Comments on "Cybersecurity Vulnerabilities Administrative Regulation"

July 17, 2019

The Cyber Threat Alliance (CTA) and the Cybersecurity Coalition submit these comments in response to the Ministry of Industry and Information Technology's (MIIT) draft "Cybersecurity Vulnerabilities Administrative Regulation."[1] Thank you for the opportunity to provide input on the draft regulation and support efforts to strengthen cybersecurity and protect users.

The CTA is a not-for-profit organization that is working to improve the cybersecurity of our global digital ecosystem by enabling near real-time, high-quality cyber threat information sharing among companies and organizations in the cybersecurity field. The mission of the Cybersecurity Coalition is to bring together leading companies to help policymakers develop consensus-driven policy solutions that promote a vibrant and robust cybersecurity ecosystem; support the development and adoption of cybersecurity innovations; and encourage organizations of all sizes to take steps to improve their cybersecurity.

The CTA and the Cybersecurity Coalition urge MIIT to align its cybersecurity vulnerability disclosure and management regulations with internationally recognized standards for coordinated vulnerability disclosure - specifically ISO 30111 and ISO 29147.[2] These standards are widely used and provide effective guidance for vendors, vulnerability finders, and vulnerability coordination bodies globally. At present, the draft regulation deviates sharply from these standards in several respects - such as the restrictions on publicly disclosing vulnerability information before vendors publish preventative measures, and the requirement that vendors publish preventative measures in 95 days or less. This creates a conflict between MIIT's draft regulation and how coordinated vulnerability disclosure is routinely practiced in other

[1] Ministry of Industry and Information Technology of the People's Republic of China, Cybersecurity Vulnerabilities Administrative Regulation, Jun. 18, 2019, https://mp.weixin.qq.com/s/TnYAoxtBV_Oq-dvE-l1ZpQ. See also translation by Dahlia Peterson and Rui Zhong, New America, Jun. 19, 2019, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-rules-managing-cybersecurity-vulnerabilities-published-draft-form.

[2] ISO/IEC 30111:2013, Information Technology – Security Techniques – Vulnerability Handling, International Standards Organization, Nov. 1, 2013, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53231. ISO/IEC 29147:2018, Information Technology – Security Techniques – Vulnerability Disclosure, International Standards Organization, Oct. 2018, https://www.iso.org/standard/72311.html.

jurisdictions that more closely align with international standards. MIIT should provide guidance clarifying how the draft regulation will be enforced if the vendor, vulnerability finder, or publication of vulnerability information is located outside the border of China.

- Recommendation #1: We urge MIIT to modify the draft regulation so that it is harmonized with ISO 30111 and 29147. This would include additional flexibility on disclosing vulnerability information, disclosing tools and methods, and avoiding strict deadlines for vendors to patch vulnerabilities.

Article 6(I) of the draft regulation restricts third parties and individuals from publicly disclosing vulnerability information until after the vendor publishes preventative measures to the public. However, there will be situations where disclosure might be appropriate under international standards and industry best practices when the vendor does not undertake preventative measures and user notification, and when disclosure may enable users to consider alternative mitigation measures. The draft Article 6 would prevent vulnerability finders from disclosing vulnerabilities in the cases where mitigations may never be developed. For example, if the product is no longer supported,[3] the vendor has gone out of business, or if the vendor and the finder disagree on whether a vulnerability exists or is serious enough to justify mitigation. The vulnerability may be exploited against users while the vendor fails to take any action to develop mitigation.[4]

- Recommendation #2: Modify Article 6(I) - Third parties may publish vulnerability information without the vendor patching or taking a preventative measure if 1) the third party first attempts to contact the vendor, and 2) the vendor will not develop a preventative measure in a reasonable time.

Article 6(III) states third parties cannot "publish or provide methods, procedures, or tools specifically designed to exploit network product, service, or system vulnerabilities which would harm cybersecurity." This appears to apply even if the vendor mitigates the vulnerability, so long as publishing the exploit would "harm cybersecurity." However, this restriction may prevent providing methods, procedures, and tools for beneficial purposes. For example, penetration testing services use exploits to help clients strengthen cybersecurity by simulating attacks and identifying vulnerabilities. In addition, published vulnerability research or classroom instruction may include a proof-of-concept to explain the vulnerability.

- Recommendation #3: Modify Article 6(III) - Third parties may publish or provide methods, procedures, or tools for the purpose of improving cybersecurity after a patch or preventative measures have been developed and made publicly available to end-users.

[3] In this case, it should be considered if disclosure of information may increase risk of exploitation in other dependent supported products.
[4] Cybersecurity Coalition, Policy Priorities for Coordinated Vulnerability Disclosure and Handling, Feb. 25, 2019, pg. 8, https://www.cybersecuritycoalition.org/policy-priorities.

Article 3(I) requires vendors to patch or take preventative measures within 90 days for network products and 10 days for network services. However, not every vulnerability can be patched within a 90- or 10-day deadline. For example, a patch may need to undergo quality testing in different environments to ensure the patch does not cause new problems.[5] Article 3 seems to assume only one vendor will be involved, but the vulnerability may involve multiple vendors and other affected parties. These deadlines also do not recognize the added complexities of mitigating vulnerabilities that implicate hardware and firmware, which involve supply chains with interdependencies that must often be coordinated with outside suppliers to validate, develop and test the mitigation.[6] Hard deadlines for patching and public notification can interfere with focusing resources for more severe vulnerabilities. At the same time, it is critical for vendors to review vulnerability information and begin developing patches as quickly as possible taking into consideration the completeness and effectiveness of the proposed mitigation, and the severity of the vulnerability. Flexibility in the patching deadline should not permit the vendor to unreasonably delay mitigating the vulnerability.

- Recommendation #4: Modify Article 3(I) - Vendors must verify the vulnerabilities as quickly as possible, and take patching or preventive measures for relevant network products and services as quickly as possible, while taking into account the severity of the vulnerability and the completeness and effectiveness of the proposed mitigation.

Article 8 describes administrative punishment for vendors that fail to patch or take preventative measures within the timelines imposed in Article 3. However, vulnerability finders face more severe penalties for violating Article 6 by disclosing vulnerability information before the vendor has published preventative measures. This risks an incentive for vendors to mitigate a vulnerability but not publish the preventative measures, effectively preventing the researcher from publicly disclosing the vulnerability. It should be clear from the regulation that intentional violations of Article 3 for failing to take reasonable measures may warrant an enhanced administrative punishment.

Recommendation #5: Modify Article 8 - Administrative punishment may be enhanced where a vendor intentionally fails to take reasonable actions by withholding or delaying a patch, preventative measure, or user notification for a known vulnerability in a supported product, in accordance with the regulation, without justifiable cause.

* * *

[5] See Improving Hardware Component Vulnerability Disclosure, Center for Cybersecurity Policy and Law, Apr. 2019, pgs. 4-5, https://centerforcybersecuritypolicy.org/improving-hardware-component-vulnerability-disclosure.
[6] *Id*.

Thank you for considering our recommendations. The Cyber Threat Alliance and the Cybersecurity Coalition look forward to working with you to strengthen and harmonize global vulnerability disclosure and management practices.