A national program of Responsible Disclosure

Cybersecurity@CEPS Events - Brussels, 23/06/2017

Gianluca Varisco


Digital
Transformation
Team

Origin

Italian Government appointed **Diego Piacentini** as **Commissioner** for Digital Transformation of the Public Administration

Diego started his new job hiring a **team of tech-savvy people**

Vision

The “**operating system**”
of the country

Manifesto

- Security and privacy
- Obsessed by simplification
- Mobile first
- Open Source
- Data driven, using AI/ML
- … and more!

  (see teamdigitale.governo.it…)

Skills

- Big Data
- Content Design
- Cybersecurity
- Data Science
- Developer Relations
- Digital Payments
- Metrics & Analytics
- Mobile/Apps Developer
- Product & UX/UI
- Software Architects
- Software Developers
- Technical Project Managers

Programs

Programs

- SPID (secure digital identity)
- DAF (Data Analytics Framework)
- PagoPA (Digital Payments)
- Developer Community
- ANPR (Centralized registry on national population)
- API Marketplace
- **Responsible Disclosure**

Responsible Disclosure

Current status

Goals

What’s missing

What we are doing

How can you help?

Current status

- Reports are not being handled (acknowledgement, triaging, resolution) **in a timely manner**
- Partial feedback (**if at all**) given to the researcher
- There are no **standardised** guidelines

Goals

- **Simple**, but **effective** procedures to ease the acknowledgement of vulnerability reports
- **Quick response** in solving the bugs
- Useful interaction with the **ethical hackers**' community

What is missing

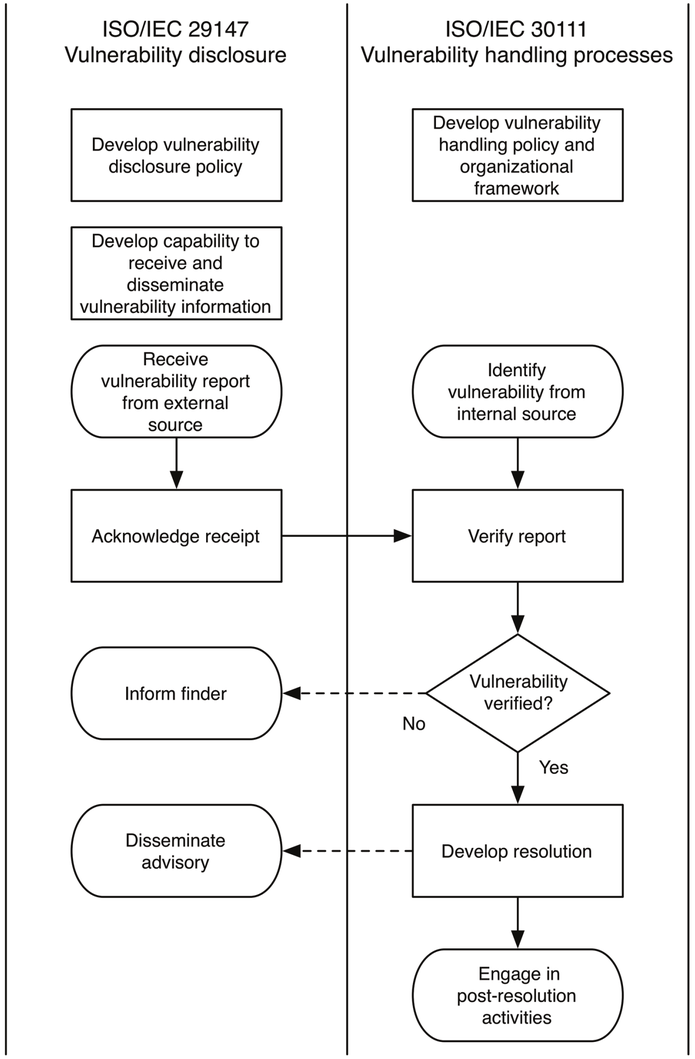
- A **simple procedure** for handling the vulnerability reports
- A complete **mapping of every asset** within the public administration, promptly shared with our national CERTs
- A **proper reference** (link, page) on corporate websites explaining the procedures to follow for reporting security bugs
- A direct (communication) channel standardised among every public administration, the private sector, national CERTs and researchers **who want to help**

What are we doing

- We’ve involved the CERT Nazionale (MISE) and CERT PA (AgID)
- A responsible disclosure policy is being **drafted**
- At the same time, we’re investigating the technical and legal frameworks (including the **legal protection** of the researcher) to meet our program’s requirements

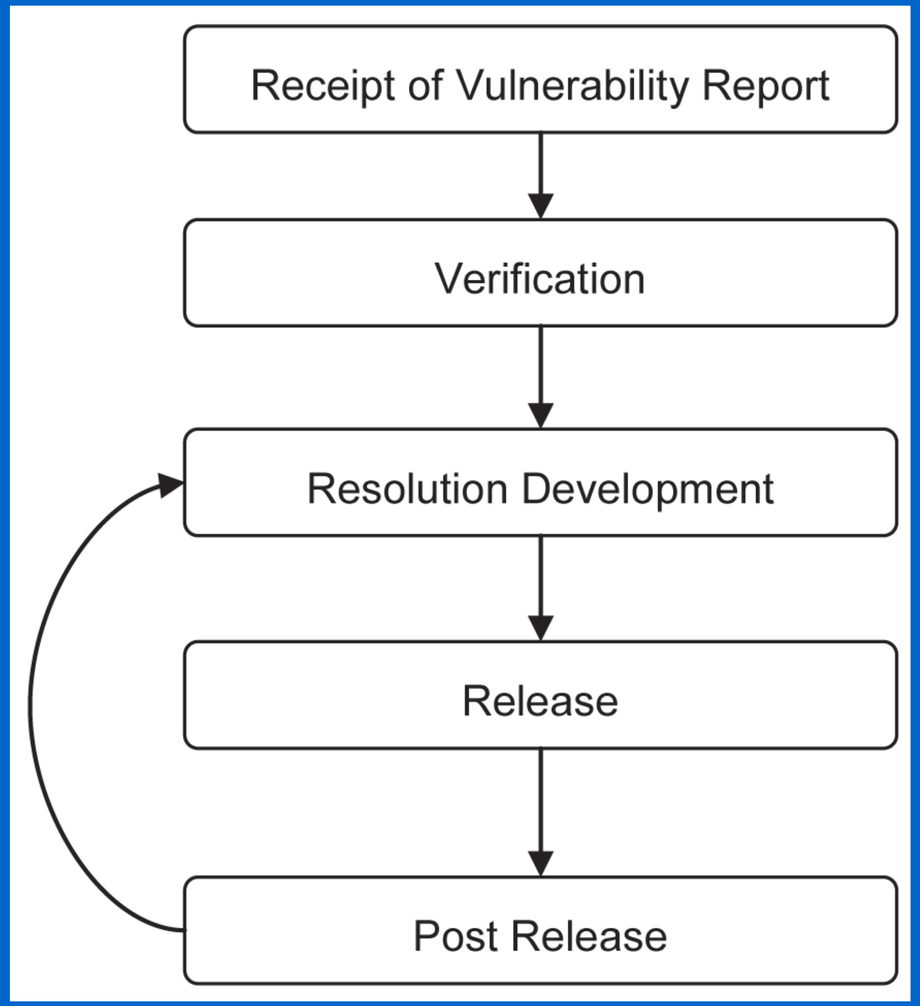
International standards

- **ISO/IEC 30111: Vulnerability handling processes**



International Standards

- **ISO/IEC 29147**
  Vulnerability disclosure



How can you help?

- **Collaborative revision of such policy**
- Definition of internal processes to handle security incidents
- Subscription and publication of such policy within your corporate websites
- Give us feedback!

Contacts

Gianluca Varisco

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

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

DIGITAL
TRANSFORMATION
TEAM
Italian Government