ISO Standards for the Vulnerability Disclosure

TASK FORCE ON SW VULNERABILITY DISCLOSURE IN EUROPE

Brussels, 27/09/2017

Gianluca Varisco


Digital
Transformation
Team

Appropriate disclosure - Advantages

As stated in the **CERT Guide to Coordinated Vulnerability Disclosure**, CVD is a **process** intended to **minimize adversary advantage** while an information security vulnerability is being mitigated.

Appropriate vulnerability responses **reduce the population of vulnerable product instances as quickly as possible** and **the impact of attacks against vulnerable systems.**

Inappropriate disclosure - Risks

Inappropriate disclosure of a vulnerability could not only delay the deployment of the vulnerability resolution but also give attackers hints to exploit it. That is why vulnerability disclosure should be carried out appropriately.

ISO/IEC 29147:2014(E) - Scope

- This ISO standard gives guidelines for the disclosure of potential vulnerabilities in products and online services.
- It details the methods a vendor should use to address issues related to vulnerability disclosure.
- Starting **April 2016**, you can download it for **FREE** from ISO.org: https://goo.gl/c7DCA2

ISO/IEC 29147:2014(E) - Scope

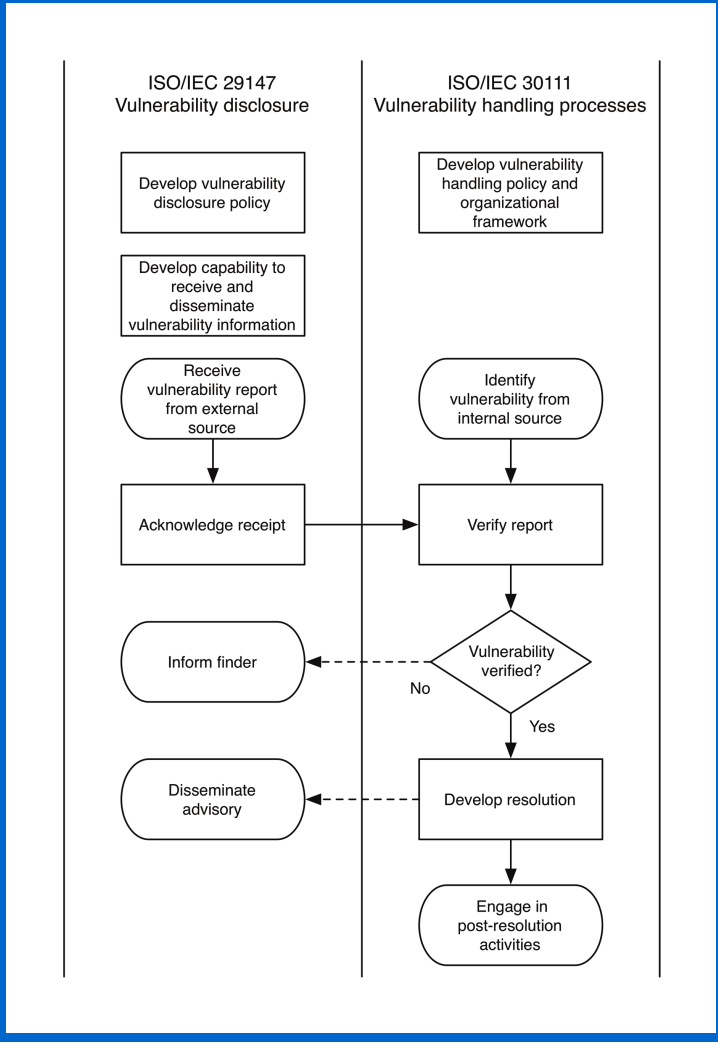
- Useful for **vendors**, as it provides:
  - guidelines on how to receive information about potential vulnerabilities in their products or online services
  - guidelines on how to disseminate resolution information about vulnerabilities in their products or online services
  - the information items that should be produced through the implementation of a vendor's vulnerability disclosure process, and examples of content that should be included in the information items.

Normative references

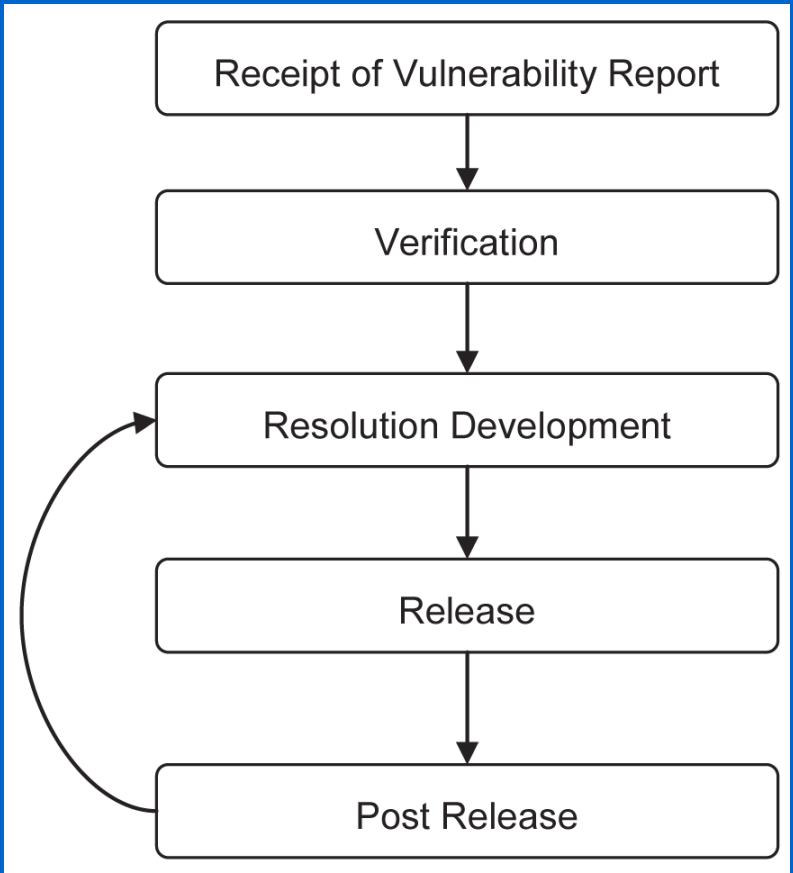
- ISO/IEC 27000:2012, Information technology — Security techniques — Information security management systems — Overview and vocabulary
- **ISO/IEC 30111, Information technology — Security techniques — Vulnerability handling processes**

ISO/IEC 29147 and ISO/IEC 30111

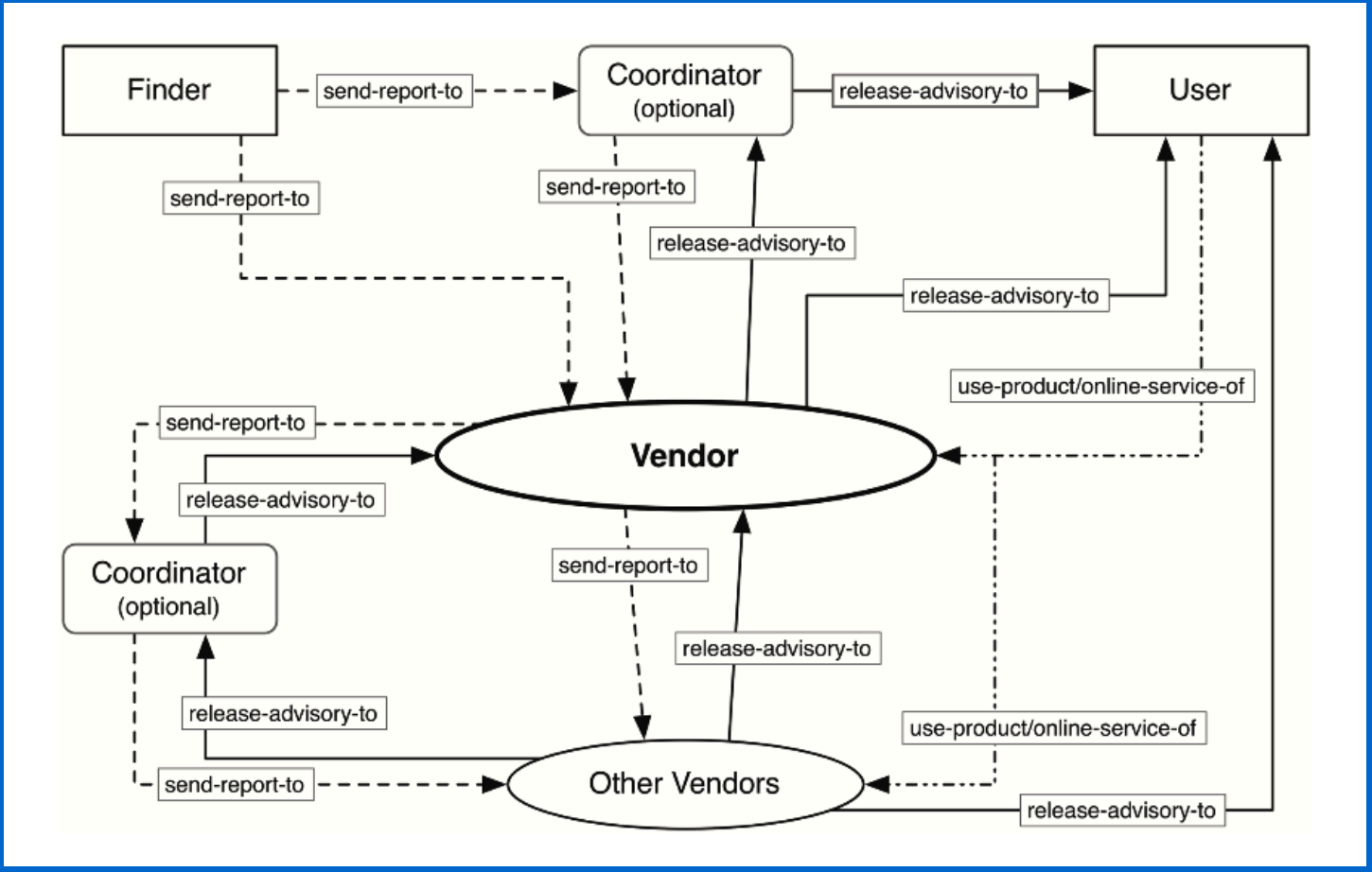
While **ISO/IEC 29147** deals with the interface between vendors and those who find and report potential vulnerabilities, **ISO/IEC 30111** deals with the investigation, triage, and resolution of vulnerabilities, regardless if the source of the potential vulnerability was external to the vendor or from within the vendor's own security, development, or testing teams.



ISO/IEC 30111: Disclosure Process



Vulnerability information exchange



Challenges and open QA

- Organizations are really facing a challenge in deciding which standards' framework to adopt and when
- Implementation and adoption by a broader audience
- ISO **and**/or the Dutch model (guidelines)?
- Standardize CVD policies across all member states (and harmonise them together with relevant legislations, eg. IP, Export Control, Cyber Criminal law, Data protection)

Contacts

Gianluca Varisco

- Email: gianluca@teamdigitale.governo.it
- Twitter: @gvarisco
- Medium: @gvarisco

Sito Web: https://teamdigitale.governo.it

DIGITAL
TRANSFORMATION
TEAM
Italian Government