Vulnerability Coordination SIG

Mission

Historically, foundational work on best practices, policy and process for vulnerability disclosure focused on bi-lateral coordination and did not adequately address the current complexities of multi-party vulnerability coordination. Factors such as a vibrant open source development community, the proliferation of bug bounty programs, third party software, supply chain vulnerabilities, and the support challenges facing CSIRTs and PSIRTs are just a few of the complicating aspects.

The Industry Consortium for Advancement of Security on the Internet, ICASI, proposed to the FIRST Board of Directors that a Special Interest Group (SIG) be considered on Vulnerability Disclosure. After holding meetings at the FIRST Conferences in Boston in June 2014, ICASI formally requested FIRST to charter a SIG to review and update vulnerability coordination guidelines.

No single entity or group of stakeholders has tried to solve this coordination challenge, as it requires a multi-faceted perspective looking at working a multi-stakeholder solution.

The Vulnerability Coordination SIG is chartered to do this.

We took the opportunity to create a community-led work group to address the challenges and opportunities related to handling these issues and develop a multi-faceted solution.

Goals & Deliverables

Develop and execute a strategy for improving vulnerability coordination globally.

- Develop and publish a common set of 'coordination principles'
- Develop and publish vulnerability coordination best practices, which include use cases or examples that describe scenario and disclosure paths:
  - The *Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure* was updated in May 2020. It is available both in web and PDF formats. The SIG welcomes comments at vulncoord-sig-comments@first.org.
- Collate and publish a compendium of coordination resource documents

Chairs

- Art Manion, CERT Coordination Center
- Bruce Monroe, Intel

Member Expectations

- Participants should be willing to actively participate, contribute, write, and review.
- Participants should be active members of FIRST or other key stakeholders in the communities of interest to this SIG (e.g., PSIRTs, open source, vendors, CSIRTs).
- Activities will include participation in working conference calls and the development and review of SIG materials.

Request to Join

Initiatives

- Special Interest Groups (SIGs)
  - SIGs Framework
  - Academic Security SIG
  - Automation SIG
  - Big Data SIG
  - Common Vulnerability Scoring System (CVSS-SIG)
  - CSIRT Framework Development SIG
  - Cyber Insurance SIG
  - Cyber Threat Intelligence SIG
  - DNS Abuse SIG
  - Ethics SIG
  - Exploit Prediction Scoring System (EPSS)
  - FIRST Multi-Stakeholder Ransomware SIG
  - Industrial Control Systems SIG (ICS-SIG)
  - Information Exchange Policy SIG (IEP-SIG)
  - Information Sharing SIG
  - Malware Analysis
  - Metrics SIG
  - Passive DNS Exchange
  - PSIRT SIG
  - Red Team SIG
  - Retail and Consumer Packaged Goods (CPG) SIG

Multi-Party Vulnerability Coordination and Disclosure

Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure — Version 1.1 is available as:

- HTML Format
- PDF Format