UPDATED May 12, 2020

ISSUE BRIEFING: Coordinated Vulnerability Disclosure

The Issue: A vulnerability is a weakness in a system that can be exploited. Vulnerabilities can be found by actors with a variety of intentions. Encouraging good faith security researchers to find and report vulnerabilities through a coordinated vulnerability disclosure (CVD) program can help reduce the risks associated with vulnerabilities. CVD programs can increase the opportunity for system owners and operators to become aware of vulnerabilities and address them before bad faith adversaries become aware of vulnerabilities in order to exploit them. CVD programs must be prescribed by a vulnerability disclosure policy.

What does a vulnerability disclosure policy for a system owner and operator entail?
Vulnerability disclosure policies usually include the following components:

- A statement that encourages good faith security research and expresses that you will not pursue legal action against security researchers acting in good faith, in accordance with the policy;
- A statement that defines the scope of the policy, meaning to which system(s) it applies;
- Guidelines for good-faith security research which include clear parameters of what the policy permits and does not permit researchers to do;
- Clear instructions for how to report vulnerabilities; and
- An explanation of what security researchers who report vulnerabilities in accordance with the policy can expect from you, including:
    - A timeframe during which you will acknowledge receipt of the report;
    - A statement that you will assess the vulnerability;
    - An explanation of how and when you may contact the researcher for more information;
    - The process for notifying the researcher of a resolution, when appropriate; and
    - The process for further disclosure up to public recognition, when appropriate.

Have CVD programs been implemented by governmental organizations in the US?
Yes. Though currently still limited, states and the federal government have begun implementing CVD programs. Here are a few examples of vulnerability disclosure policies from government organizations:

- U.S. Department of Defense
- General Services Administration's 18F and Technology Transformation Services
- State of Delaware

All federal agencies will soon be required to implement a vulnerability disclosure program per the following draft policies: the Cybersecurity and Infrastructure Security Agency (CISA)'s Binding Operational Directive (BOD) 20-01, Develop and Publish a Vulnerability Disclosure Policy, and the Office of Management and Budget (OMB)'s Memorandum for the Heads of Executive Departments and Agencies: Improving Vulnerability Identification, Management, and Remediation[1].

[1] The CISA BOD and OMB memorandum are currently in draft form. This document will be updated to link to the final versions.

Where do we start?
A CVD program for your public-facing website(s) is often a good place to start. Start by creating your vulnerability disclosure policy. Ensure you have the necessary processes in place to implement the program before publishing the policy – your program's success is dependent on your organization's ability to meet the expectations set in your policy, such as reviewing and responding to reports within the designated timeframe. Below are some resources to help you get started:

- Carnegie Mellon's Software Engineering Institute, Computer Emergency Response Team's CVD Guide
- ISO/IEC 29147 – Standard for Vulnerability Disclosure (available for purchase)
- ISO 30111 – Standard for Vulnerability Handling (available for purchase)
- National Telecommunications and Information Administration's CVD template
- U.S. Department of Justice's CVD Framework for Online Systems

You may also want to explore companies that run CVD programs on behalf of other organizations and/or attend security research conferences to make connections with independent security researchers.

For additional questions on this issue, please contact NASS: (202) 624-3524 or lforson@sso.org.