The challenges for vulnerability disclosure in cybersecurity

kaspersky

How we work

- "Vulnerability Report": 10-year program for RVD and vulnerability handling
- Global Transparency Initiative (GTI) and Bug Bounty Program with awards of up to $100k for the most critical flaws: 63 bugs have been resolved, 23 reports – rewarded with total bounties = $46,250
- Partnering with Dislose.io to offer safe harbor for security researchers
- Sharing best practices with policy makers through public consultations, 2018 CEPS study on Software VD in Europe
- Code of Conduct to published soon

Challenges

1. Lack of normative/legislative practices, incl.:
    - Aligned terminology, clearly defined actors and processes, designated industry-specific competent authorities and contact points;
    - Use case law and open liability question;
    - Risks of uncoordinated multi-party vulnerability disclosure;
2. Risks of too prescriptive strict administrative measures, incl.:
    - Unreasonable timeframes for vulnerability disclosure;
    - Measures sanctioning public security investigations.
3. Lack of trust and conflicting interests of the parties; lack of clearly established and trusted communication channels, and financial/time/reputational costs due to a delay in response from affected vendors;

Challenges

4. Insufficient transparency in vulnerability disclosure and remediation plans/activities; risks of disclosure to unnecessary third parties and the likelihood of information leaks that could enable malicious actors and harm users;

5. Lack of accessible means to unilaterally deliver mitigations to vulnerabilities (in case of global software/hardware supply chains);

6. Legal/compliance risks for security researchers;

7. Immature process and lack of RVD code of conduct in industry.

Institutional set-up

Fragmented regulation vs. borderless ICTs

Patching

Thank you!

Anastasiya.Kazakova@Kaspersky.com