Vulnerability Model Workshop

Harold Booth

NIST

Agenda

- What is the Vulnerability Data Model (VDM)?
- What is the Common Vulnerability Reporting Framework (CVRF)? – Mike Schiffman (Cisco)
- What are the use cases?
- Questions

What is the Vulnerability Data Model?

- Next iteration of the NVD data feed format
- Documented and now with a name
- Separate out remediation (currently just patch) and threat information
- Restructure the element organization
- Allow for multiple CVSS base vectors and scores (attack-vector element) one per configuration

Don’t Worry

- Any information NVD currently provides that is not in the model will be added as an NVD specific extension for anyone who needs the information

What is the Vulnerability Data Model?

Property	Type	Count	Description
vulnerability-id (element)	vulnerabilityIdType	1	The primary globally unique identifier for the vulnerability. An example is a CVE identifier.
vulnerability-id-alias (element)	vulnerabilityIdType	0-n	Additional identifiers for the vulnerability that represent it in other data sources.
record-metadata (element)	metadataType	1	Additional metadata about the record.
summary (element)	meta:localeTextType	1-n	A summary of the vulnerability. No more than a single instance of this element should exist per language.
description (element)	meta:xhtmlLocaleTextType	1-n	A brief formatted description of the vulnerability. This description should provide sufficient detail to allow an individual to determine why a given vulnerability is distinct from any other vulnerability. Providing descriptions in multiple languages and in a marked up format such as XHTML will assist in internationalization of the data and in providing consistent display capabilities. No more than a single instance of this element should exist per language.
references (element)	vulnerabilityReferenceType	1-n	References to additional information about the vulnerability.

What is the Vulnerability Data Model?

Property	Type	Count	Description
discovered (element)	meta:lifecycleEventType	0-1	Date that the vulnerability was first discovered.
disclosure (element)	meta:lifecycleEventType	0-1	Date and time that the vulnerability was disclosed to the public.
vendor-notification (element)	meta:lifecycleEventType	0-1	Date and time that the software vendor was first notified of the vulnerability.
vulnerable-software-list (element)	vulnerableSoftwareType	0-1	A list of CPE names corresponding to the software versions that have this vulnerability.
vulnerable-configuration (element)	vulnerableConfigurationType	0-n	A CPE Language construct that identifies the conditions under which the vulnerability exists. Only needed when the vulnerability is situationally exploitable.
attack-method (element)	attackMethodType	0-n	Information on the attack method(s) that could be used to exploit the vulnerability.
exploit-info (element)	exploitInfoType	0-n	The set or sequence of actions that could be used to exploit the vulnerability.
##other	xsd:any	0-n	Extension point for additional information.

Common Vulnerability Reporting Framework

Mike Schiffman

Use Cases

- Enable a “Value Chain”
  - MITRE creates a CVE
  - NVD adds configuration and CVSS information
  - Security vendors add additional information useful to their customer base
    - Temporal metrics
    - Additional assessment information
  - End-user organizations may further augment with proprietary information

Use Cases

- Vulnerability Reporting
  - Product vendors
  - Security researchers
  - Security vendors
  - Vulnerability databases

Use Cases

- Machine Processing
  - Consumed and processed by a machine
    - Analytics
    - Automated decision support
- Analytics
  - Prioritization
  - Risk Scoring
  - Enterprise Impact Analysis
  - Attack Graph Analysis
  - Trending

Use Case

- Others?

Minimum number of elements?

- What are the minimum elements required?
- ID
- Summary
- Description
- References

Allow check content directly?

- Optionally allow check content directly instead of references?

Temporal Metrics?

- Do they belong here or in threat?

Additional fields?

- What additional fields are useful to support other use cases?
  - Additional Analytics
  - Further Explicit decomposition of the description
- Provenance information to support the value-chain

What are vulnerability facts?

- CVSS Version 2 Exploit Metrics
  - Access Vector
  - Access Complexity
  - Authentication
- CVSS Version 2 Impact Metrics
  - Confidentiality
  - Integrity
  - Availability
- Are there more granular items that we could capture?

Getting Involved

- Contact me: harold.booth@nist.gov
- Email to: emerging-specs@nist.gov
- Submit comments on NIST IR 7690
- CVRF: mschiffm@cisco.com