

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1521

(03/2016)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Cybersecurity information exchange – Vulnerability/state
exchange

Common vulnerability scoring system 3.0

Recommendation ITU-T X.1521

ITU-T

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
PKI related Recommendations	X.1340–X.1349
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.1521

Common vulnerability scoring system 3.0

Summary

Recommendation ITU-T X.1521 on the common vulnerability scoring system (CVSS) provides an open framework for communicating the characteristics and impacts of information and communication technologies (ICT) vulnerabilities in the commercial or open source software used in communications networks, end user devices, or any of the other types of ICT capable of running software. The goal of the Recommendation is to enable ICT managers, vulnerability bulletin providers, security vendors, application vendors and researchers to speak from a common language of scoring ICT vulnerabilities.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1521	2011-04-20	17	11.1002/1000/11062
2.0	ITU-T X.1521	2016-03-23	17	11.1002/1000/12614

Keywords

Common vulnerability scoring system, CVSS, CYBEX, , metrics.

* 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 2016

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 About common vulnerability scoring system	3
6.1 Introduction	3
6.2 Base metrics.....	5
6.3 Temporal metrics.....	10
6.4 Environmental metrics.....	12
6.5 Qualitative severity rating scale	14
6.6 Vector string	14
6.7 CVSS v3.0 XML schema definition.....	16
6.8 CVSS v3.0 equations.....	16
Appendix I – CVSS v3.0 user guide	19
I.1 Introduction	19
I.2 Changes in CVSS v3.0	19
I.3 Scoring guide.....	23
I.4 Glossary of terms.....	25
I.5 Scoring rubric	26
Appendix II – Resources and links	29
Bibliography.....	30

Introduction

The common vulnerability scoring system (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: base, temporal, and environmental. The base group represents the intrinsic qualities of a vulnerability, the temporal group reflects the characteristics of a vulnerability that change over time, and the environmental group represents the characteristics of a vulnerability that are unique to a user's environment. The base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the temporal and environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. This Recommendation provides the official specification for CVSS v3.0.

CVSS v3.0 represents radical improvements over CVSS v2.0 and is not backward compatible with it. During the use of CVSS v2.0, several limitations of that specification came to light. Some of them are: scoring vulnerabilities in virtual environment, representing "indirect" vulnerabilities like cross site scripting, lack of ability to capture interdependencies between applications within the same system and capturing actions of a user other than attacker. More information of v3.0 improvements is given in Appendix I, clause 2.

While working to address these limitations, CVSS working group realised that it is not possible to maintain backward compatibility with the CVSS v2.0. While acknowledging that lack of compatibility will cause some issues with existing systems that use and process CVSS v2.0, it is our belief that version 3.0 brings sufficient value that would compensate for the inconvenience. We are strongly advising users and vendors that are currently producing and processing CVSS v2.0 to migrate to CVSS v3.0.

While the CVSS v2.0 specification will continue to be available for historic purposes it will cease to be in force. Implementers of tools and processes are strongly encouraged to adopt the CVSS v3.0 specification while keeping support for v2.0 in order to process existing vulnerabilities already scored with the v2.0 specification.

Recommendation ITU-T X.1521

Common vulnerability scoring system 3.0

1 Scope

This Recommendation provides a standardized approach for communicating the characteristics and impacts of ICT vulnerabilities using temporal and environmental metrics that apply contextual information to more accurately reflect the risk to each user's unique environment.

This Recommendation is technically equivalent and compatible with the "Common Vulnerability Scoring System (CVSS) version 3", 10 June 2015 which can be found at the website <http://www.first.org/cvss>

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.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 vulnerability [b-ITU-T X.1500]: Any weakness that could be exploited to violate a system or the information it contains.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 access: A subject's ability to view, modify, or communicate with an object. Access enables the flow of information between the subject and the object.

3.2.2 availability: The reliable and timely access to data and resources by authorized individuals.

3.2.3 confidentiality: A security principle that works to ensure that information is not disclosed to unauthorized subjects.

3.2.4 integrity: A security principle that makes sure that information and systems are not modified maliciously or accidentally.

3.2.5 risk: The relative impact that an exploited vulnerability would have to a user's environment.

3.2.6 threat: The likelihood or frequency of a harmful event occurring.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

A	Availability Impact
AC	Attack Complexity
AR	Availability Requirement
ARP	Address Resolution Protocol
AV	Attack Vector
C	Confidentiality Impact
CIA	Confidentiality, Integrity and Availability
CPU	Central Processing Unit
CR	Confidentiality Requirement
CVE	Common Vulnerability Exposure
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DMA	Direct Memory Access
DNS	Domain Name System
DOM	Document Object Model
DoS	Denial-of-Service
E	Exploit code maturity
I	Integrity impact
ICT	Information and Communication Technologies
ID	Identifier
IP	Internet Protocol
IR	Integrity Requirement
ISC	Impact Sub Score
IT	Information Technology
LAN	Local Area Network
MA	Modified Availability
MAC	Modified Attack Complexity
MAV	Modified Attack Vector
MC	Modified Confidentiality impact
MI	Modified Integrity
MPR	Modified Privileges Required
MS	Modified Scope
MUI	Modified User Interaction
NIST	National Institute of Standards
OS	Operating System

OSI	Open Systems Interconnection
PCI DSS	Payment Card Industry Data Security Standard
PR	Privileges Required
RC	Report Confidence
RL	Remediation Level
RPC	Remote Procedure Call
S	Scope
SCAP	Security Content Automation Protocol
SQL	Structured Query Language
TCP	Transmission Control Protocol
UI	User Interaction
USB	Universal Serial Bus
VM	Virtual Machine
XSS	Cross Site Scripting

5 Conventions

None.

6 About common vulnerability scoring system

The common vulnerability scoring system (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base group represents the intrinsic qualities of a vulnerability, the Temporal group reflects the characteristics of a vulnerability that change over time, and the Environmental group represents the characteristics of a vulnerability that are unique to a user's environment. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. This Recommendation provides the official specification for CVSS v3.0.

6.1 Introduction

Software, hardware and firmware vulnerabilities pose a critical risk to any organization operating a computer network, and can be difficult to categorize and mitigate. The common vulnerability scoring system (CVSS) provides a way to capture the principal characteristics of a vulnerability, and produce a numerical score reflecting its severity, as well as a textual representation of that score. The numerical score can then be translated into a qualitative representation (such as low, medium, high and critical) to help organizations properly assess and prioritize their vulnerability management processes.

In short, CVSS affords three important benefits. First, it provides standardized vulnerability scores. When an organization uses a common algorithm for scoring vulnerabilities across all IT platforms, it can leverage a single vulnerability management policy defining the maximum allowable time to validate and remediate a given vulnerability. Next, it provides an open framework. Users may be confused when a vulnerability is assigned an arbitrary score by a third party. With CVSS, the individual characteristics used to derive a score are transparent. Finally, CVSS enables prioritized risk. When the environmental score is computed, the vulnerability becomes contextual to each

organization, and helps provide a better understanding of the risk posed by this vulnerability to the organization.

This Recommendation describes the official CVSS v3.0 specification.

6.1.1 Metrics

CVSS is composed of three metric groups, Base, Temporal and Environmental, each consisting of a set of metrics, as shown in Figure 1.

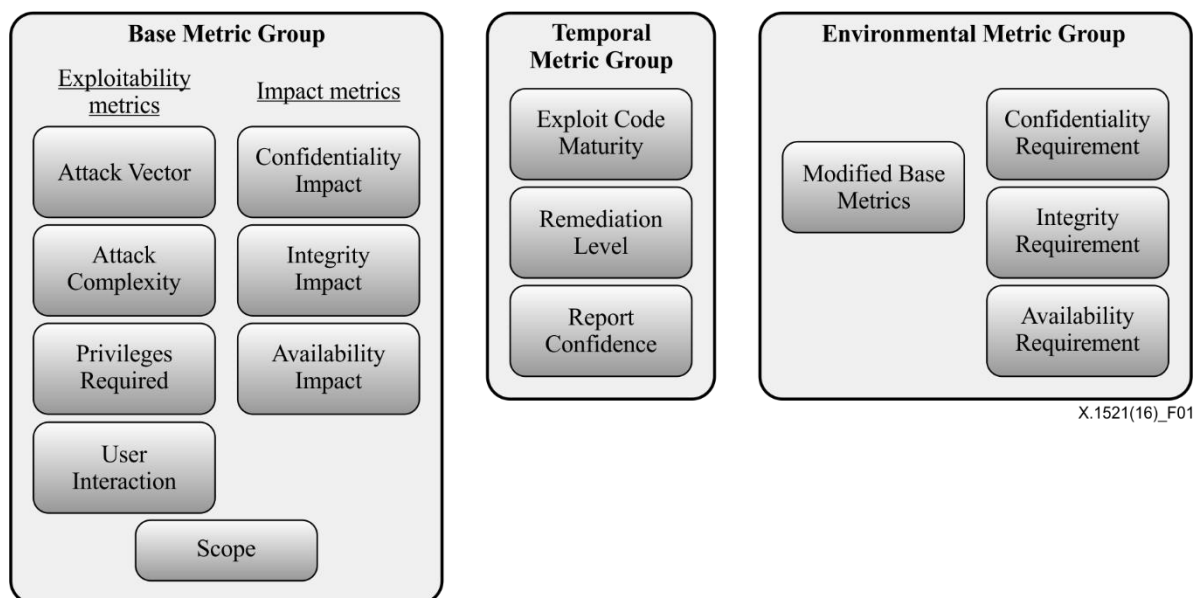


Figure 1 – CVSS v3.0 metric groups

The Base metric group represents the intrinsic characteristics of a vulnerability that are constant over time and across user environments. It is composed of two sets of metrics: the exploitability metrics and the impact metrics.

The exploitability metrics reflect the ease and technical means by which the vulnerability can be exploited. That is, they represent characteristics of the *thing that is vulnerable*, which we refer to formally as the *vulnerable component*. On the other hand, the Impact metrics reflect the direct consequence of a successful exploit, and represent the consequence to the *thing that suffers the impact*, which we refer to formally as the *impacted component*.

While the vulnerable component is typically a software application, module, driver, etc. (or possibly even a hardware device), the impacted component could be a software application, a hardware device or a network resource. This potential for measuring the impact of a vulnerability other than the vulnerable component, is a key feature of CVSS v3.0. This property is captured and further discussed by the Scope metric below.

The Temporal metric group reflects the characteristics of a vulnerability that may change over time but not across user environments. For example, the presence of a simple-to-use exploit kit would increase the CVSS score, while the creation of an official patch would decrease it.

The Environmental metric group represents the characteristics of a vulnerability that are relevant and unique to a particular user's environment. These metrics allow the scoring analyst to incorporate security controls which may mitigate any consequences, as well as promote or demote the importance of a vulnerable system according to her business risk.

Each of these metrics are discussed in further detail below.

6.1.2 Scoring

When the Base metrics are assigned values by an analyst, the base equation computes a score ranging from 0.0 to 10.0 as illustrated in Figure 2.

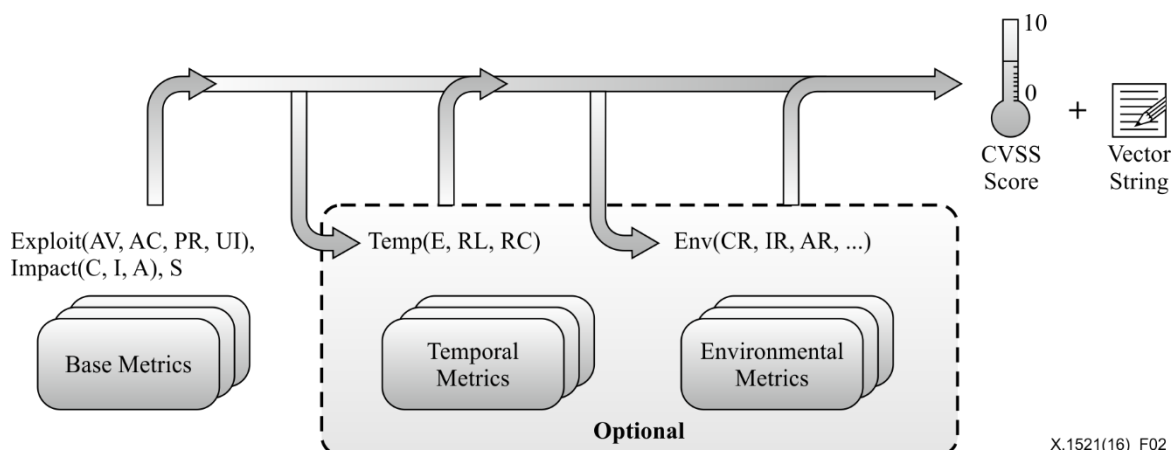


Figure 2 – CVSS metrics and equations

Specifically, the base equation is derived from two sub equations: the exploitability sub score equation, and the impact sub score equation. The exploitability sub score equation is derived from the base exploitability metrics, while the impact sub score equation is derived from the base impact metrics.

The Base score can then be refined by scoring the temporal and environmental metrics in order to more accurately reflect the risk posed by a vulnerability to a user's environment. However, scoring the temporal and environmental metrics is not required.

Generally, the Base and Temporal metrics are specified by vulnerability bulletin analysts, security product vendors, or application vendors because they typically possess the most accurate information about the characteristics of a vulnerability. On the other hand, the Environmental metrics are specified by end-user organizations because they are best able to assess the potential impact of a vulnerability within their own computing environment.

Scoring CVSS metrics also produces a vector string, a textual representation of the metric values used to score the vulnerability. This vector string is a specifically formatted text string that contains each value assigned to each metric, and should always be displayed with the vulnerability score.

The scoring equations and vector string are explained further below.

Note that all metrics should be scored under the assumption that the attacker has already located and identified the vulnerability. That is, the analyst need not consider the means by which the vulnerability was identified. In addition, it is likely that many different types of individuals will be scoring vulnerabilities (e.g., software vendors, vulnerability bulletin analysts, security product vendors, etc.), however, note that vulnerability scoring is intended to be agnostic to the individual and their organization.

6.2 Base metrics

6.2.1 Exploitability metrics

As mentioned, the exploitability metrics reflect the characteristics of the *thing* that is vulnerable, which we refer to formally as the *vulnerable component*. Therefore, each of the exploitability metrics listed below should be scored relative to the vulnerable component, and reflect the properties of the vulnerability that lead to a successful attack.

6.2.1.1 Attack vector (AV)

This metric reflects the context by which vulnerability exploitation is possible. This metric value (and consequently the Base score) will be greater the more remote an attacker is (in terms of logical and physical distance) in order to exploit the vulnerable component. The assumption is that the number of potential attackers for a vulnerability that could be exploited from across the Internet is larger than the number of potential attackers that could exploit a vulnerability requiring physical access to a device, and therefore warrants a greater score. The list of possible values is presented in Table 1.

Table 1 – Attack vector

Metric value	Description
Network (N)	A vulnerability exploitable with network access means the vulnerable component is bound to the network stack and the attacker's path is through open systems interconnection (OSI) layer 3 (the network layer). Such a vulnerability is often termed "remotely exploitable" and can be thought of as an attack being exploitable one or more network hops away (e.g., across layer 3 boundaries from routers). An example of a network attack is an attacker causing a denial-of-service (DoS) by sending a specially crafted transmission control protocol (TCP) packet from across the public Internet (e.g., CVE-2004-0230).
Adjacent (A)	A vulnerability exploitable with adjacent network access means the vulnerable component is bound to the network stack, however the attack is limited to the same shared physical (e.g., Bluetooth, IEEE 802.11), or logical (e.g., local Internet protocol (IP) subnet) network, and cannot be performed across an OSI layer 3 boundary (e.g., a router). An example of an adjacent attack would be an address resolution protocol (ARP) (IPv4) or neighbour discovery (IPv6) flood leading to a denial of service on the local area network (LAN) segment. See also CVE-2013-6014.
Local (L)	A vulnerability exploitable with local access means that the vulnerable component is not bound to the network stack, and the attacker's path is via read/write/execute capabilities. In some cases, the attacker may be logged in locally in order to exploit the vulnerability, otherwise, he or she may rely on user interaction (UI) to execute a malicious file.
Physical (P)	A vulnerability exploitable with physical access requires the attacker to physically touch or manipulate the vulnerable component. Physical interaction may be brief (e.g., evil maid attack ¹) or persistent. An example of such an attack is a cold boot attack which allows an attacker access to disk encryption keys after gaining physical access to the system, or peripheral attacks such as Firewire/universal serial bus (USB) direct memory access attacks.

6.2.1.2 Attack complexity (AC)

This metric describes the conditions beyond the attacker's control that must exist in order to exploit the vulnerability. As described below, such conditions may require the collection of more information about the target, the presence of certain system configuration settings, or computational exceptions. Importantly, the assessment of this metric excludes any requirements for user interaction in order to exploit the vulnerability (such conditions are captured in the User interaction metric). This metric value is largest for the least complex attacks. The list of possible values is presented in Table 2.

¹ See https://www.schneier.com/blog/archives/2009/10/evil_maid_attac.html for a description of the evil maid attack.