Value of Global Vulnerability Reporting

David Waltermire

National Institute of Standards and Technology

david.waltermire@nist.gov

Current State of Global Vulnerability Reporting

- Software is increasingly being distributed globally
- Vulnerability identifiers are generally assigned within a database, vendor, regional, or national context
- While vulnerabilities are disclosed asynchronously, vulnerability information is shared synchronously
  - Based on direct collaboration between governments, vendors, and security researchers
  - Sharing is largely point-to-point
- Threats posed by vulnerabilities are asynchronous

Challenges

- Software is increasingly distributed outside national and regional boundaries.
- Thus, the management of software vulnerabilities is becoming increasingly a global problem.
- Corporate, regional, and national differences complicate the management of software vulnerabilities.
  - Language differences
  - Cultural differences in how businesses and commerce are conducted
  - Unique national concerns
  - Regional and global economic factors
- Vulnerability management solutions often use proprietary, regional or national identification formats limiting the ability to share and link useful information.
- The potential for automation is restricted due to limited standardization in this space.

Why are we here?

- To better enable the global management of software vulnerabilities we all need to understand:
  - The global landscape for vulnerability reporting.
  - Regional and global vulnerability challenges
    - Challenges that have been addressed historically and their solutions.
    - What approaches haven't worked well to address historic challenges.
    - Current challenges and what is being done to address them.
    - Potential future challenges.
- To begin a dialog to identify possible solutions.

What is the Value of Global Vulnerability Reporting

- Enable greater collaboration between companies, researchers, and nations supporting the management of software vulnerabilities and security incidents.
  - Standardized identification method(s)
  - Standardized data formats
  - Coordination methods and processes
  - Makes data sharing more asynchronous
- Improve the efficiency, fidelity, and accuracy of software vulnerability information on a global scale.
- Enable greater automation in the identification, detection, and management of vulnerabilities.

Key Questions – Software Publication

For each nation/region:

- Is software distributed on a national, regional, or global basis?
- Are there regional market or national concerns that need to be addressed?

Key Questions – Vulnerability Identification

For each nation/region:

- What are the rules or criteria used in deciding what vulnerabilities need to be identified?
- How are vulnerability identifiers structured?
- How are vulnerability identifiers used?
- What is the process you use to assign and manage vulnerability identifiers?
- Are there regional market or national concerns that need to be addressed?
- Do identifiers in your nation/region look similar to vulnerability identification schemes used elsewhere?
- Do you support zero-day issues or only previously identified vulnerabilities?

Key Questions – Vulnerability Reporting

For each nation/region:

- What vulnerability information is shared?
- What are the authoritative locations of vulnerability information for your area?
- How is your approach similar to approaches used elsewhere? How is it unique to your nation/region?
- Are there regional market or national concerns that need to be addressed?

Key Questions – General

For each nation/region:

- What do you like about your approach to vulnerability reporting?
- What do you like about approaches used in other places?
- Do you see common processes, standards, technologies, and techniques that would address your challenges?

Conclusions

Through better understanding of how vulnerabilities are managed, we can put in place global solutions that enable:

- Greater collaboration between companies, researchers, and nations supporting the management of software vulnerabilities and security incidents.
- Improve the efficiency, fidelity, and accuracy of software vulnerability information on a global scale.
- Enable greater automation in the identification, detection, and management of vulnerabilities.