Task Force

Software Vulnerability Disclosure in Europe

Afonso Ferreira
French National Research Centre (CNRS)
Computer Science Research Institute at Toulouse (IRIT)
France
Quick background

• Researcher in Algorithms, Optimisation, Networks, Cybersecurity, Insurance, CPS
• Policy maker in Future and Emerging Technologies, Cybersecurity, Privacy at the European Commission (until end March 2017)
• Foresight designer and practitioner, mainly on the impact of the Digital Revolution and Digital Transformation
• Adviser to Institutions and to EU Projects
Vulnerability disclosure

The process by which someone shares information about a security vulnerability so that it can be mitigated or fixed

Types:

• Full disclosure
• Responsible disclosure
• Coordinated vulnerability disclosure
• No disclosure
Coordinated vulnerability disclosure

• Process of
  • Gathering information from vulnerability finders
  • Coordinating the sharing of that information between relevant stakeholders
  • Disclosing the existence of software vulnerabilities
  • Disclosing their mitigations to various stakeholders including the public

Finders: individuals or organisations that identify a potential software vulnerability in a product or service
Task Force
Software Vulnerability Disclosure in Europe

Sponsor:
- Centre for European Policy Studies – CEPS

Chair:
- Marietje Schaake, Member of European Parliament

Research Group:
- Romain Bosc, Rapporteur
- Afonso Ferreira, Rapporteur
- Lorenzo Pupillo, Coordinator
- Gianluca Varisco, Rapporteur
Members of the Task Force

- **Private Sector:** Airbus, Cloudflare, Enter, ETNO, ICANN, Mozilla, Microsoft, SAP

- **European Institutions:** Council of European Union, DG Connect, DG Home Affairs, JRC European Commission

- **European Governments:** Dutch National Cyber Security Center

- **Civil Society:** Access Now

- **Advisory Committee:**
  - Ross Anderson, Cambridge University;
  - Michael Daniel, Cyber Threat Alliance,
  - Allan Friedman, NTIA,
  - Andriani Ferti, Karatzas & Partners Law Firm,
  - Trey Herr, Belfer Center Harvard University,
  - Tim Watson, Warwick University.

*In conversations with CERTs and ENISA*
Methodology

**Exploration**
- Consultations with Task Force members.
- CEPS will draft short papers and submit them to members before each meeting to serve as the basis for discussions.

**Meetings**
- Based on the short papers submitted by CEPS to members in advance of each meeting.
- Targeted presentations by members and invited experts.
- Debate among members.

**Final Report**
- CEPS independent research.
- Members' comments and observations on the body of the final report.
- Members' consensus on the list of policy conclusions and proposals.

**Launch**
- Open meeting in Brussels.
- Panel with stakeholders/policy makers.
- Wide media coverage.
- Printed copies of the final report distributed to key stakeholders.
Events

First meeting
• Held on September 27\textsuperscript{th}, 2017 in Brussels

Next meetings
• November 29\textsuperscript{th}
• January 31\textsuperscript{st}
Questions?

Want to contribute?

Afonso.Ferreira@irit.fr