SONiC security issues process

See also: sonic-report-security-issue

The security working group leads the discussion about security issues, engages resources to address them, and creates security advisories.

The basic workflow is:

1. A community member reports a problem publicly on github/forum/slack or privately to the security private email.
2. The security team works to understand the problem and engages community members to resolve it.
3. Workarounds and fixes are created, reviewed, and approved.
4. An SONiC security advisory is created if needed.

Work flow highlights:

1. Handle new problem reports
    - Within 2 business days, acknowledge you received the report.
    - Communicate within the security working group.
2. Analyze the problem
    - Is this problem new or known?
    - Is this problem in SONiC, upstream, or downstream?
    - Which SONiC areas should address the problem?
    - Gather data for the security advisory if applicable.
3. Bring in folks as needed (upstream, downstream, and SONiC)
    - Coordinate with all stakeholders and keep them informed.

    For private communicated issues:
    - Use private channels, e.g., email.
    - Keep the issue private untill it is resolved or workarounded.
4. For SONiC problems:
    - Determine if this is a high severity problem.
      For example use: CVSS metrics
    - Create SONiC security advisory if needed.
    - Improve SONiC processes to avoid future problems.