Mozilla EU
Rue du Trône 51
Ixelles
Brussels 1050
Belgium

Mozilla position paper on the legislative proposal for an EU Cybersecurity Act

Enhancing cybersecurity through government vulnerability disclosure

I. INTRODUCTION

This paper provides an overview of Mozilla's perspectives and recommendations for EU policymakers with respect to the EU Cybersecurity Act legislative proposal.

Mozilla is a global community of technologists, thinkers, and builders working together to keep the internet open, accessible, and secure. We are the creators of Firefox, an open source browser that hundreds of millions of people around the world use as their window to the web, as well as other products including Pocket, Rocket, and Focus. To fulfill the mission of keeping the web open and accessible to all, we are constantly investing in the security of our products, the internet, and its underlying infrastructure.

In that context, Mozilla commends the European Commission's ambition with this legislative proposal, and looks forwards to supporting the EU Institutions in realising a legislative outcome that ensures the EU's cybersecurity regulatory framework is tailored for the evolving threat landscape.

II. POLICY RECOMMENDATION: ENISA'S ROLE IN GOVERNMENT VULNERABILITY DISCLOSURE

Our recommendations focus exclusively on the elements of the proposal that concern the enhanced mandate for ENISA, namely articles three to eleven. Specifically, we recommend the EU co-legislators to include within ENISA's reformed responsibilities a mandate to assist Member States in establishing and implementing **policies and practices for the responsible management and coordinated disclosure of vulnerabilities** in ICT products and services that are not publicly known.

In computing, the term ''vulnerability'' means a design, configuration, or implementation weakness in a technology, product, system, service, or application that can be exploited or triggered to cause unexpected or unintended behavior. Colloquially referred to as 'security bugs', vulnerabilities have been at the heart of many recent high-profile cybersecurity incidents, including WannaCry[1], Meltdown, and Spectre[2].

While not being excessively prescriptive, the proposed EU Cybersecurity Act offers a unique opportunity to advance the norm that Member States should have robust, accountable, and transparent government vulnerability disclosure review processes, thereby fostering greater cybersecurity in Europe. Indeed, through its capacity to assist and advise on the development of policy and practices, a reformed ENISA is well-placed to support the EU Member States in developing government vulnerability disclosure review mechanisms and sharing best practices.

In the proceeding sections, we will elaborate on why the EU Member States ought to introduce government vulnerability disclosure review processes, and why the proposed EU Cybersecurity Act offers a useful starting point to advance that end.

III. WHY VULNERABILITY DISCLOSURE IS CRUCIAL TO MOZILLA

Firstly, as the producer of one of the world's most popular web browsers, it is essential for Mozilla that vulnerabilities in our software are quickly identified and patched. Simply put, the safety and security of our users depend on it. More generally, the coordinated disclosure of vulnerabilities allows vendors and manufacturers to:

- patch vulnerabilities quickly;
- increase the security, privacy, and safety of their systems and users;
- reduce conflict and improve trust with government; and,
- benefit from external discovery of vulnerabilities in their products and systems that they may not otherwise have the resources to find, which is especially important for small and medium-sized enterprises.

As witnessed in, for instance, the recent Petya[3], and Heartbleed[4] cyberattacks, vulnerabilities can be exploited by cybercriminals to cause serious damage to

[1] Symantec, 'What you need to know about the WannaCry ransomwhere', Available at: https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack, accessed on 29.03.2018

[2] For an overview of the Meltdown and Spectre vulnerabilities and the process that led to their discovery, see https://meltdownattack.com/. Accessed on 29.03.2018

[3] McAfee, 'Petya is here, and it's taking clues from WannaCry', Available at: https://securingtomorrow.mcafee.com/consumer/consumer-threat-notices/petya-ransomware/, accessed on: 12.03.2018

citizens, enterprises, public services, and governments. Vulnerabilities are especially destructive when they are exploited by malicious actors in the form of 'zero-day' attacks, for which the vendor was not aware of the vulnerability and hence unable to provide a security patch for vulnerable machines at the time of attack.

In spite of their risks, it should be recognised that vulnerabilities are inevitable in the course of software development. The complexity and interdependency of contemporary programming applications means it is practically impossible to build software that is completely 'bugless'. For that reason, **software vendors depend on security researchers, governments, and citizens to disclose potential vulnerabilities** such that they can be quickly patched to enhance the privacy, security, and safety of all users.

IV. GOVERNMENTS AND VULNERABILITIES

Governments learn about vulnerabilities in many ways: through their own research and development, by purchasing them, through intelligence work, or by reports from third parties. While such vulnerabilities can cause serious harm to citizens, enterprises, and even public authorities themselves, **certain government agencies – particularly within the intelligence communities – have an interest in withholding knowledge of software vulnerabilities for 'offensive' purposes.** For instance, knowledge of a software vulnerability in a smartphone application can serve as a useful investigatory tool for the intelligence community when seeking e-evidence with respect to serious crimes.

In that context, owing to their resources and interests, governments are uniquely placed to gather information on software vulnerabilities, yet face competing incentives and interests as to whether to immediately disclose the software vulnerabilities they learn about or delay disclosure. To address this situation, governments should establish robust, transparent, and accountable policies and practices to consider all risks and interests when making these decisions.

Frameworks for such are generically known as **government vulnerability disclosure (GVD) review processes.** In both the US and the EU, Mozilla has long led calls for governments to codify and improve their policies and processes for handling vulnerability disclosure, including speaking out strongly in favor of the Protecting Our

[4] Kaspersky, '"Heartbleed" vulnerability may compromise your security on thousands of sites', Available at: https://www.kaspersky.com/blog/heartbleed-howto/4431/, accessed on 12.03.2018

Ability to Counter Hacking Act (PATCH Act) in the United States. Mozilla is also a member of the Centre for European Policy Studies' Task Force on Software Vulnerability Disclosure, a multistakeholder effort dedicated to advancing thinking on this important topic, including mapping current practices and developing a model for government vulnerability disclosure review[5].

V. MODEL PRINCIPLES FOR GVD REVIEW PROCESSES

While only a handful of countries around the world currently have GVD review processes, we nonetheless believe that there are certain key principles which can allow GVD frameworks to contribute to realising balanced outcomes with respect to competing cybersecurity and investigatory policy concerns. Specifically, we believe that Member States should incorporate the following principles into their frameworks:

1. All security vulnerabilities are subject to a government vulnerability disclosure review process.[6]
2. All relevant ministries, including those with missions for user, business, and government security, should participate in the government vulnerability disclosure review process and participants should work together using a standard set of criteria to ensure all risks and interests are considered.
3. The government vulnerability disclosure review process' policies, practices, and determinations should be subject to regular review and independent oversight and transparency.
4. The government vulnerability disclosure review process' executive secretariat should be housed within a civilian ministry with expertise in coordinated vulnerability disclosure[7].

[5] On 27 February 2018, MEP Marietje Schaake, Chair of the CEPS Task Force on Software Vulnerability Disclosure, hosted a workshop in the European Parliament where the Task Force's work and preliminary findings were discussed. A recording of the workshop is available at: https://alde.livecasts.eu/software-vulnerability-disclosure-in-europe; accessed on 11.04.2018

[6] This should not be construed to include vulnerabilities that are shared with a country's CERT, CSIRT, or other competent body charged with coordinated vulnerability disclosure [and security incident response management].

[7] Coordinated vulnerability disclosure 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". See 'CERT Guide to Coordinated Vulnerability Disclosure', Available at:

5. The government vulnerability disclosure review process should be codified in law or other legally binding policy to ensure compliance and permanence.

Ultimately, by developing and engaging with meaningful GVD review processes that enshrine the principles above, governments can significantly improve the safety, security, and privacy of citizens and enterprises. Moreover, GVD review processes enhance the trust and confidence between software providers and governments, a crucial benefit given the multistakeholder nature of cybersecurity. Finally, small and medium-sized software vendors are most at risk from vulnerability exploitation by cybercriminals. GVD processes thus ensure that these providers – who typically do not have sufficient resources to engage in intensive vulnerability detection efforts – can benefit from external discovery. In effect, **robust GVD frameworks in EU Member States would enhance the cyber-resilience of the Union as a whole.**

VI. HOW THE EU CYBERSECURITY ACT CAN LEAD THE WAY

In spite of the importance of having effective systems in place to review and coordinate the disclosure of the software vulnerabilities that they learn about, it appears that most EU Member States currently lack a mechanism for GVD review processes.

In recognition of the key role that vulnerabilities play in cybersecurity, the recently-adopted Network and Information Security Directive aimed to facilitate information sharing from companies to governments[8]. Yet, to ensure effective cyber resilience in the face of a broadening cyber attack surface, information sharing must be a two-way street. Indeed, it is essential that there are mechanisms in place to ensure that governments are sharing information about vulnerabilities *back out* to affected companies.

In that context, the proposed European Cybersecurity Act offers a unique opportunity to advance the norm that Member States should have robust, accountable, and transparent government vulnerability disclosure review processes,

https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf, accessed on 20.03.2018

[8] Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. See especially articles 14 and 16 of the directive concerning incident notification to competent authorities by affected private actors.

thereby fostering greater cooperation, coordination, and resilience in Europe. We believe the European Commission and a newly-strengthened ENISA can be powerful players in helping Member States to develop government vulnerability disclosure review mechanisms and share best practices. **We thus recommend the EU co-legislators to introduce a mandate for ENISA to assist and advise Member States on developing GVD review processes.**

VII. CONCLUSION

The cyber threat landscape is constantly evolving, and now more than ever governments and companies need be working better together if we are to keep Europeans citizens and infrastructure as secure as possible.

Mozilla looks forward to working with the EU Institutions on the EU Cybersecurity Act to realise a legislative outcome that positions the EU as a global norm setter with respect to government vulnerability disclosure review processes.

***

For questions or further information please contact:

Jochai Ben-Avie, Senior Global Policy Manager, Mozilla (jochai@mozilla.com)
Owen Bennett, EU Internet Policy Manager, Mozilla (obennett@mozilla.com)