Recommendations from a Report of a CEPS Task Force

Software Vulnerability Disclosure in Europe

Technology, Policies and Legal Challenges

27 February 2018

Chair: Marietje Schaake, Member of European Parliament

Coordinator: Lorenzo Pupillo, Associate Senior Research Fellow, CEPS

Rapporteurs: Afonso Ferreira, Directeur de Recherche CNRS
Gianluca Varisco, Italian Digital Transformation Team

Participants of the CEPS Task Force on Software Vulnerability Disclosure in Europe

Chair: Marietje Schaake, Member of the European Parliament

Coordinator: Lorenzo Pupillo, Associate Senior Research Fellow, CEPS

Rapporteurs: Afonso Ferreira, Directeur de Recherche CNRS and Gianluca Varisco, Cybersecurity Expert, Italian Digital Transformation Team

Research Assistant: Antonella Zarra, CEPS

Advisory Board

Ross Anderson, Professor of Security Engineering at Computer Laboratory, University of Cambridge

Andriani Ferti, Senior Associate Karatzas & Partners Law Firm

Allan Friedman, Cybersecurity Director, US National Telecommunications and Information Administration

Tim Watson, Director of the WMG Cyber Security Centre, University of Warwick

Companies and European Organisations

Jochai Ben-Avie, Senior Global Policy Manager, Mozilla

Mariano Cunietti, Chief Technology Officer, Enter

Jeroen van der Ham, National Cyber Security Centre, The Netherlands

Lise Fuhr, Director General, European Telecommunications Network Operators

Caroline Greer, Head of European Public Policy, Cloudflare

Evgeny Grigorenko, Head of Public Affairs, Europe, Kaspersky Lab

Baiba Kaskina, CERT Latvia and Chair TF-CSIRT

Stephane Lenco, Chief Information Security Officer, Airbus

Jan Neutz, Cybersecurity Policy Director, EMEA, Microsoft

Jan-Jacque Sahel, Vice President for Global Stakeholder Engagement, Europe and Civil Society, ICANN

Corinna Schulze, Director, EU Government Relations, Global Corporate Affairs, SAP

Mark Smitham, Senior Manager, Microsoft

European Institutions

Laurent Beslay, Project Leader, Joint Research Centre, European Commission

Monika Kopcheva, Political Administrator, Council of the European Union

Aristotelis Tzafalias, Policy Officer, Cybersecurity and Digital Privacy, European Commission

Claudia Warken, Policy Officer, DG Home Affairs, European Commission

Mathias Vermeulen, Policy Advisor to MEP Marietje Schaake, European Parliament

Civil Society

Jens-Henrik Jeppesen, European Policy Director, Center for Democracy and Technology

Lucie Krahulcova, EU Policy Associate, Access Now

Academia

Stefano Fantin, Legal Researcher, Centre for IT and IP Law, Katholieke Universiteit Leuven

Extra -EU Organisations

Uchiyama Takayuki, CERT Japan

Introduction

This document puts forward the main recommendations for the design and the implementation of a forward-looking policy on Software Vulnerability Disclosure (SVD) in Europe. It is the result of a collective effort led by CEPS, which in September 2017 formed a Task Force on Software Vulnerability Disclosure in Europe, composed of industry experts, representatives of EU and international institutions, academics, civil society organisations and practitioners (see a list of participants in the Annex). The Task Force explored ways to formulate guidelines for governments and businesses to harmonise the process of handling SVD throughout Europe and formulate policy recommendations for member states and the EU institutions in the development of an effective policy framework for introducing processes of so-called Coordinated Vulnerability Disclosure (CVD) and Government Vulnerability Disclosure (GVD) processes in Europe.

Today, software is embedded in every connected device – our smartphones, our cars, our offices and our homes. This fact of 21st century life, however, means that most software and software-based products are susceptible to vulnerabilities (see definitions of key terms in the annex). It has been estimated that the average programme has at least 14 separate points of vulnerability.[1] Each of those weaknesses could permit an attacker to compromise the integrity of the product and exploit it for personal gain. Moreover, with the development of the "Internet of Things" (IoT) and billions of devices connected to the internet, software plays an ever-greater role in our daily lives. Indeed, the attack surface is becoming broader, which greatly increases the potential impact of vulnerabilities on the ecosystem. Large attacks, such as Wannacry, have shown that vulnerabilities can be used to construct exploits that can put unprecedented pressure on critical infrastructure. Software vulnerabilities pose a serious concern for individuals, companies and governments alike. What can we do to protect ourselves? Who should search for vulnerabilities and should the vendors or the users be informed about them?

Coordinated vulnerability disclosure (CVD) and government vulnerability disclosure (GVD)

Coordinated vulnerability disclosure is a process by which we can mitigate/eradicate the potential negative impacts of vulnerabilities. It can be defined as "the process of gathering information from vulnerability finders, coordinating the sharing of that information between relevant stakeholders, and disclosing the existence of vulnerabilities and their mitigations to various stakeholders, including the public".[2] The process involves different actors such as finder, reporter, vendor, patch deployer and coordinator and encompasses various actions such as reporting, coordinating and publishing information about a vulnerability and its resolution. The main goals of CVD are to: i) ensure that identified vulnerabilities are addressed, ii) minimise the risk from vulnerabilities and iii) provide users with sufficient information to evaluate risks from vulnerabilities to their systems.[3] Input into this process includes vulnerability reports from vulnerability discovery, and its output takes the form of patches, vulnerability reports and database records.

The ***government vulnerability disclosure*** process involves the management of vulnerabilities discovered by government agencies and it focuses on the process by which the government determines when and how to announce the vulnerability in their possession.

The analysis of this Task Force shows that only a few countries across Europe have managed to put SVD processes in place. The Netherlands has been the most proactive member state in establishing vulnerability disclosure policies and has supported other member states to address their challenges and concerns. Supported by the Dutch Ministry of Security and Justice and the Public Prosecution Service, which supports and advocates this process, the government has a proper framework in place, as well as clear processes for

[1] "The myth of cyber-security", *The Economist,* 8 April 2017, p. 9.

[2] CERT Guide to Coordinated Vulnerability Disclosure", by Allen D. Householder, Garret Wassermann, Art Manion and Chris King, Software Engineering Institute, Carnegie Mellon University, August 2017, p. 3.

[3] ISO/IEC, "ISO/IEC 29147:2014 Information Technology-Security Techniques-Vulnerability disclosure", 2014.

reporting vulnerabilities, including protection of the researcher. Similarly, France has recently included vulnerability disclosure in its revised legislative framework - Law for a Digital Republic (Article 47). According to recent reports, Lithuania has joined these ranks and put in place a vulnerability disclosure framework, including a disclosure deadline, scheduled resolution and an acknowledgement report. In addition, some organisations in Lithuania have successfully established processes to receive and disseminate vulnerability information.

A significant barrier to the implementation of CVD policies across the EU is the lack of a single interpretation of what constitutes 'hacking' among the member states, which has led to the conflation of this term – typically associated with cybercrime in the EU – with security research and its role in vulnerability discovery as opposed to vulnerability disclosure. Therefore, the first step is to provide the necessary legal certainty to security researchers involved in vulnerability discovery as well as setting appropriate vulnerability disclosure processes through complementary guidance and best practices. Based on current best practices in Europe, the US and Japan, the Task Force recommends implementation of the following CVD-related policies.

CVD Policy. The Task Force calls upon the European Commission and the member states to collectively draft a European-level framework complemented by national legislation in accordance with the guidelines and recommendations defined in ISO/IEC 29147:2014 and ISO/IEC 30111 in order to provide legal clarity for software vulnerability discovery and disclosure. The National Cyber Security Centre (NCSC) in the Netherlands has published a general guideline for responsible disclosure, which can serve as a useful model that EU member states can follow in drafting their own responsible disclosure policy. In addition, it gives reporters guidance on how to act in finding and reporting a vulnerability.[4]

It's also worth mentioning that the Cybersecurity Unit, Computer Crime and Intellectual Property Section Criminal Division of the U.S. Department of Justice, in July 2017 released the first version of the framework for a "Vulnerability Disclosure Program for Online Systems"[5] that EU member states could examine as a possible model. Recognising that different organisations may have different goals and priorities for their vulnerability disclosure programmes, the US framework does not dictate the form of or objectives for vulnerability disclosure. Instead, the framework outlines a process for designing a vulnerability disclosure programme that will clearly describe authorised vulnerability disclosure and discovery behaviour, thereby substantially reducing the likelihood that such described activities will result in a civil or criminal violation of law.

The Task Force recommends that national CERTs (computer emergency response teams) should put in place frameworks that are similar to the ones adopted in the Netherlands and the US. Moreover, such frameworks should be prominently announced on the websites of organisations that establish a CVD, which researchers can consult and rely on for legal certainty.

Recommendations to implement CVD in Europe

National Legislation

1. **Amending national legislation to support CVD.** As a medium-to-long term solution and given that the revision of the EU cybercrime Directive (from 2013) may take several years, the Task Force recommends member states to consider amending their national legislation bearing on CVD, using the framework on CVD introduced in the Netherlands as a model. The Task Force acknowledges that such a recommendation may lead to certain discrepancies in the regulatory framework

[4] See https://www.ncsc.nl/english/current-topics/news/responsible-disclosure-guideline.html

[5] See https://www.justice.gov/criminal-ccips/page/file/983996/download

covering CVD across member states, but it would allow for the establishment of a safer environment for the security research community to report vulnerabilities until legislation addressing the relevant issues to a sufficient degree comes into effect at the EU level.

EU Legislation

2. **Amending Directive 2013/40/EU on attacks against information systems (the "EU cybercrime Directive") to support CVD**. In the context of a potential future revision of the EU cybercrime Directive, the European Commission should consider an amendment to the Directive that would allow for CVD if certain circumstances prescribed by law are met, thereby creating a safe environment for the security researcher community to report vulnerabilities that it identifies. Such an amendment would ensure a more harmonised interpretation of the relevant rules across the EU, and the security researcher community would have a clearer idea of what constitutes or not an infringement of the relevant laws.
3. **Protection of security researchers.** Researchers involved in vulnerability discovery are often exposed to criminal or civil liability.[6] The Task Force notes that there is no legal instrument at the European-level aimed at protecting security researchers and "white-hat hackers" from prosecution as part of vulnerability disclosure. Given the importance of their work to the overall security of society, the legal liability and responsibilities of security researchers should be fully clarified to enable them to continue their work without fear of prosecution.
4. **Incentives for security researchers**. This Task Force would welcome appropriate policies aimed at encouraging 'white-hat hackers' to actively participate in coordinated vulnerability disclosure programmes. No policy on this specific matter has yet been established at the EU level.
5. **Directive on security of network information systems (NIS).** Member states are currently developing their accompanying guidelines on the "technical and organisational measures", as prescribed in Article 14 of this Directive and falling with the scope of the Directive. Therefore, in transposing the NIS Directive, and particularly its Article 14, member states may explicitly consider including CVD as one of those measures. Furthermore, companies may proactively consider establishing CVD as part of their own "technical and organisational measures", since the NIS Directive leaves open the range of measures a company can take to ensure compliance with Article 14.
6. **General data protection Regulation (GDPR**). This Regulation comes into force in May 2018 and offers some relevant points that could serve to stimulate software vulnerability search and disclosure. According to the GDPR, software owners and tech firms become data controllers when they exercise overall control over the purpose for which, and the manner in which personal data are processed. Assuming that irresponsible handling of vulnerabilities could lead to personal data breaches falling within the scope of GDPR, CVD can be an effective tool to mitigate the relevant risks. Indeed, if a controller implements a CVD allowing vulnerabilities to be dealt with in a timely manner, then it may reduce the risk of incurring fines arising from possible breaches of confidentiality, availability or integrity of personal data under its Article 33. It is recommended that data protection supervisory authorities, together with relevant stakeholders, reflect on the role that CVD can play in ensuring the integrity of data and in mitigating risk.
7. **Cybersecurity Act.** According to the proposed Regulation submitted by the European Commission in October 2017 concerning the European Network and Information Security Agency (ENISA) and cybersecurity certification (the **Cybersecurity Act**), in its coordination and capacity-building roles, ENISA can contribute to the harmonised development of CVD in the EU by having its mandate amended, thereby allowing it to engage in the following activities:

[6] See https://techcrunch.com/2017/07/25/hungarian-hacker-arrested-for-pressing-f12/

- Writing EU-wide guidelines for the reporting process, addressing the issues it raised in its January 2017 "Good Practice Guide on Vulnerability Disclosure" report[7];
- Installing and operating a web portal where disclosure of software and hardware vulnerabilities can be coordinated at the European-level and contributed to anonymously. In the portal back-office ENISA would analyse the vulnerability, contact the owner/vendor/manufacturer of the software solution or hardware product, make sure that the vulnerability is safely patched, and keep a confidential record of all operations, in close coordination with ISACs (Information Sharing and Analysis Centers), CSIRTs (Computer Security Incident Response Teams), and the CSIRT network, for which it provides the secretariat. An 'assurance' seal for owners/vendors/manufacturers could be explored.
- Being entrusted with a team of "white-hat hackers" who would conduct campaigns to assist EU member states and operators of essential services to mitigate software vulnerabilities, with the objective of increasing the security of critical infrastructure;
- Implementing training in all issues that may arise in the context of CVD, e.g. technical, legal, etc., to build capacity on CVD in the EU; and
- Liaising formally with other key international actors on CVD in order to enhance cooperation, collaboration and the sharing of best practices.

Furthermore, Article 47 (1)j of the Cybersecurity Act states that a European cybersecurity certification scheme is expected to include *inter alia* "rules concerning how previously undetected cybersecurity vulnerabilities in ICT products and services are to be reported and dealt with." This provision of the Cybersecurity Act provides the possibility to introduce CVD in a European Cybersecurity Certification Scheme, which in fact may encourage CVD as a good practice. In addition, the scope of the Cybersecurity Certification Framework could explicitly cover the certification of processes that qualify as good practices in overall cybersecurity risk management. In this manner, companies could be encouraged to deploy Coordinated Vulnerability Disclosure policies.

EU Research Funding

8. **Framework Programmes for Research and Innovation**. The various European Framework Programmes for research and innovation offer several ways to leverage funding to promote CVD among public and private researchers in Europe. For instance, the following H2020 calls described in the Work Programme 2018-2020 could be used to finance research and innovation in this area:
   - SU-ICT-03-2018: Establishing and operating a pilot project to create a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research and Innovation Roadmap.
   - SU-DS02-2020: Management of cyber-attacks and other risks. This topic is not yet defined and will be the subject of a later amendment to the Work Programme, where explicit mention to CVD could be introduced.
   - SU-DS03-2019-2020: Digital Security and privacy for citizens and small and medium enterprises and micro enterprises. The Work Programme already states: "The proposals should develop targeted, user-friendly and cost-effective solutions enabling SMEs & MEs to: (1) dynamically monitor, forecast and assess their security, privacy and personal data protection risks55; (2) become more aware of vulnerabilities, attacks and risks that influence their business; (3)

[7] See https://www.enisa.europa.eu/publications/vulnerability-disclosure

manage and forecast their security, privacy and personal data protection risks in an easy and affordable way;…".

- SU-DS04-2018-2020: Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches. The Work Programme states: "The proposals shall implement the following series of activities to make the electric system cyber secure: (i) assessing vulnerabilities and threats of the system in a collaborative manner (involving all stakeholders in the energy components provision supply chain)…".
- SU-DS05-2018-2019: Digital security, privacy, data protection and accountability in critical sectors. The Work Programme states: "(1): In collaboration with all stakeholders in the healthcare ecosystem and CERTs/CSIRTs, develop dynamic vulnerability data basis for collecting, uploading, maintaining, and disseminating vulnerabilities of ICT-based medical systems, technologies, applications and services (enhancing the ICT generic ones e.g. NIST, MITRE)…".

The next Framework Programme for Research and Innovation, FP9, should also provide explicit funding for CVD across Europe.

Recommendations to implement government vulnerability disclosure (GVD) in Europe

In the course of their day-to-day functioning, governments often acquire insights into vulnerabilities. Thus, ensuring that governments and their agencies have strong policies for reviewing and coordinating the disclosure of vulnerabilities is a critical norm that should be advanced within the EU. It appears, however, that most member states have not implemented a government vulnerability disclosure review process.

1. **GVD Characteristics**. The Task Force recommends that all member states adopt the following policies and practices to inform the GVD activities of their government institutions and agencies:
   - All security vulnerabilities should be subject to a government vulnerability disclosure review process.
   - All relevant ministries, including those with missions for user, business and government security, should participate in the GVD review process and participants should work together using a standard set of criteria to ensure that all risks and interests are considered.
   - The policies, practices and determinations of the GVD review process should be subject to independent oversight and transparency. Regular public reporting should be viewed as a critical part of this.
   - The executive secretariat of the GVD review process should be housed within a civilian agency with expertise in existing coordinated vulnerability disclosure.
   - The GVD review process should be codified in law or other legally binding policy to ensure compliance and permanence.
   - Any non-disclosure agreement with contractors, resellers or security researchers should be prohibited, and any other exceptions should be limited (e.g. for ultra-sensitive issues).
   - Any decision to retain a vulnerability should be subject to a six-month review after its adoption

   ENISA can play a vital role in sharing best practices in GVD review processes and assisting and advising member states in their implementation.
2. **Survey of Member States' Government Vulnerability Disclosure**. It may also be useful for the European Commission or ENISA to conduct a study of member states' efforts to implement a GVD review process. A better understanding of how member states are handling vulnerabilities will contribute to a more robust and informed debate about cybersecurity in Europe and the types of measures that are needed to improve coordination and cooperation vis-á-vis cybersecurity incidents in the EU.

Annex

Definitions of key terms

Vulnerability: "Set of conditions or behaviour that allows the violation of an explicit or implicit security policy. Vulnerabilities can be caused by software defects, configuration or design decisions, unexpected interactions between systems or environmental changes. Successful exploitation of a vulnerability has technical and risk impacts. Vulnerabilities can arise in information processing systems as early as the design phase and as late as system deployment."[8]

Exploit: Software programme that uses a vulnerability to generate some effect.

Malware: Software programme used to compromise the security of a system.

Incident: "Violation or an attempted violation of a security policy and may involve malware, exploits or vulnerabilities".[9]

Patch: Piece of software designed to update a computer programme or its supporting data, to fix or improve it. This includes fixing security vulnerabilities and other bugs.[10]

Zero-day vulnerability: Also known as a computer zero day, a flaw in software, hardware or firmware that is unknown to the party or parties responsible for patching or otherwise fixing the flaw.

[8] See CERT Guide to Coordinated Vulnerability Disclosure", by Allen D. Householder, Garret Wassermann, Art Manion and Chris King, Software Engineering Institute, Carnegie Mellon University, August 2017, p. 2.

[9] Ibid., p. 2.

[10] https://en.wikipedia.org/wiki/Patch_(computing)