Cybersecurity Coalition

Position on Vulnerability Disclosure Programs

Regarding issue area #3 – *Guidelines outlining security measures that shall be applied to the federal government's use of critical software,* the Cybersecurity Coalition believes that, in addition to least privilege, network segmentation, and proper configuration, there should be significant attention paid to the role of Vulnerability Disclosure Programs (VDPs) in determining which security measures apply to the federal government's guidelines for use of critical software. On September 2, 2020, the Office of Management and Budget issued M-20-32, *Improving Vulnerability Identification, Management, and Remediation*. This memo provided agencies with the guidance for obtaining and managing vulnerability disclosure programs. At the same time, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) released Binding Operational Directive (BOD) 20-01 requiring each agency to develop and publish a vulnerability disclosure policy and maintain procedures for handling vulnerabilities.

While the Cybersecurity Coalition applauds these steps, there is still much work to be done by agencies to implement these policy changes and to work with its industry partners on building out and implementing similar measures. Given that need, it is imperative that any additional guidance issued by the federal government around protecting critical software and the systems on which that software runs ties into both agency and critical software supplier vulnerability disclosure programs and policies.

The proliferation of interdependent technologies across the ICT supply chain is creating a landscape where coordinated vulnerability disclosure and handling (CVD) is more important than ever. CVD and agency programs that drive the disclosure efforts are increasingly recognized as a key cybersecurity activity, and existing standards and guidance have served the global community well in building a general consensus around best practices, leveraging international standards (e.g. ISO/IEC 30111 and 29147) and industry best practices. CVD and the programs that drive its processes provide an opportunity for federal government agencies and critical software suppliers to work with finders and reporters of vulnerabilities to analyze, mitigate, and communicate publicly about security flaws. This leads to a more positive resolution than if the vulnerabilities went unaddressed or if federal agencies, critical software suppliers, and vulnerability reporters did not collaborate.

In summation, the developer of the critical piece of software, whether the federal agency itself or external developer, needs to have a VDP. As critical software is identified and protections are recommended, NIST should double down on guidance to federal agencies about the need for such disclosure programs as part of its suite of protections for critical software. Additionally, in the case of external developers, NIST should consider guidance to agencies that require agencies to contract with critical software suppliers who can attest to VDPs and underlying CVD practices.

The Cybersecurity Coalition would like a representative to speak on June 2 or June 3 about building out VDPs and some of the best practices around coordinated vulnerability disclosure. Proposed speakers include but are not limited to, Harley Geiger from Rapid 7 or Ari Schwartz from Venable representing the Cybersecurity Coalition.

Contact Info: Please reach out to Ross Nodurft (RBNodurft@venable.com) and Bri Law (BLaw@venable.com) for follow up on panels.