

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1524

(03/2012)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Cybersecurity information exchange – Vulnerability/state
exchange

Common weakness enumeration

Recommendation ITU-T X.1524

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

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

Recommendation ITU-T X.1524

Common weakness enumeration

Summary

Recommendation ITU-T X.1524 on the use of the common weakness enumeration (CWE) provides a structured means to exchange information security weaknesses that 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 communications technology (ICT) capable of running software. The goal of CWE is to enable more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source codes and operational systems as well as better understanding and management of software weaknesses related to architecture and design. This Recommendation defines the use of CWE to provide a mechanism for software security tools, services, knowledge bases and other capabilities to be used together, and to facilitate the comparison of security tools and services. CWE also offers supportive context information about possible risks, impacts, fix information, and detailed technical information about what the software weaknesses could mean to a software system.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1524	2012-03-02	17

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 2012

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	3
6	High-level requirements	3
7	Accuracy	4
8	Effectiveness.....	5
9	Documentation.....	5
10	CWE version usage.....	5
11	Revocation of CWE compatibility	6
12	Review authority.....	7
	Annex A – Type-specific requirements	8
A.2	Tool requirements.....	8
A.3	Security service requirements.....	9
A.4	Online capability requirements.....	9
	Annex B – Media requirements	11
B.3	Electronic documents (HTML, word processor, PDF, ASCII text, etc.)	11
B.4	Graphical user interface (GUI).....	11
	Appendix I – List of CWE repositories for identifiers and the associated context information	12
	Appendix II – List of review authorities.....	13
	Bibliography.....	14

Introduction

The common weakness enumeration (CWE) Recommendation describes the use of CWE, a structured means to exchange unified, measurable sets of software weaknesses that aims to provide common names for publicly known problems. The goal of CWE is to make it easier to enable more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as to promote better understanding and management of software weaknesses related to architecture and design.

The intention of CWE is to be comprehensive with respect to the causes behind all publicly known vulnerabilities and exposures, whether from weaknesses in the software's architecture, design, code, or deployment. While CWE is designed to contain mature information, the primary focus is on identifying the weaknesses that can cause vulnerabilities and exposures. The review authority determines conformance on the use of CWE identifiers, as defined in this Recommendation.

CWE gives leverage to existing work from within the cybersecurity community such as the large number of diverse real-world vulnerabilities specified in Recommendation ITU-T X.1520 – Common vulnerabilities and exposures (CVE). Many sources and examples are leveraged to develop the specific and succinct definitions of the CWE list elements and classification tree structures. In addition, appropriate mappings are created between CWEs and CVE names so that each CWE identifier has a list of the specific CVE names that belong to that particular CWE category of software security weaknesses. In constructing the CWE list and classification tree, maximum comprehensive coverage across appropriate conceptual, business, and technical domains is sought.

This Recommendation is technically equivalent to and compatible with the "Requirements and Recommendation for CWE Compatibility and Effectiveness", version 1.0, dated July 28, 2011

https://cwe.mitre.org/compatible/requirements_v1.0.html.

Recommendation ITU-T X.1524

Common weakness enumeration

1 Scope

This Recommendation on the use of the common weakness enumeration (CWE) provides a "structured means" for the global exchange of information about software security weaknesses in architecture, design, code, or deployment that can make software systems insecure, unreliable and vulnerable to attack. Security tools, assessment services, and some types of security reviews can detect these types of software weaknesses. This "structured means" is often referred to as "CWE Compatibility" and defines the correct use of CWE. An information security weakness is a mistake in the software that could result in a vulnerability that can be used by a hacker to gain access to a system or network. The assignment of CWE identifiers is not within the scope of this Recommendation. A list of repositories for CWE identifiers and the associated context information is available in Appendix I.

The intention of CWE, the use of which is defined in this Recommendation, is to be comprehensive with respect to the software architecture, design, coding, and deployment errors that are the root causes of vulnerabilities and exposures. While CWE is designed to contain mature information, the primary focus is on identifying, educating, and describing these root causes of vulnerabilities and exposures so they can be avoided by developers, tested for, and managed by development teams as well as consistently reported by security tools and services.

This Recommendation is technically equivalent to and compatible with the "Requirements and Recommendation for CWE Compatibility and Effectiveness", version 1.0, dated July 28, 2011 <https://cwe.mitre.org/compatible/requirements.html>.

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 CWE identifiers.

3.2.2 capability: An assessment tool, Integrated Development Environment (IDE), code review tool, code checking compiler, database, website, advisory, or service that provides information about implementation, design, or architecture-level weaknesses that can lead to an exploitable security vulnerability in software.