PSIRT Special Interest Group

2021/2022 Highlights

Co-chairs: Pete Allor, Josh Dembling

Agenda

- Our History
- Our Future
- Call to action

Our Mission

The PSIRT SIG is an assembly of **active industry practitioners** driving the evolution of PSIRT practices by developing and maturing product security response, through **collaborating** to bridge the knowledge gap between vulnerability and response aspects of product security from newly formed to well-established teams.

The SIG will **educate and inform PSIRTs on known good practices**, continue the development of the PSIRT Services Framework, curate and develop supporting training materials, and empower them to rapidly address the evolving threat landscape.

Our History

- Formed 8 years ago to create the PSIRT Services Framework
- Developing the PSIRT Common Body of Knowledge
- We have ~100 individuals from 44 companies (22 / 9)
- Conducted the 6th Annual FIRST PSIRT TC – and first hybrid TC
- Delivered PSIRT Services Framework v1.0 2017, v1.1 2019
- Produced Overview PSIRT Training Videos and Maturity Guide 2018
- Enable the Exchanged Best Practices between PSIRT participants
- Conference vs TC

Goals and Deliverables

- Foster collaboration between PSIRTs across different organizational and industry verticals
- Develop and share a common body of knowledge (CBK) on PSIRT best practices
- Produce PSIRT-focused collateral to assist in educating corporate leadership and Government CSIRTs / legislative bodies
- Curate a list of all PSIRT-focused conferences and colloquia
- Publish a PSIRT capability maturity assessment
- Develop and publish PSIRT focused materials to quickly establish new groups to work well from starting operations

Goals and Deliverables

- Provide online education and training materials to PSIRTs of various maturity levels.
    - Publish presentations on PSIRT Education topics on the FIRST website under a creative commons license.
    - The presentations will be organized by topic (Intro, Process, Consuming (i.e. OSS, vendor code), Response, Scoring, Tooling, Support).
    - Reach a wide audience (Baseline, Company, PSIRT Ops, PSIRT Leadership/Management, QA, Security Officers, Security Engineers).
    - The content will be compiled by PSIRT SIG members and the greater FIRST community and will align to the PSIRT Framework and terminology.
    - The presentations are grouped by priority level (high 1 – 5 low) and will be released in batches according to priority level.

Working Group Strategy

Past: The SIG has operated now for the past seven years continuously and prior to moving into our four regular working groups, met bi-weekly with about 20 sessions per year plus a three day in-person TC, with a workshop and the Annual Conference for an additional face-to-face.

Current: there are now four constituted Working Groups:

- Framework 2.0, Maturity and Supporting Documentation
- PSIRT Tooling
- PSIRT Education
- Third Party Components

Working Groups focus

- Services Framework - Develops guides and information on the implementation and operation of a PSIRT and maturity
- Education - curate and develop educational and training materials to empower entities to start and operate their own PSIRTs
- Third Party Components - discuss common issues, share expertise, and best practices regarding component manifest related to their security programs; provide productive input to the industry
- Tooling - Explore, gather, establish and improve an arsenal of tools and techniques that help PSIRTs deliver their services

Future Thoughts / Considerations

- PSIRTs Conference Track
- Open source tooling for our PSIRT Needs
  - Devops versus Operators
  - VINCE modifications(?)
  - Manifesting and SBOM preparations
- Organizational Coordination & Response
- CVD updates to operational approaches
- Do we restructure
- Can we maintain momentum (Participation)
- TC Planning for 2021

Our Future - Working Groups

Does your organization write and distribute apps?

Are you producing code and putting it out for customers?

If you are, you have crossed into needing to run PSIRT Operations.

Doing PSIRT ops well, come share your practices and challenges

Members of PSIRTs come join us!