HACKING POLICY COUNCIL

Position Statement: Requiring Vulnerability Disclosure to Governments

Hacking Policy Council – June 2023

The Hacking Policy Council releases this statement to highlight our public position that laws requiring premature disclosure of software vulnerabilities to governments risk undermining cybersecurity.[1] The Hacking Policy Council supports efforts by governments to encourage adoption of vulnerability disclosure policies, and to encourage software publishers to patch or address vulnerabilities. However, mandatory reporting of unmitigated vulnerabilities to government agencies raises security risks to nations and the technology ecosystem as a whole. Proposals, such as the EU Cyber Resilience Act, to require disclosure of all newly exploited software vulnerabilities to governments must include safeguards to prevent misuse of the information.

Vulnerability disclosure and handling should, to the extent possible, follow recognized international standards.[2] When an organization discovers a significant software vulnerability, a top priority is addressing the vulnerability to protect users and prevent loss or damage. A software vendor should patch or mitigate vulnerabilities in its products, but the vendor will need time to develop a fix. If the vulnerability is in another organization's software, such as when an enterprise discovers they are using a vulnerable product, that vulnerability should be communicated to the vendor so that it has the opportunity to mitigate it.

During the vulnerability disclosure and handling process, organizations should generally not disclose an unmitigated vulnerability to third parties or the public, unless necessary to respond to a substantial cyber incident or to alert users so that they can take steps to avoid attacks. This may include circumstances where users are being actively harmed and should take defensive measures, the organization needs assistance mitigating the vulnerability or responding to a vulnerability disclosure, or the organization is unwilling or unable to mitigate the vulnerability. However, laws that require disclosure of unmitigated vulnerabilities to government agencies as a default create risks that outweigh the benefits of disclosure.

Risk of alerting adversaries. Requiring companies to share information about unmitigated vulnerabilities with government agencies undermines cybersecurity by increasing the risk that the information will be exposed to adversaries before a mitigation is in place. The more agencies, officials, and contractors that possess the vulnerability information, the greater the risk. Even if the disclosure is

[1] The Hacking Policy Council is a group of organizations working to make technology safer and more transparent by promoting adoption and best practices for coordinated vulnerability disclosure, good faith security research, bug bounty programs, penetration testing, and vulnerability management.
[2] See e.g., ISO/IEC 29147 and 30111.

a notification of an unmitigated vulnerability, rather than a detailed technical assessment, "Releasing partial information can help adversaries. [M]ere knowledge of a vulnerability's existence [is] sufficient for a skillful person to discover it for themselves."[3] To prevent this, regulations need to ensure that companies have the opportunity to take appropriate steps to fix known vulnerabilities, while not risking disclosure of sensitive data related to zero-days.

Risk of intelligence use. Requiring the disclosure of unmitigated vulnerabilities to government agencies raises the risk that those vulnerabilities may be used for state intelligence or offensive purposes. Chinese laws requiring businesses to immediately report vulnerabilities to the central government have been associated with the increased use of zero-day vulnerabilities from China-based actors.[4] To prevent this, laws that require disclosure of vulnerabilities for market safety or incident response should include a clear restriction on the use of those vulnerabilities for intelligence or offensive purposes.[5]

Risk of international precedent. Laws that require disclosure of unmitigated vulnerabilities to government agencies create a precedent that may be reflected by other countries. As global governments update their cybersecurity authorities, deviation from international standards and best practices for vulnerability disclosure should be avoided. If governments in major economies require premature vulnerability disclosure, this model may spread internationally and upend current best practices.

Risk of deterring good faith security research. Security researchers benefit society by identifying vulnerabilities so that they can be fixed. However, independent security research may be chilled if vulnerabilities discovered through that research must be disclosed to governments. Organizations may be less hospitable to vulnerability disclosures from good faith security researchers if each disclosure must trigger notifications to government agencies. To avoid this, laws should distinguish between vulnerabilities exploited by malicious actors and good faith security researchers.

Safeguards needed. Regulatory proposals such as the EU Cyber Resilience Act[6] and other policies that require disclosure of vulnerabilities to governments must include safeguards to reduce the risk of misuse of vulnerability information:

1) **Provide time to mitigate.** In the absence of a substantial cyber incident or user harm, laws should ensure organizations have a reasonable time to remediate or address the vulnerability before requiring disclosure to governments.

2) **Secure vulnerability information.** Agencies that process or maintain vulnerability information should ensure the information is subject to robust security safeguards. Information about

[3] CERT, Guide to Coordinated Vulnerability Disclosure, 5.7 Disclosure Timing, Sep. 16, 2019, https://vuls.cert.org/confluence/display/CVD/5.7+Disclosure+Timing#id-5.7DisclosureTiming-ReleasingPartialInf.
[4] Microsoft, Digital Defense Report 2022, pg. 39, https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022.
[5] ENISA, Developing National Vulnerability Programmes, Feb. 2023, pg. 16, https://www.enisa.europa.eu/publications/developing-national-vulnerabilities-programmes.
[6] Cyber Resilience Act (CRA), Articles 11.1, 13.6, 14.4, https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

unmitigated vulnerabilities should be shared only on a need-to-know basis.

3) **Prohibit offensive uses**. Laws that require disclosure of vulnerabilities to government agencies for market access, consumer safety, incident response or other defensive purposes should include a clear restriction on the government's use of disclosed vulnerabilities for intelligence, surveillance, or offensive purposes.

4) **Protect independent good faith security researchers.** Laws requiring disclosure to governments should distinguish between vulnerabilities discovered in good faith and those that are exploited by malicious actors.

* * *

For more information, please visit https://HackingPolicyCouncil.org.