Vulnerability Disclosure handling

Kendall Bean
Vulnerability Disclosure Team Lead
Idaho National Laboratory

Insights into the CVD Process

Presenter: Kendall Bean

Date: May 12th, 2026

Introduction

- Team lead for Idaho National Laboratory's (INL) Coordinated Vulnerability Disclosure (CVD) team
- INL supports CISA in vulnerability disclosure and role as a CNA Root
- Very involved in CVD policy and process development

- Three primary forms of collecting vulnerabilities:
  - Direct reports from the researcher or vendor
  - Open-source scraping
  - CISA vulnerability analysis
- Ensure novelty:
  - Check for existing CVEs
  - Check old cases/publications
- Catalog findings and open a case

- The analyst connects the vendor and the researcher and helps facilitate correspondence between involved parties
  - VINCE, CISA's dedicated vulnerability coordination platform, is the preferred portal for analysts to use to communicate with researchers and vendors
- Analysts ask vendors to validate the researchers' claims about previously unknown “zero-day” vulnerabilities
  - If necessary, technical impact is assessed by the Verification & Validation Laboratory (V&V Lab)

- The vendor is encouraged to develop a patch for the vulnerability
  - INL mediates timeline requirements between vendor development cycles and researcher disclosure policies
- If no patch can be developed, mitigations are developed to be released with the disclosure
  - Vendor recommendations are sought, when possible, but researcher and V&V Lab recommendations are used in the absence of vendor input

- When possible, the analyst will ask the researcher to validate the mitigation and/or patch
  - The V&V Lab acts as a fallback for uncooperative/unresponsive vendors and researchers. They can be asked to verify patches or proposed workaround mitigations
- A rollout time is accounted for in disclosure deadline coordination

- An advisory is drafted and then published after being reviewed by both the security researcher and the vendor
- A CVE number is assigned (can happen any time during the coordination process)
- An advisory is published on CISA's website
- A CVE record is submitted to the CVE Program

Comments/Questions?