Requirements and Recommendations for CVE Compatibility

Date: June 30, 2013
Document version: 1.3

Authors:

Robert A. Martin, CVE Compatibility Lead - ramartin@mitre.org
Steven M. Christey, CVE Technical Lead - coley@mitre.org

Table of Contents

1. Definitions
2. High-Level Requirements
3. Accuracy
4. Documentation
5. CVE Date Usage
6. Old Style CVE Name Support
7. Revocation of CVE Compatibility
8. Review Authority
9. Appendix A: Type-Specific Requirements
10. Appendix B: Media Requirements

1. Definitions

Capability - security tool, database, Web site, advisory, or service that provides a security vulnerability or exposure identification function.

User - a consumer or potential consumer of the Capability.

Owner - the owner or maintainer of the Capability.

Security Element - a database record, email message, security advisory, assessment probe, signature, etc., which is related to a specific vulnerability or exposure.

Repository - an implicit or explicit collection of security elements that supports a capability, e.g., a vulnerability database, advisory archive, the set of signatures in an intrusion detection system (IDS), or Web site.

Tool - a software application or device that either examines a host or network and produces information that is related to vulnerabilities or exposures or aggregates this type of information, e.g., a vulnerability scanner, intrusion detection system, risk management, security information manager, or compliance reporting tool or service.

Task - a Tool’s probe, check, signature, etc., which performs some action that produces security information (i.e., the security element).

Map/Mapping - the specification of relationships between security elements in a Repository and the CVE names that are related to those elements.

Review - the process of determining whether a capability is CVE-compatible.

Review Date - the date of the CVE content that is being used for determining CVE compatibility of a capability.

Review Authority - an entity that performs a Review. MITRE is the only Review Authority at this time.

Review Sample - the set of security elements in the capability’s repository that is used by the Review Authority for evaluating accuracy.

Accuracy Percentage - the percentage of security elements in the Review Sample that reference the correct CVE identifiers

Sampling Method - the method by which the Review Authority identifies the set of security elements in the Review Sample.

Sample Size - the percentage and/or the number of security elements to be examined by the Review Authority.

2. High-Level Requirements

These are the high-level requirements for all capabilities. Many of them are described in detail in later sections.

Prerequisites

2.1) The Owner MUST be a valid legal entity, i.e., an organization or a specific individual, with a valid phone number, email address, and street mail address.

2.2) The capability MUST provide additional value or information beyond that which is provided in CVE itself (i.e., name, description, references, and associated data).

2.3) The Owner MUST provide the Review Authority with a technical point of contact who is qualified to answer questions related to the mapping and any CVE-related functionality of the capability.

2.4) The capability MUST be available to the public, or to a set of consumers, in a production version.

2.5) The Owner MUST provide the Review Authority with a completed "CVE Compatibility Requirements Evaluation Form."

2.6) For a capability with a Repository, the Owner MUST provide the Review Authority with free access to the Repository so that the Authority can determine that the Repository satisfies all associated requirements.

2.7) For a capability with a Repository, the Owner MUST allow the Review Authority to use the Repository to identify any vulnerabilities that must be added to CVE.

2.8) The Owner MUST agree to abide by all of the mandatory CVE Compatibility Requirements, which includes the mandatory requirements for the specific type of capability.

Functionality

2.9) The capability MUST allow users to locate security elements using CVE names ("CVE-Searchable").

2.10) When the capability presents security elements to the user, it MUST allow the user to obtain the associated CVE names ("CVE-Output").

2.11) For a capability with a Repository, the capability's mapping MUST accurately link security elements to the appropriate CVE names ("Mapping Accuracy").

2.12) The capability's documentation MUST adequately describe CVE, CVE compatibility, and how the CVE-related functionality in the capability is used ("CVE-Documentation").

2.13) The capability MUST state the date of its currency with respect to CVE ("Date Usage")

2.14) The capability MUST satisfy any additional requirements for the specific type of capability, as specified in Appendix A.

2.15) The capability MUST satisfy all requirements for its distribution media, as specified in Appendix B.

2.16) The capability is NOT REQUIRED to do any of the following:

- use the same descriptions or references as CVE
- include every CVE name in its repository

Miscellaneous

2.17) If the capability does not satisfy all requirements, then the Owner MUST NOT advertise that it is CVE-compatible.

3. Accuracy

CVE compatibility only facilitates data sharing if the capability's mapping is accurate. Therefore, CVE-compatible capabilities must meet minimum accuracy requirements.

3.1) For a capability with a Repository, the Repository MUST have an Accuracy Percentage of 90 percent or greater.

3.2) During the review period, the Owner MUST correct any mapping errors found by the Review Authority.

3.3) After the review period, the Owner SHOULD correct a mapping error within a reasonable time frame after the error was initially reported, i.e., within six (6) months for tools and three (3) months for on-line capabilities and services.

3.4) For a capability with a Repository, the Owner SHOULD prepare and sign a statement that, to the best of the Owner's knowledge, there are no errors in the mapping.

3.5) If the capability is based on, or uses, another CVE-compatible capability (the "Source" capability), and the Owner becomes aware of mapping errors in the Source capability, then the Owner MUST report those errors to the Owner of the Source capability.

3.6) The mapping accuracy for Advisory archives MUST be performed against all of the security elements of the archive repository subsequent to, and including, the archive's first use of a CVE name in a security element.

3.7) A capability MUST accurately reflect the status of deprecated CVE names within three (3) months for on-line capabilities and services.

4. Documentation

The following requirements apply to documentation that is provided with the capability.

4.1) The documentation MUST include a brief description of CVE and CVE compatibility, which can be based on verbatim portions of documents from the CVE Web site.

4.2) The documentation MUST describe how the user can find individual security elements in the capability's repository by using CVE names.

4.3) The documentation MUST describe how the user can obtain CVE names from individual elements in the capability's repository.

4.4) If the documentation includes an index, then it SHOULD include references to CVE-related documentation under the term "CVE."

5. CVE Date Usage

Users must know how "up-to-date" a capability's repository is with respect to its mapping to CVE. The capability owner needs to indicate the currency of a mapping by providing the date of its last update of CVE information and indicate what portion of CVE content they utilize and where they gather the CVE content from.

5.1) Each new version of the capability MUST identify the most recent date of CVE content that was used in creating or updating the mapping through at least one of the following: change logs, new feature lists, help files, or some other mechanism. The capability is "up-to-date" with respect to that date.

5.2) Each new version of the capability MUST be up-to-date with respect to a stated CVE date that is no more than three (3) months before the capability was made available to its users. If a capability does not satisfy this requirement, then it is "out-of-date."

5.3) The Owner MUST publicize how quickly it will update the capability's repository to include new CVE information.

5.4) The Owner MUST describe the criteria and mechanism for selecting the CVE information they include in their capability.

5.5) The Owner MUST describe where it gathers new CVE content from.

6. Different Styles of CVE Name Support

A capability MUST function with CVE names independent of the format of the CVE name's representation in the capability, whether it is using the older style four-digit CVE-ID Syntax or the, four-digit or higherdigit CVE-ID Syntax (used after the CVE-ID Syntax modification in use after December 31, 2013).

6.1) If a user performs a search using YYYY-NNNN, YYYY-NNNNN, or YYYY-NNNNNN, the capability MUST return the security elements that correspond to CVE-YYYY-NNNN, CVE-YYYY-NNNNN, or CVE-YYYY-NNNNNN respectively, regardless of whether the CVE name has a CVE or CAN as the first part of its name, within the capability's repository.

6.2) If the Capability contains the CVE name CVE-YYYY-NNNN, but the user searches using the old format for a CVE name, CAN-YYYY-NNNN (used before the CVE naming scheme modification introduced 19 October 2005), then the Capability SHOULD return CVE-YYYY-NNNN.

7. Revocation of CVE Compatibility

7.1) If a Review Authority has verified that a Capability is CVE-compatible, but at a later time the Review Authority has evidence that the requirements are not being met, then the Review Authority MAY revoke its approval.

7.1.1) The Review Authority MUST identify the specific requirements that are not being met.

7.2) The Review Authority MUST determine if the actions or claims of the Owner are "intentionally misleading."

7.2.1) The Review Authority MAY interpret the phrase "intentionally misleading" as it wishes.

7.3) Unless recommended by two CVE Editorial Board members who do not have a conflict of interest, the Review Authority SHOULD NOT consider revoking CVE compatibility for a particular Capability more often than once every six (6) months.

Warning and Evaluation

7.4) The Review Authority MUST provide the Capability Owner and Technical POC with a warning of revocation at least two (2) months before revocation is scheduled to occur.

7.4.1) If the Review Authority has found that the Owner's actions or claims are intentionally misleading, then the Review Authority MAY skip the warning period.

7.5) If the Owner believes that the requirements are being met, then the Owner MAY respond to the warning of revocation by providing specific details that indicate why the Capability meets the requirements under question.

7.6) If the Owner modifies the Capability so that it complies with the requirements in question during the warning period, then the Review Authority SHOULD end the revocation action for the Capability.

Revocation

7.7) The Review Authority MAY delay the date of revocation.

7.8) The Review Authority MUST publicize that CVE compatibility has been revoked for the capability.

7.9) If the Review Authority finds that the Owner's actions with respect to CVE compatibility requirements are intentionally misleading, then revocation SHOULD last a minimum of one year.

7.10) The Review Authority MAY publicize the reason for revocation.

7.11) If the approval is revoked, the Owner MUST NOT apply for a new review during the period of revocation.

8. Review Authority

For any review conducted by the Review Authority:

8.1) The Review Authority MUST review the capability for CVE compatibility with respect to a specific CVE content date, i.e., the Review Date.

8.2) The Review Authority MUST clearly identify the Review Date that was used to determine compatibility for the capability.

8.3) The Review Authority MUST clearly identify the version of the CVE compatibility requirements document that was used to determine compatibility for the capability.

8.4) The Review Authority MUST define and publish a Sample Size.

8.4.1) The Review Authority SHOULD use a Sample Size of 50 elements plus 5 percent of the capability's repository, up to a maximum Sample Size of 400 elements.

8.4.2) The Review Authority MAY review every element in the capability's repository.

8.5) The Review Authority MUST publicize the Sampling Method.

8.6) The Review Authority MAY use a Review Sample that was not randomly selected.

8.7) The Review Authority MUST use the same Sampling Method and Sample Size for all capabilities that are evaluated within the same time frame.

Appendix A: Type-Specific Requirements

Since a wide variety of capabilities use CVE, certain types of capabilities may have unique features that require special attention with respect to CVE compatibility.

A.1) The Capability MUST satisfy all additional requirements that are related to the specific type of capability.

A.1.1) If the Capability is a vulnerability assessment scanner, intrusion detection system (IDS), or a product which integrates the results of one or more scanners and IDSs, then it must satisfy the Tool Requirements, A.2.1 - A.2.8.

A.1.2) If the Capability is a service (such as a managed intrusion detection and response service, or a remote scanning service) then it must satisfy the Security Service Requirements, A.3.1 - A.3.5.

A.1.3) If the Capability is an online vulnerability or signature database, Web-based archive, or maintenance/patch site, then it must satisfy the Online Capability Requirements, A.4.1 - A.4.3.

A.1.4) If the Capability is an aggregation tool like a security information manager, a compliance reporting tool, or a service supplying these types of aggregations of vulnerability type information, then it must satisfy the Aggregation Capability Requirements, A.5.1 - A.5.6.

Tool Requirements

A.2.1) The Tool MUST allow the user to use CVE names to locate associated Tasks in that Tool ("CVE-Searchable") by providing at least one of the following: a "find" or "search" function, a mapping between that Tool's Task names and CVE names, or another mechanism.

A.2.2) For any report that identifies individual security elements, the Tool MUST allow the user to determine the associated CVE names for those elements ("CVE-Output") by doing at least one of the following: including CVE names directly in the report, providing a mapping between the Tool's Task names and CVE names, or using some other mechanism.

A.2.3) Any required reports or mappings MUST satisfy the media requirements as specified in Appendix B.

A.2.4) The Tool, or the Owner, SHOULD provide the user with a list of all CVE names that are associated with the Tool's Tasks.

A.2.5) The Tool SHOULD allow the user to select a set of Tasks by providing a file that contains a list of CVE names.

A.2.6) The interface of the Tool SHOULD allow the user to browse, select, and deselect a set of Tasks by using individual CVE names.

A.2.7) If the Tool does not have a Task that is associated with a CVE name as specified by the user in the A.2.5 or A.2.6 Tool requirements, then the Tool SHOULD notify the user that it cannot perform the associated Task.

A.2.8) The Owner MUST warrant that (1) the rate of false positives is less than 100 percent, i.e., if the Tool reports a specific security element, it is at least sometimes correct, and (2) the rate of false negatives is less than 100 percent, i.e., if an event occurs that is related to a specific security element, then sometimes the Tool reports that event.

Security Service Requirements

Security services might use CVE-compatible tools in their work, but they may not provide their customers with direct access to those tools. Thus it could be difficult for customers to identify and compare the capabilities of different services. The Security Service Requirements address this potential limitation.

A.3.1) The Security Service MUST be able to use CVE names to tell a user which security elements are tested or detected by the service ("CVE-Searchable") by doing one or more of the following: providing the user with a list of CVE names that identify the elements that are tested or detected by that Service, providing the user with a mapping between the Service's elements and CVE names, responding to a user-supplied list of CVE names by identifying which of the CVE names are tested or detected by the Service, or by using some other mechanism.

A.3.2) For any report that identifies individual security elements, the Service MUST allow the user to determine the associated CVE names for those elements ("CVE-Output") by doing one or more of the following: allowing the user to include CVE names directly in the report, providing the user with a mapping between the security elements and CVE names, or by using some other mechanism.

A.3.3) Any required reports or mappings that are provided by the Service MUST satisfy the media requirements as specified in Appendix B.

A.3.4) If the Service provides the user with direct access to a product that identifies security elements, then that product SHOULD be CVE-compatible.

A.3.5) The Owner MUST warrant that (1) the rate of false positives is less than 100 percent, i.e., if a Tool reports a specific security element, it is at least sometimes correct, and (2) the rate of false negatives is less than 100 percent, i.e., if an event occurs that is related to a specific security element, then sometimes the Service reports that event.

Online Capability Requirements

A.4.1) The Online Capability MUST allow a user to find related security elements from the Online Capability's repository ("CVE-Searchable") by providing one of the following: a search function with returns CVE names for related elements, a mapping that links each element with its associated CVE name(s), or some other mechanism.

A.4.1.1) The Online Capability SHOULD provide a URL "template" that allows a computer program to easily construct a link that accesses the search function as outlined in Online Capability Requirements A.4.1.

Examples:
http://www.example.com/cgi-bin/db-search.cgi?cvename=CVE-YYYY-NNNN
http://www.example.com/cgi-bin/db-search.cgi?cvename=CVE-YYYY-NNNNN
http://www.example.com/cgi-bin/db-search.cgi?cvename=CVE-YYYY-NNNNNN
http://www.example.com/cve/CVE-YYYY-NNNN.html
http://www.example.com/cve/CVE-YYYY-NNNNN.html
http://www.example.com/cve/CVE-YYYY-NNNNNN.html

A.4.1.2) If the URL template is for a CGI program, the program SHOULD accept the HTTP "GET" method.

A.4.2) For any report that identifies individual security elements, the Online Capability MUST allow the user to determine the associated CVE names for those elements ("CVE-Output") by doing at least one of the following: by allowing the user to include CVE names directly in the report, providing the user with a mapping between the security elements and CVE names, or by some other mechanism.

A.4.3) If the Online Capability does not provide details for individual security elements, then the Online Capability MUST provide a mapping that links each element with its associated CVE name(s).

Aggregation Capability Requirements

A.5.1) The Aggregation capability MUST allow the user to use CVE names to locate associated elements in that capability ("CVE-Searchable") by providing at least one of the following: a "find" or "search" function, a mapping between that capability's names and CVE names, or another mechanism with the approval of the Review Authority.

A.5.2) For any report that identifies individual security elements, the Aggregation capability MUST allow the user to determine the associated CVE names for those elements ("CVE-Output") by doing at least one of the following: including CVE names directly in the report, providing a mapping between the capability's names and CVE names, or using some other mechanism.

A.5.3) Any required reports or mappings MUST satisfy the media requirements as specified in Appendix B.

A.5.4) The Tool, or the Owner, SHOULD provide the user with a list of all CVE names that are associated with the Tool’s Tasks.

A.5.5) The Tool SHOULD allow the user to select a set of Tasks by providing a file that contains a list of CVE names.

A.5.6) The interface of the Tool SHOULD allow the user to browse, select, and deselect a set of Tasks by using individual CVE names.

Appendix B: Media Requirements

B.1) The distribution media that is used by a CVE-compatible capability MUST use a media format that is covered in this appendix.

B.2) The media format MUST satisfy the specific requirements for that format.

Electronic Documents (HTML, word processor, PDF, ASCII text, etc.)

B.3.1) The document MUST be in a commonly available format that has readers which support a "find" or "search" function ("CVE-Searchable"), such as raw ASCII text, HTML, or PDF.

B.3.2) If the document only provides short names or titles for individual elements, then it MUST list the CVE names that are related to those elements ("CVE-Output").

B.3.3) The document SHOULD include a mapping from elements to CVE names, which lists the appropriate pages for each element.

Graphical User Interface (GUI)

B.4.1) The GUI MUST provide the user with a search function that allows the user to enter a CVE name and retrieve the related elements ("CVE-Searchable").

B.4.2) If the GUI lists details for an individual element, then it MUST list the CVE name (or names) that map to that element ("CVE-Output"). Otherwise, the GUI MUST provide the user with a mapping in a format that satisfies the B.3.1 Electronic Documents requirement.

B.4.3) The GUI SHOULD allow the user to export or access CVE-related data in an alternate format that satisfies the B.3.1 Electronic Documents requirement.

Learn More about CVE Compatibility

https://cve.mitre.org/compatible/index.html