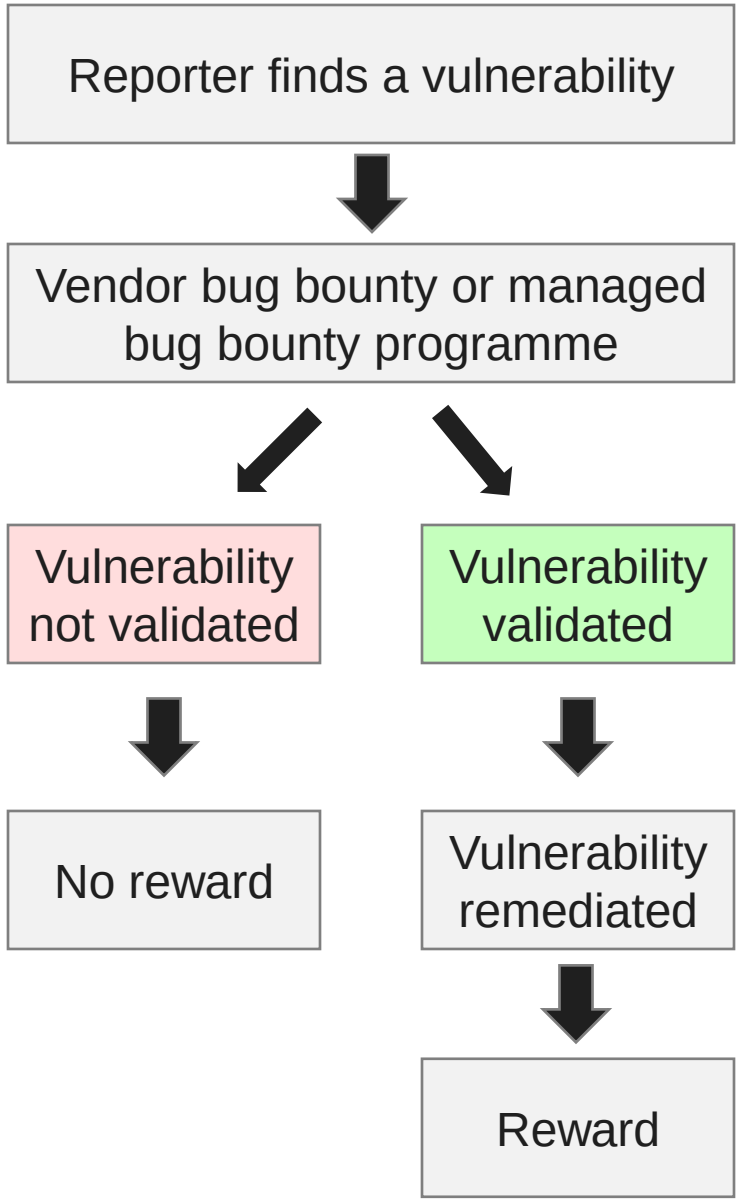
FIRST (2017)

Common responsible disclosure challenges

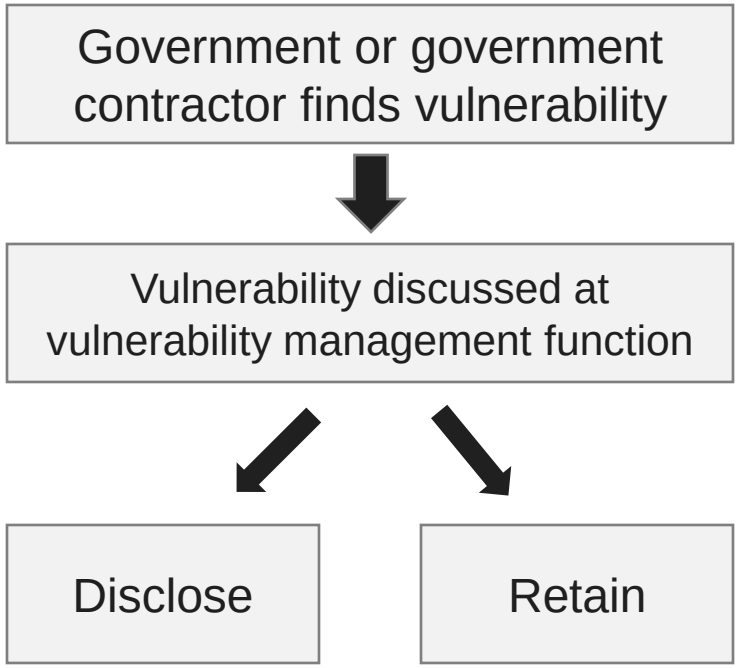
- Reporter cannot find a vendor contact or the vendor does not reply to the reporter.
- Reporter and vendor do not agree that the vulnerability report is valid.
- Reporter discloses the vulnerability to put pressure on vendor to release appropriate patch.
- The number of vulnerable vendors it too large for the finder to deal with.
- Reporter is motivated by public recognition or fame.
- Reporter has legal concerns with the disclosure process.
- Active exploitation of the vulnerability is discovered.

FIRST (2017)

Bug bounty programmmes



Government vulnerability management



Government vulnerability management

- How much is the vulnerable system used in the core Internet infrastructure, in other critical infrastructure systems, in the U.S. economy, and/or in national security systems?
- Does the vulnerability, if left unpatched, impose significant risk?
- How much harm could an adversary nation or criminal group do with knowledge of this vulnerability?
- How likely is it that someone else will discover the vulnerability?

References

ENISA. 2015. Good practice guide on vulnerability disclosure: https://www.enisa.europa.eu/publications/vulnerability-disclosure

ENISA. 2018. Economics of vulnerability disclosure: https://www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure

FIRST. 2017. Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure: https://www.first.org/newsroom/releases/20170706

ISO/IEC 29147:2018: Vulnerability disclosure: https://www.iso.org/standard/72311.html

Thank you

esilfver@rand.org