COMMENTARY

Thinking ahead for Europe

28 June 2018

Protecting Europe against software vulnerabilities: It's time to act!

Lorenzo Pupillo, Afonso Ferreira and Gianluca Varisco

A new CEPS Task Force report suggests concrete policy measures and recommendations addressed to all stakeholders to help jumpstart coordinated vulnerability disclosure and government disclosure decision processes across Europe.

The year 2018 kicked off with two of the worst computer security flaws ever experienced – Meltdown and Spectre – affecting nearly every computer chip manufactured over the past 20 years. And last year, people all over the world became familiar with the names of malicious ransomware, such as WannaCry and Petya, which blocks access to a computer system until the owner forks over a sizeable sum of money.

Software today is embedded nearly everywhere: in our smartphones, our cars, our offices and our homes. This fact of 21st century life means that most products are susceptible to vulnerabilities. It has been estimated that the average software programme has at least 14 separate points of vulnerability. Each of those weaknesses can permit an attacker to compromise the integrity of the programme and exploit it for personal gain. Therefore, software vulnerabilities and their timely patching have become a serious concern for everyone. What can we do to protect ourselves? Who should look for vulnerabilities and should the vendors or the users be informed about them?

CEPS is publishing a major report today on software vulnerability disclosure (SVD) in Europe, which puts forward the analysis, policy implications and main recommendations for the design and implementation of a forward-looking policy addressing this great challenge. 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.

Lorenzo Pupillo is Associate Senior Research Fellow at CEPS. Afonso Ferreira is Directeur de Recherche, Centre national de la recherche scientifique (CNRS) (France) and Gianluca Varisco is a Cybersecurity Expert with the Italian Digital Transformation Team. All three authors served as rapporteurs of a CEPS Task Force on Software Vulnerability Disclosure in Europe, chaired by Marietje Schaake, Member of the European Parliament. This Commentary distills the main conclusions and policy recommendations reached by the Task Force, whose final report can be downloaded here.

The report offers the first comprehensive analysis of the various measures that EU member states are taking to face the challenges of vulnerabilities disclosure. As of today, 13 EU member states are considering the creation of a national coordinated vulnerability disclosure (CVD) policy. Two countries have already put a CVD policy in place, but the remaining member states have no immediate plans in this area.

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. Therefore, the first step is to provide the necessary legal certainty to security researchers involved in vulnerability discovery as well as to set up appropriate vulnerability disclosure processes through complementary guidance and best practices. To this end, the members of the Task Force carried out an extensive survey of current best practices in Europe, the US and Japan, and based on their findings, have put forward several policy recommendations presented below.

Providing legal clarity for software vulnerability discovery and disclosure

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 standards, aimed at providing legal clarity for software vulnerability discovery and disclosure. The National Cyber Security Center (NCSC) in the Netherlands has published a general guideline for responsible disclosure, which can serve as a useful model for EU member states to follow in drafting their own responsible disclosure policy. The Coordinated Vulnerability Disclosure Template from the National Telecommunications and Information Administration (NTIA) of the US Department of Commerce and the first version of a framework for a Vulnerability Disclosure Program for Online Systems from the US Department of Justice can also offer helpful suggestions.

The Task Force suggests that Europe should consider implementing the operational steps outlined below for implementing coordinated vulnerability disclosure processes:

- Private sector: The private sector could take the lead in implementing coordinated vulnerability disclosure by defining and publishing on companies' websites public reporting mechanisms on vulnerabilities disclosure, based on ISO standards. The Netherlands Responsible Disclosure Guidelines, the NTIA template and the DOJ Vulnerability disclosure programmes could also be followed as best practices.
- CERTs*:* Computer emergency response teams should help put in place a framework to implement coordinated vulnerability disclosure processes by playing the role of a trusted third party and coordination centre in this process.
- Member states: Member states should act in creating the necessary legal certainty for security researchers involved in vulnerability discovery, revising national legislation to allow for the recognition of ethical hacking.
- EU: The EU should amend European legislation to allow for legal certainty for security researchers involved in vulnerability discovery and to foster agreement on common rules and procedures across member states to allow for a shared process of coordinated software vulnerability disclosure in Europe.

Constructing an effective policy framework for implementing CVD in Europe

The discussions in the Task Force led also to policy recommendations, addressed to member states and the EU institutions, for the development of an effective policy framework for introducing coordinated vulnerability disclosure (CVD) in Europe.

These recommendations include: amending national legislation and Directive 2013/40/EU on attacks against information systems (the EU cybercrime Directive) to support CVD and to create a safe environment for the community of security researchers to report vulnerabilities that they identify; promoting the protection of security researchers and creating incentives for security researchers to actively participate in CVD programmes; incorporating CVD policies in the technical and organisational measures envisaged by the EU Directive on security of network and information systems; amending the Cybersecurity Act to engage the European Union Agency for Network and Information Security (ENISA) in the development of CVD practices and policy in the EU; proposing *ad-hoc* measures to use EU research funding to promote CVD; and envisaging *ad-hoc* initiatives to manage SVD in products such as cars and medical devices.

Implementing government disclosure decision processes (GDDP) throughout Europe

In the course of their day-to-day functioning, governments often acquire intelligence about software vulnerabilities. Thus, it is essential that governments and their agencies adopt strong policies for reviewing and coordinating the disclosure of vulnerabilities as a critical norm that should be facilitated throughout the EU. At the present time, however, it appears that very few member states have taken the necessary steps to implement such a process.

To address this shortcoming, the Task Force recommends that all member states adopt policies and practices designed to share information about the GDDP activities of their government institutions and agencies. These activities should be subject to independent oversight and transparency and involve the active participation of all relevant ministries. The executive secretariat of the GDDP should be housed within a civilian agency with expertise in coordinated vulnerability disclosure and should operate under a default policy of immediate disclosure to the affected vendor(s) so that any vulnerability can be quickly patched.

Creating a safer cyber space in Europe

The overall work of the Task Force aims to benefit Europeans by creating a safer cyberspace in which people can connect with one another without fear that software vulnerabilities will cause them harm. This goal is particularly important since the risk of cyberattacks linked to the exploitation of vulnerabilities will inevitably increase with the digital transformation. It is time to act! The CEPS Task Force report suggests concrete policy measures and recommendations addressed to all stakeholders to help jumpstart coordinated vulnerability disclosure and government disclosure decision processes across Europe.