A Model for Exchanging Vulnerability Information draft-booth-sacm-vuln-model-01

http://datatracker.ietf.org/doc/draft-booth-sacm-vuln-model/

David Waltermire (david.waltermire@nist.gov)

Presenting for:

Harold Booth (harold.booth@nist.gov)

What is it?

- An XML-based data format that enables the exchange of structured information related to vulnerabilities

- A revision to the current Vulnerability Data Model v2.0 used by the National Vulnerability Database
  - Feeds downloaded by academia, security tool vendors, industry and other vulnerability databases

What information does it capture?

- Community and proprietary vulnerability identifiers (e.g. Common Vulnerability and Exposures (CVE), vendors ids, vulnerability database identifiers)
  - Captures relationships within the same identification system (e.g. supersession, deprecation)
  - Identifies aliases between different identification systems
- Uses the Common Platform Enumeration (CPE) to relate vulnerable product configurations
  - Application
  - Operating system
  - Application running on operating system
- Plugs-in Common Vulnerability Scoring System (CVSS) v2 scoring information
  - Allows other scoring systems to be used
- Relates a vulnerability to references:
  - Vulnerability advisories, alerts and bulletins describing the vulnerability in greater detail
  - Patch and work-around information
  - Assessment methods

How does it relate to the IETF?

Security Automation and Continuous Monitoring (SACM)

Use Case 1: System State Assessment (draft-waltermire-sacm-use-cases-02)

- Vulnerability Management Use Case (4.1.2.2)
  - Enumerates technical assessment methods
- Assessment Result Analysis (4.1.3)
  - Provides vulnerability scores enabling comparison/ weighting of assessment results
  - Supports Risk-based decision making
- Content management (4.1.4)
  - Captures scoring models and vulnerability information
  - References additional vulnerability and patch information

How does it relate to the IETF? (Cont'd)

Security Automation and Continuous Monitoring (SACM)

Use Case 3: Security Control Verification and Monitoring (draft-waltermire-sacm-use-cases-02)

- Tasking and Scheduling (4.3.1)
  - Selection of assessment criteria
  - Defining in-scope assets (i.e. targeting)
- Data Aggregation and Reporting (4.3.2)
  - Enables correlation by vulnerability identifiers and other vulnerability attributes (e.g.. scores, product)

How does it relate to the IETF? (Cont'd)

Managed Incident Lightweight Exchange (MILE WG)

IODEF-extension to support structured cybersecurity information (draft-ietf-mile-sci-05)

- Section 4.3.3: Vulnerability
  - Enables inclusion of information for (candidate) vulnerabilities related to incidents or events
  - Possible candidate for inclusion in the IANA registry (Appendix II)

Possible work / How you can help?

- Greater consensus on use cases for vulnerability format
  - Collaboration/integration with other related efforts (e.g. Common Vulnerability Reporting Format (CVRF))
  - Update model to reflect growing consensus
- Develop an IANA registry for pluggable components
  - Allow for additional product identification schemes (e.g. ISO/IEC 19770-2 Software ID Tags)
  - Support multiple scoring metrics/methods (e.g. CVSSv3)
  - Extensible reference types
- Should it be extended to hold patch information?
  - Product/version applicability
  - Patch location information
  - How to install (i.e. exact command-line or execution instructions)
- JSON vs. XML