

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1520

(01/2014)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Cybersecurity information exchange – Vulnerability/state
exchange

Common vulnerabilities and exposures

Recommendation ITU-T X.1520



International
Telecommunication
Union

Documents
Document Sharing Hub

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1520

Common vulnerabilities and exposures

Summary

Recommendation ITU-T X.1520 on the use of the common vulnerabilities and exposures (CVE) provides a structured means to exchange information security vulnerabilities and exposures, which provides common names for publicly known problems in the commercial or open source software used in communication networks, end-user devices or any of the other types of information and communication technology (ICT) capable of running software. The goal of the Recommendation is to define the use of CVE to make it easier to share data across separate vulnerability capabilities (tools, repositories and services) with this common naming. This Recommendation defines the use of CVE to provide a mechanism for vulnerability databases and other capabilities to be used together, and to facilitate the comparison of security tools and services. 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 repository of CVE identifiers is available at cve.mitre.org/cve/cve.html.

The intention of CVE, the use of which is defined in this Recommendation, 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.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1520	2011-04-20	17	11.1002/1000/11061
2.0	ITU-T X.1520	2014-01-24	17	11.1002/1000/12040

* To access the Recommendation, type the URL <http://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID. For example, <http://handle.itu.int/11.1002/1000/11830-en>.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2014

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope	1
2	References.....	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation.....	1
4	Abbreviations and acronyms	2
5	Conventions	2
6	High-level requirements	2
7	Accuracy	4
8	Documentation.....	4
9	CVE date usage	4
10	Different styles of CVE name support.....	5
11	Revocation of CVE compatibility	5
12	Review authority.....	6
	Annex A – Type-specific requirements	7
	Annex B – Media requirements	10
	Annex C – Media requirements	11
	Bibliography.....	14

Introduction

This Recommendation on the use of the common vulnerabilities and exposures (CVE) provides a structured means to exchange information security vulnerabilities and exposures, which provides common names for publicly known problems. The goal of this Recommendation is to define use of CVE to make it easier to share data across separate vulnerability capabilities (tools, repositories and services) with this common naming. This Recommendation is designed to allow vulnerability databases and other capabilities to be used together, and to facilitate the comparison of security tools and services. 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 repository of CVE identifiers is available at <http://cve.mitre.org/cve/cve.html>.

The intention of CVE, the use of which is defined in this Recommendation, 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.

This Recommendation 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, and includes explicit reference to the corresponding specific version maintained by the user community.

Recommendation ITU-T X.1520

Common vulnerabilities and exposures

1 Scope

This Recommendation on the use of the common vulnerabilities and exposures 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. This "structured means" is often referred to as "CVE compatibility" and defines the correct use of CVE. 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.

Recommendation ITU-T X.1520 has been developed on a collaborative basis with the MITRE Corporation, bearing in mind the importance of maintaining, to the extent possible, technical compatibility between Recommendation ITU-T X.1520 and the "Requirements and Recommendations for CVE Compatibility", 30 June 2013, available at https://cve.mitre.org/compatible/Requirements_for_CVE_Compatibility_V1.3.pdf.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 accuracy percentage: The percentage of security elements in the review sample that reference the correct CVE identifiers.

3.2.2 capability: Security tool, database, website, advisory or service that provides a security vulnerability or exposure identification function.

3.2.3 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.

3.2.4 map/mapping: The specification of relationships between security elements in a repository and the CVE names that are related to those elements.

3.2.5 owner: The custodian (real person or company) having responsibility for the capability.

3.2.6 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 website.

3.2.7 review: The process of determining whether a capability is CVE-compatible.

3.2.8 review authority: Any entity that performs a review.

NOTE – MITRE is the only review authority at this time.