ONAP Vulnerability Management process review

Pawel Pawlak

12th June 2019

History

- Process documented on Wiki based on some industry best practices compilation
- Some updates required based on discussions with Robert…
- Updated process proposal with Krzysztof
- https://wiki.onap.org/display/DW/ONAP+Vulnerability+Management

Intro

- Vulnerability Management Subcommittee (VMS) is responsible for coordinating the response to a reported vulnerability from initial reporting until coordinated disclosure.
- Supported versions: Dublin and beyond
- Third party components (i.e. dependencies) are only in scope for security support if they are statically compiled or otherwise bundled by an ONAP project.
- Vulnerabilities of managed functions (e.g. VNFs) are out of the scope of ONAP, however if an ONAP vulnerability has a dependence with a managed function, the managed functions vulnerability procedures will be used to coordinate the issue.

The Process

- Reception:
  - By jira ticket
  - By e-mail sent to VMS member
  - Bug reception should be confirmed no later than **within 3 business days**.
  - Vulnerability Reporting Jira Project by default is visible only to reporter and VMS members
- Triage
  - The bug must then be confirmed to be a security problem and assigned initial severity level. This may require the inclusion of additional subject matter experts to determine if the problem needs to be treated as a security flaw. If the bug is determined not be a security issue then a statement should be added indicating the justification. The bug should then be opened and fixed by following the normal development process.
- Patch development
- Patch review
- Draft Vulnerability description
- Review impact description
- Send CVE request
- Get assigned CVE
- Embargoed disclosure
- Coordinated disclosure
- Handling public/leaked security issues

Lessons Learned

- It takes time…
- As we are pioneers, we all learn
- Not all stakeholders received notifications
- Politics in companies ;-)
- Rules for the distribution list: onap-vulnerability-notification@lists.onap.org
- Repo: OSA = ONAP Security Advisory


ONAP
OPEN NETWORK AUTOMATION PLATFORM