INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2009-2012

STUDY GROUP 17

TD 1162

English only

Original: English

Question(s): 4/17 Geneva, 8-17 December 2010

TEMPORARY DOCUMENT

Source: Editors, CYBEX Correspondence Group

Title: Draft Recommendation ITU-T X.1520 [X.cve], *Common Vulnerabilities and Exposures*

Introduction

The annex to this document contains proposed draft Recommendation ITU-T X.1520, *Common Vulnerabilities and Exposures*, for determination at the SG17 December 2010 meeting. This proposed action and the work were re-approved by SG17 at the April 2010, Geneva, meeting (TD 0943 Rev.2).

The editors designated for the progress of the Recommendation were Robert A. Martin (MITRE) and Tony Rutkowski (Yaana Technologies)

The draft was reviewed and edited in detail at the Q.4/17 October Interim Meeting at Tokyo, and accepted with further changes indicated in the document for editing by the CYBEX Correspondence Group and submission to the December 2010 meeting for determination. See Q4-2010-Oct-Doc-009R1, and the report, Q4-2010-Oct-Doc-006R1.

This draft includes continuing work and review since the CYBEX framework was initially conceived at February 2010 Study Group 17 meeting and evolved at multiple subsequent meetings (Q4/17, Geneva, June 2009; SG17, Geneva, Sept 2009; Q4, Redmond, Nov 2009; Q4, Sophia-Antipolis, Jan 2010; SG17, Geneva, Apr 2010; Q4, eMeeting, July 2010; and Q4, Tokyo, Oct 2010) and via teleconferences. The work includes not only that of the editors and others present at these meetings and teleconferences, but also the multiple participating cybersecurity user communities associated with the specifications included in the Framework. As a result, it can be stated with some confidence that global cybersecurity will be significantly enhanced by the adoption of this Recommendation and its continuing evolution.

Appendix:

Recommendation ITU-T X.1520, *Common Vulnerabilities and Exposures* (CVE)

Contact: Robert A. Martin
Editor
Tel: +1 781 271 3001
Email: ramartin@mitre.org

Contact: Tony Rutkowski
Rapporteur
Tel: +1 408 854 8041
Email: tony@yaanatech.com

X.1520

Recommendation ITU-T X.1520

Common Vulnerabilities and Exposures (CVE)

Summary

The **Common Vulnerabilities and Exposures (CVE)** recommendation is a structured means to exchange information security vulnerabilities and exposures that aims to provide common names for publicly known problems. The goal of CVE is to make it easier to share data across separate vulnerability capabilities (tools, repositories, and services) with this "common enumeration." CVE is designed to allow vulnerability databases and other capabilities to be linked together, and to facilitate the comparison of security tools and services. As such, CVE does not contain information such as risk, impact, fix information, or detailed technical information. CVE only contains the standard identifier number with status indicator, a brief description, and references to related vulnerability reports and advisories.

The intention of CVE is to be comprehensive with respect to all publicly known vulnerabilities and exposures. While CVE is designed to contain mature information, the primary focus is on identifying vulnerabilities and exposures that are detected by security tools and any new problems that become public, and then addressing any older security problems that require validation.

X.1520

Recommendation ITU-T X.1520
Common Vulnerabilities and Exposures (CVE)

Table of Contents

Introduction

The **Common Vulnerabilities and Exposures (CVE)** recommendation is a structured means to exchange information security vulnerabilities and exposures that aims to provide common names for publicly known problems. The goal of CVE is to make it easier to share data across separate vulnerability capabilities (tools, repositories, and services) with this "common enumeration." CVE is designed to allow vulnerability databases and other capabilities to be linked together, and to facilitate the comparison of security tools and services. As such, CVE does not contain information such as risk, impact, fix information, or detailed technical information. CVE only contains the standard identifier number with status indicator, a brief description, and references to related vulnerability reports and advisories.

The intention of CVE is to be comprehensive with respect to all publicly known vulnerabilities and exposures. While CVE is designed to contain mature information, the primary focus is on identifying vulnerabilities and exposures that are detected by security tools and any new problems that become public, and then addressing any older security problems that require validation.

CVE is one of a class of ITU-T Recommendations that comes from a large, existing, global development and user community that has written and evolved an open specification that is made available to the ITU-T for adoption with agreement that any changes or updates to the specification will be done in a manner that ensures full technical equivalency and compatibility will be maintained, that discussions about changes and enhancements will be done through the original user community processes, and includes explicit reference to the corresponding specific version maintained by the user community. Thus, at the time of initial adoption of Rec. X.1520, a due diligence verification and statement of equivalency will occur; and as changes are effected among the user community, timely reflection of those changes will be incorporated in subsequent versions of the Recommendation through continued collaboration.

History

This Recommendation is technically equivalent and compatible with the 1.2 version of the "Requirements and Recommendations for CVE Compatibility," 24 August 2009.

RECOMMENDATION ITU-T X.1520

Common Vulnerabilities and Exposures (CVE)

1. Scope

This Recommendation provides a structured means for the global exchange of publicly known, mature vulnerabilities and exposures information that are detected by security tools or otherwise become public. An information security vulnerability is a mistake in software that can be directly used by a hacker to gain access to a system or network. An information security exposure is a mistake in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network. The assignment of CVE identifiers is not within the scope of this Recommendation.

2. References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

3. Definitions

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

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

Exposure: An information security exposure is a mistake in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network.

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

Owner: the owner or maintainer of the Capability.

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.

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: any 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.

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.

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

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

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.

User: a consumer or potential consumer of the Capability.

Vulnerability: An information security vulnerability is a mistake in software that can be directly used by a hacker to gain access to a system or network.

4. Abbreviations and acronyms

IDS Intrusion Detection System

5. Conventions

The key words "required", "shall", "shall not", "should", "should not", "recommended", "may", and "optional" in this Recommendation are interpreted in accordance with ITU-T Author's Guide.

6. High-Level Requirements

Prerequisites

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

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

6.3 The Owner shall 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.

6.4 The capability shall be available to the public, or to a set of consumers, in a production version.

6.5 The Owner shall provide the Review Authority with a completed "CVE Compatibility Requirements Evaluation Form."

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

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

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

Functionality

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

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

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

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

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

6.14 The capability shall satisfy any additional requirements for the specific type of capability, as specified in Appendix A.

6.15 The capability shall satisfy all requirements for its distribution media, as specified in Appendix B.

6.16 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

6.17 If the capability does not satisfy all requirements, then the Owner shall not advertise that it is CVE-compatible.

7. Accuracy

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

7.1 For a capability with a Repository, the Repository shall have an Accuracy Percentage of 90 percent or greater.

7.2 During the review period, the Owner shall correct any mapping errors found by the Review Authority.

7.3 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 two (2) versions of the repository or six (6) months for tools and three (3) months for on-line capabilities and services.

7.4 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.

7.5 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 shall report those errors to the Owner of the Source capability.

7.6 The mapping accuracy for Advisory archives shall 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.

8. Documentation

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

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

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

8.3 The documentation shall describe how the user can obtain CVE names from individual elements in the capability's repository.

8.4 If the documentation includes an index, then it should include references to CVE-related documentation under the term "CVE."

9. 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.

9.1 Each new version of the capability shall 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.

9.2 Each new version of the capability shall 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."

9.3 The Owner shall publicize how quickly it will update the capability's repository to include new CVE information.

9.4 The Owner shall describe the criteria and mechanism for selecting the CVE information they include in their capability.

9.5 The Owner shall describe where it gathers new CVE content from.

10. Old Style CVE Name Support

A capability shall function with CVE names independent of the format of the CVE name’s representation in the capability.

10.1 If a user performs a search using YYYY-NNNN, the capability shall return the security elements that correspond to CVE-YYYY-NNNN, regardless of whether the CVE name has a CVE or a CAN as part of its name, within the capability’s repository.

10.2 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.

11. Revocation of CVE Compatibility

11.1 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.

11.1.1 The Review Authority shall identify the specific requirements that are not being met.

11.2 The Review Authority shall determine if the actions or claims of the Owner are "intentionally misleading."

11.2.1 The Review Authority may interpret the phrase "intentionally misleading" as it wishes.

11.3 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

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

11.4.1 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.

11.5 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.

11.6 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

11.7 The Review Authority may delay the date of revocation.

11.8 The Review Authority shall publicize that CVE compatibility has been revoked for the capability.

11.9 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.

11.10 The Review Authority may publicize the reason for revocation.

11.11 If the approval is revoked, the Owner shall not apply for a new review during the period of revocation.

12. Review Authority

For any review conducted by the Review Authority:

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

12.2 The Review Authority shall clearly identify the Review Date that was used to determine compatibility for the capability.

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

12.4 The Review Authority shall define and publish a Sample Size.

12.4.1 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.

12.4.2 The Review Authority may review every element in the capability's repository.

12.5 The Review Authority shall publicize the Sampling Method.

12.6 The Review Authority may use a Review Sample that was not randomly selected.

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

Annex 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 shall 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 shall 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 shall 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 shall 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 shall 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 shall 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 shall 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 shall 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 shall 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 shall 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/cve/CVE-YYYY-NNNN.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 shall 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 shall provide a mapping that links each element with its associated CVE name(s).

Aggregation Capability Requirements

A.5.1 The Aggregation capability shall 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 shall 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 shall 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.

Annex B: Media Requirements

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

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

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

B.3.1 The document shall 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 shall 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 shall 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 shall list the CVE name (or names) that map to that element ("CVE-Output"). Otherwise, the GUI shall 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.

Annex C: Media Requirements

The current CVE XML schema is available at: http://cve.mitre.org/schema/cve/cve_1.0.xsd

_____