Joint industry letter on Cybersecurity Vulnerabilities Administrative Regulation

Response to MIIT published draft for comments

Brussels, 18 July 2019

The undersigned associations welcome the opportunity to submit their comments on the Coordinated Vulnerability Disclosure Regulation put forward by the Chinese Ministry of Industry and Information Technology (MIIT).

We encourage MIIT to align the proposed Regulation with well-established and broadly adopted best practices and industry standards. These practices and standards have been carefully developed globally in the field of Coordinated Vulnerability Disclosure ('CVD') and vulnerability handling.

We support alignment with these practices, as articulated in ISO international standards such as ISO/IEC 29147 (2018) and ongoing work expected to become a standard,[1] given the globally intertwined nature of technology and vulnerability management processes.

Below we highlight subject areas and sections where we suggest the current proposed Regulation could be aligned with already widely accepted and followed practices.

- **Article 3**: The proposed Article includes a requirement for mitigation to be developed within 90 days and to patch services within 10 days. Mandating specific timelines diverges from international standards and undermines companies' ability to deliver effective and stable mitigations, thus potentially putting end-users at risk and compromising the affected infrastructure.

[1] See also the ENISA Report *Good Practice Guide on Vulnerability Disclosure: From Challenges to Recommendations* (2016), p. 9: 'The global nature of the internet requires a more transnational approach to the topic of vulnerability disclosure, where successful cases in certain countries or regions can be used for policy learning purposes in other areas of the world.'

The CVD process is a standardised, multi-step process through which stakeholders identify, develop, validate, distribute and deploy mitigations for security vulnerabilities. In complex systems like hardware, CVD often requires multi-party coordination ('multi-party CVD') with the relevant ICT manufacturers (OEMs) or ecosystem partners (cloud providers and OS developers and supporters) to validate the vulnerability, develop the mitigations, test the mitigations in various environments and finally effectively deliver it to end-users.[2]

Thus, the time needed to develop the mitigation for supported products or services differs according the technology at hand.[3] Widely adopted international standards that take onboard the complexity of the CVD process, which includes multi-party environments, do not recommend any timeframes. Rather, they instruct vendors to balance the need to develop remediation as soon as possible 'with the overall testing required to ensure the remediation does not negatively impact affected users due to quality issues,' meaning the completeness and effectiveness of the proposed mitigation.

In some cases, remediation may not be possible in the short term because of negative effects on interoperability or a need to develop new approaches or cryptographic standards; other factors may include the number of parties involved, the complexity of technologies, the degree of risk and the impact of the vulnerability.

In addition, Article 3 does not consider that product suppliers often build products by embedding third-party products in order to provide common or special functions. Products available to end-users often contain multiple layers of embedded products. Those third-party products may themselves embed further products from other product suppliers (fourth-party products).

For these reasons, it is critical that no fixed timeline is set for addressing vulnerabilities as it will impede a vendor's ability to apply risk management and prioritise fixes that would impact customers. Instead of addressing the most important issues first, vendors would be forced to address the fixes in chronological order, thus putting end-users at even greater risk.[4]

---

[2] See Center for Cybersecurity Policy and Law, *Improving Hardware Component Vulnerability Disclosure* (2019), available at https://centerforcybersecuritypolicy.org/improving-hardware-component-vulnerability-disclosure. See also FIRST, *Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure*, available at https://first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.0.

[3] Hardware manufacturers often do not have a means to unilaterally deliver mitigations without direct participation of such entities in the global supply chain.

[4] See ISO/IEC 30111 (2013), Section 7.2.4 (Remediation Development): 'When determining the best remediation, the vendor should attempt to balance the need to create a remediation quickly, with the overall testing required to ensure the remediation does not negatively impact affected users due to quality issues.' See also Section 7.3 with respect to vulnerability handling phases monitoring.

***Suggested approach**: Requiring that mitigations be developed as quickly as possible and in reasonable timeframes, taking into consideration the completeness and effectiveness of the proposed mitigation, as well as the severity of the vulnerability, but with no specific timeframes outlined.*

- **Article 4:** The proposed Article describes in general terms that MIIT, MPS and relevant industry-specific administrative departments can urge network product suppliers, service providers and network operators to take patching or preventative measures in accordance with their respective responsibilities.

***Suggested approach**: We recommend greater clarification and details with regard to the different roles of MIIT, MPS and departments responsible for relevant industries respectively.*

- **Article 6:** According to international standards and broadly adopted industry best practices on coordinated vulnerability disclosure, security researchers should not disclose vulnerability information prior to the issuance of a patch or update addressing the vulnerability. If a product or service is no longer supported, the same process should be followed, starting with the notification of the technology developer.

  For limited cases where vendors fail to issue patches or updates within a reasonable time period following the identification or notification of the vulnerability, it can be useful for security researchers to have the option of disclosing vulnerability information as a way to accelerate a vendor's response or to enable users to otherwise take mitigation measures.

***Suggested approach**: Aligning Article 6 with international standards – such as ISO/IEC 30111:2013 (and its revisions currently in process) and ISO/IEC 29147:2018 – and not sanctioning disclosure in limited cases where it may be warranted and reasonable under international standards and industry best practices.*

- **Article 8:** The decision as to whether to adopt and deploy a proposed mitigation (delivered by the network operator to the end-user) ultimately resides with the end-user (including network operators) and may differ on a case-by-case basis, given the technology and risk-assessment, since additional costs may be associated with deploying the patch. Thus, absent failure to take reasonable measures, such decision should not be generally sanctioned.

***Suggested approach**: International standards and industry best practices generally require taking reasonable measures to validate a vulnerability, develop a remediation or adopt a remediation. We recommend such standards of reasonableness should be reflected in Article 8.*

- **Article 10**: One key objective of CVD and vulnerability handling processes is to minimise users' risk, potential harm and cost associated with the vulnerability. To achieve this, CVD directs the recipient of a vulnerability to only disclose information about the vulnerability to other parties that are absolutely required in order to develop and deploy mitigation or remedial measures. Disclosure to unnecessary third parties increases the likelihood of information leaks that could enable malicious actors and harm users.[5]

  Requiring disclosure by finders to specific entities assumes that all the listed parties are necessary. Generally, under international standards and industry-wide adopted CVD best practices, the external finders or entities that are made aware of the vulnerability should report the relevant information to the potentially impacted vendor or manufacturer, who is best positioned to lead the coordination efforts, validate the vulnerability and finally develop remediation and remediation delivery processes.[6]

  An organisation or finder should not be required to report vulnerability information to a third-party organisation, due to potential risks to security while mitigations are not available. The proposed Article 10 diverges from these standards alongside introducing vagueness in this respect, noting that finders and organisations should report the issues to third-party organisations such as vulnerability collection platforms, as opposed to the impacted vendors.

***Suggested approach**: Clarifying that, following CVD best practice, only the parties that are essential to the mitigation development and deployment should be informed as the vendor leads the coordination efforts. The finder or organisation made aware of the vulnerability should report the issue immediately to the potentially impacted network product suppliers, service providers and network, but otherwise keep the information in confidence until mitigations are available. After mitigations are available and information concerning the vulnerability is reported to end-users, the vendor should then be encouraged to notify the vulnerability collection platforms.*

- Under international standards, mitigations are generally developed and delivered for supported products or services (and certain products eventually reach end-of-life).[7]

***Suggested approach**: The Regulation should make it clear that vulnerability handling and management processes are generally only applicable to supported products and technologies.*

[5] See ISO/IEC 30111 (2013) at Section 7.4: 'Premature disclosure of sensitive vulnerability information can increase the costs and risks associated with disclosure for vendors and users.' ISO/IEC 29147 (2018) at Section 5.8 and p. vii. See also the ENISA Report on Good Practice Guide on Vulnerability Disclosure, at p. 10: 'From the perspective of the security and trust of the end-users of systems, there is consensus that vulnerabilities must be disclosed in a way that minimises damage.'

[6] See Section 5.6.3 ISO 29147 (2018): 'A reporter identifies potential vulnerabilities in products or services and notifies the vendor.' As mentioned, in hardware settings, manufacturers often do not have a means to unilaterally deliver mitigations without direct participation of entities such as OEMs and operating system providers.

We appreciate the MIIT's attention to this very important issue. We recommend alignment with widely adopted international standards (such as ISO/IEC 30111 (2013) and its revisions currently in process, and ISO/IEC 29147 (2018)) and further consultations with industry experts.

- DIGITALEUROPE – digitaleurope.org
- 日本电子信息技术产业协会（JEITA）– jeita.or.jp
- AmCham EU – amcham.eu
- BSA | The Software Alliance – bsa.org
- ITI – itic.org