Future of Global Vulnerability Reporting Summit

Summit Days

15 November 2012
afternoon session
agenda and discussion notes

November 15, 2012

Masato Terada

afternoon session agenda.

- Discussion topics
    - Requirements for Global Sharing
    - Process for Global Sharing
    - Best Practice for Vulnerability Information Sharing
        - Vulnerability Databases
        - Coordination
        - Vendors
        - Researchers
        - ALL (includes above)
    - Taxonomy / Format for exchange (Publication)
- Proposal VRDX SIG activities

afternoon session discussion notes.

- **[Requirements for Global Sharing]**
  - Establish universal communication channels
    -> Infrastructure (mailing list, server, ID management, etc.)
  - Funding??
  - Maintenance of this system
    - One database for global identifiers?
    - How to manage various databases that use/reference global databases
    - An easy way to cross-reference??
  - Established set of steps necessary to be able to obtain/contribute information into this scheme
  - Must be flexible
  - Must be usable in all markets
  - Minimize overhead (less required coordination, maintenance)

afternoon session discussion notes(cont).

- **[Requirements for Global Sharing]**
  - Timely distribution of a "universal identifier“
  - There is a proper balance between globalization / localization
    -> Supporting multiple languages => is this required?
    -> Supporting different calendars (Gregorian vs Buddhist)
    -> Being able to handle cultural / time differences / multiple types of disclosure practices
  - Mechanism to know "what issue we are talking about" in communications
  - Properly scoped -> who is "responsible“
    -> determining the timing for global sharing of this information
    -> criteria for what issues should be shared on global scale
  - Mechanism for dealing with conflicts and duplicates
    -> A good process that minimizes conflicts / duplicates
  - Machine readable format for global exchange of information

afternoon session discussion notes(cont).

- **[Requirements for Global Sharing]**
  - A global vulnerability identifier format/definition that can be used globally
    -> Easy migration for users
    -> Transition plan from current "global ID = CVE“
    -> User education on the new format
  - Mechanism or definition on how to count vulnerabilities
  - What details need to be shared (need to agree on at least the minimum attributes)

afternoon session discussion notes(cont).

- **[Process for Global Sharing]**
  - Separate procedures for already disclosed vulnerabilities / coordinated vulnerabilities
  - Instead of defining "steps" but a "guideline" on the steps that may occur during the process
  - Defining the types of organizations that are involved in this process
    -> Vendor / developer
    -> Disclosure coordinator (CERT/CC, JPCERT/CC, CERT-FI, KrCERT/CC, etc.)
    -> Global / Regional ID managing entities
  - Operational training for organizations that will be sharing this information
  - Classifications of the information to be shared
  - Assigning a global vulnerability identifier

afternoon session discussion notes(cont).

- **[Best Practices for Vulnerability Information Sharing]**
  - These processes need to be documentation for each party
    - There may not be documentated processes for vulnerability databases
  - * Vulnerability Databases *
    - Disputes / corrections that need to be made to an issue
    - How the information is made available
    - Input on how the CNVDB currently works / managed
    - MITRE has a set of expectations that we may be able to use as a starting point
  - * Coordination *
    - Current entities (CERT/CC, JPCERT, CERT-FI) can create documentation for general guidelines on information sharing
    - Encourage input from other organizations to improve the process

afternoon session discussion notes(cont).

- **[Best Practices for Vulnerability Information Sharing]**
  - * Vendors *
    - Current expectations of vendors in the Japan Framework can be documented as a starting point for a discussion
    - MITRE has a set of expectations that we may be able to use as a starting point
  - * Researchers *
    - MITRE has a set of expectations that we may be able to use as a starting point
  - * All (including above) *

afternoon session discussion notes(cont).

- **[Taxonomy / Format for Exchange / Publication]**
  - Machine readable format
  - Is it necessary to have different formats for different times during the coordination process
    - Original report
    - Status updates on remediation
    - Advisory publication
    - Perhaps one format and fill in as the process is going on
  - Needs to be extensible for future use
    - should be flexible enough to allow other data to be incorporated
  - Capture enough context for the use case profile
    - who is providing the information / when is it being provided

About FIRST TC @ Kyoto Summit Days

Future of Global Vulnerability Reporting Summit

Future of Global Vulnerability Reporting Summit focuses on Current challenges & issues (coverage, scale, numbering and etc.) and proposed solutions of vulnerability tracking, especially "Global Vulnerability Identification Scheme".

Currently one of the most well known vulnerability identification schemes is Common Vulnerabilities and Exposures (CVE). CVE is used by many organizations throughout the world for cross-referencing vulnerabilities across various databases. However, the current process governing CVE has its limitations and has not been able to keep up with the ever increasing number of vulnerabilities being discovered and made public each year. At first, we would like to discuss the limitations of the current process, and how organizations currently use CVE to link their databases across the globe to for cross-referencing vulnerabilities. Second, we would like to discuss the next steps for challenge of "Global Vulnerability Identification Scheme" on the final day.