International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1526

(04/2013)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cybersecurity information exchange – Vulnerability/state exchange

# Open Vulnerability and Assessment Language

Recommendation ITU-T X.1526

International Telecommunication Union

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.1526

## Open Vulnerability and Assessment Language


**Summary**

In Recommendation ITU-T X.1526 the Open Vulnerability and Assessment Language (OVAL) standardizes the three main steps of the assessment process: representing configuration information of systems for testing; analysing the system for the presence of the specified machine state (vulnerability, configuration, patch state, etc.) and reporting the results of this assessment. The purpose of OVAL is to provide an international, information security, community standard to promote open and publicly available security content and to standardize the transfer of this information across the entire spectrum of security tools and services. OVAL is a language used to encode system details, and an assortment of content repositories held throughout the community.



**History**

| Edition | Recommendation | Approval | Study Group |
|---|---|---|---|
| 1.0 | ITU-T X.1526 | 2013-04-26 | 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/.

## Table of Contents

## Introduction

Recommendation ITU-T X.1526 describes the use of the Open Vulnerability and Assessment Language (OVAL), an international, information security, community standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services. OVAL includes a language used to encode system details, and an assortment of content repositories held throughout the community. The language standardizes the three main steps of the assessment process: representing configuration information of systems for testing; analysing the system for the presence of the specified machine state (vulnerability, configuration, patch state, etc.); and reporting the results of this assessment. The repositories are collections of publicly available and open content that utilize the language.

The OVAL community has developed three schemas written in Extensible Markup Language (XML) to serve as the framework and vocabulary of the OVAL language. These schemas correspond to the three steps of the assessment process: an OVAL System Characteristics schema for representing system information, an OVAL Definition schema for expressing a specific machine state, and an OVAL Results schema for reporting the results of an assessment.

Content written in the OVAL Language is located in one of the many repositories found within the community. One such repository is known as the OVAL repository. It is the central meeting place for the OVAL community to discuss, analyse, store, and disseminate OVAL definitions. Each definition in the OVAL repository determines whether a specified software vulnerability, configuration issue, program, or patch is present on a system.

The information security community contributes to the development of OVAL by participating in the creation of the OVAL Language on the OVAL developer's forum and by writing definitions for the OVAL repository through the OVAL community forum. An OVAL board consisting of representatives from a broad spectrum of industry, academia, and government organizations from around the world, oversees and approves the OVAL Language and monitors the posting of the definitions hosted on the OVAL website. This means that OVAL reflects the insights and combined expertise of the broadest possible collection of security and system administration professionals worldwide. Recommendation ITU-T X.1526 has been developed bearing in mind the importance of maintaining, to the extent possible, technical compatibility between Recommendation ITU-T X.1526 and the "Requirements and Recommendation for OVAL Adoption and Use", version 1.0, dated 20 January 2011, and published by the MITRE Corporation, [https://oval.mitre.org/adoption/requirements_v1.0.html].

# Recommendation ITU-T X.1526

## Open Vulnerability and Assessment Language

### 1 Scope

Recommendation ITU-T X.1526 provides a structured means for the global exchange of publicly available security content and for the standardization of the transfer of this information across the entire spectrum of security tools and services. The Open Vulnerability and Assessment Language (OVAL) includes a language used to encode system details, and an assortment of content repositories held throughout the community.

### 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.

[ISO/IEC 19757-3] ISO/IEC 19757-3:2006, *Information technology – Document Schema Definition Language (DSDL) – Part 3: Rule-based validation – Schematron*.

### 3 Definitions

#### 3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

**3.1.1 review authority** [b-ITU-T X.1520]: Any entity that performs a review.

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

**3.1.2 user** [b-ITU-T X.1520]: A consumer or potential consumer of the capability.

#### 3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

**3.2.1 authoring tool**: A product that aids in the process of creating new OVAL files (including products that consolidate existing OVAL definitions into a single file).

**3.2.2 capability**: A specific function or functions of a product, service, or repository.

**3.2.3 correctness testing**: The process of determining whether a product, service, or repository has correctly adopted OVAL.

**3.2.4 definition evaluator**: A product that uses an OVAL Definition to guide evaluation and produces OVAL Results (full results) as output.

**3.2.5 definition repository**: A repository of OVAL definitions made available to the community (free or pay).

**3.2.6 owner** (based on the definition given in [b-ITU-T X.1520]): The custodian (real person or company) having responsibility for the capability (as defined in this Recommendation).

**3.2.7 product**: A security application, appliance, or security database that has one or more capabilities.

**3.2.8 repository** (based on the definition given in [b-ITU-T X.1520]): An implicit or explicit collection of security elements that supports a capability (as defined in this Recommendation), e.g., a vulnerability database, advisory archive, the set of signatures in an intrusion detection system (IDS), or website.

**3.2.9 results consumer**: A product that accepts OVAL results as input and either displays those results to the user, or uses the results to perform some action (remediation, security information management (SIM), etc.).

**3.2.10 system characteristics producer**: A product that generates a valid OVAL system characteristics document based on the details of a system.

**3.2.11 test results**: Data representing the outcome of correctness testing.

## 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CCE Common Configuration Enumeration

CPE Common Platform Enumeration

CVE Common Vulnerabilities and Exposures

OVAL Open Vulnerability and Assessment Language

SIM Security Information Management

XML Extensible Markup Language

## 5 Conventions

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

## 6 High-level requirements

The following items define the concepts, roles, and responsibilities related to the five different capabilities, each targeting a different usage of the OVAL Language, that comprise the proper use of the OVAL Language. These capabilities enable members of the OVAL community to easily understand how a given product is using the OVAL Language and how it might suit their needs.

The following requirements apply to all capabilities that are implementing support for OVAL, regardless of the capability that they plan to implement. If the product, service, or repository satisfies all applicable requirements, then the capability owner will receive formal acknowledgement of correctly adopting OVAL.

### Prerequisites

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

**6.2** The capability owner shall agree to abide by all of the mandatory OVAL adoption requirements, which include the mandatory requirements for the specific capability.

**6.3** The capability owner shall provide the review authority with a technical point of contact that is qualified to answer questions regarding any OVAL-related functionality of the product, service, or repository and coordinate the preparation of the product, service, or repository for correctness testing.

**6.4** The capability owner shall provide the review authority with a completed "OVAL Adoption Questionnaire Form". This form will be sent once the declaration process has been satisfied. For

more information, see the section "How to Declare Your Product, Service, or Repository as an OVAL Adopter" at http://oval.mitre.org/adoption/requirements.html.

**6.5** The capability owner shall provide the review authority with free access to items needed to perform correctness testing, including the test results and/or the repository, in order to determine compliance with all associated requirements.

**6.6** The capability owner shall work with the review authority to make the product, service, or repository available for correctness testing.

**6.7** As a part of receiving formal acknowledgement of correctly adopting OVAL, the capability owner shall agree to support the review authority in follow-on testing activities, where appropriate types of files will be exchanged with other organizations attempting to prove the correctness of their product, service, or repository. This will be managed by the review authority and kept to reasonable levels of effort for all involved.

**6.8** The product shall provide additional value or information beyond that which is provided in OVAL itself. Therefore, forwarding or providing references to a single source of OVAL definitions that have been created by someone else is not by itself considered to be sufficient for formal acknowledgement of correctly adopting OVAL.

**6.9** The product, service, or repository shall be available to the public or a set of consumers.

**6.10** The product, service, or repository shall clearly state the schema(s) and version with which it is compatible.

**Miscellaneous**

**6.11** If the capability does not satisfy all of the applicable requirements above (clauses 6.1 through 6.10), then the capability owner shall not advertise that it is an OVAL adopter.

## 7 Correctness

OVAL adoption only facilitates interoperability if the capability's use of OVAL is correct. Therefore, OVAL adopter capabilities have to meet the minimum correctness requirements described below.

**7.1** The capability owner shall have in place a means for the user to submit correctness errors found in the use of OVAL and in any OVAL content being produced by the product, service, or repository.

**7.2** The capability owner shall have a plan in place to address any correctness errors reported to it.

**7.3** The capability owner shall address any correctness errors reported to it within a reasonable time-frame following initial reporting of the error.

## 8 Documentation

The following requirements apply to documentation that is provided with an OVAL adopter's product, service, or repository.

**8.1** The product shall include in its documentation a brief description of OVAL and OVAL adoption, which can include verbatim portions of documents from the OVAL website.

**8.2** The product shall clearly state in its documentation any component schemas or individual tests that it does not support. For example, if a product is applying for formal acknowledgement of correctly adopting OVAL as a Definition Evaluator and does not support a specific commercial product's feature test, then the product, service, or repository documentation shall state this incompatibility.

**8.3** The product, service, or repository shall clearly state in its documentation the procedure that a user must follow to submit correctness errors found in any OVAL content being produced by the product.

**8.4** If the documentation included with the product, service, or repository includes an index, then it shall include references to OVAL-related documentation under the term "OVAL".

## 9 Validity

OVAL adopters are required to work with valid documents. This helps to ensure that information is being formatted correctly and that the structure of the document follows the OVAL Language.

**9.1** The product, service, or repository shall validate all OVAL content (both produced and consumed) using W3C XML schema validation against the version of the OVAL Language with which it is stated to comply.

**9.2** The product, service, or repository shall report any W3C XML schema validation errors to the user.

**9.3** The product, service, or repository shall validate all OVAL content (both produced and consumed) using Schematron [ISO/IEC 19757-3] validation against the version of the OVAL Language with which it is stated to comply.

**9.4** The product, service, or repository shall report any Schematron validation errors to the user.

## 10 Specific capability requirements

The following requirements are related to the specific adoption capabilities and only apply to products, services, or repositories that are looking to gain formal acknowledgement of correctly adopting OVAL for that specific capability.

### System characteristics producer

These requirements apply to all products or services that intend to generate information about a specific machine in the OVAL system characteristics schema format.

**10.1** The product or service shall use a unique item ID (unique on a per file basis) for each specific system characteristic item it collects.

**10.2** The product or service shall generate system characteristics items that contain the exact system configuration values gathered at the time the product or service is executed against the system.

**10.3** The product or service that uses an OVAL Definition document to generate system characteristics items shall include a collected_objects section, with a system characteristics object for each object collected in the input OVAL Definition document.

### Definition repository

These requirements apply to all repositories that intend to provide a collection of information in the OVAL definition schema format.

**10.4** All OVAL Definitions, Tests, Objects, States, and Variables shall contain a unique ID with respect to all other OVAL Definitions, Tests, Objects, States, and Variables in the OVAL community.

**10.5** Each repository should use its own unique constant namespace portion of the ID across all OVAL content.

**10.6** Each OVAL Definition, Test, Object, State, and Variable shall keep the same ID across its existence. This enables users to reference these items based on the stable ID. An existing item should not be rewritten for any other purpose as users may be referencing the item in their own content.

**10.7** Each update or modification of an OVAL Definition, Test, Object, State, or Variable in the repository shall result in the item's version being incremented. Similarly, each item that references the updated or modified item shall also have its version incremented. This cascading of version updates up to referencing items does not need to extend beyond referencing OVAL definitions since OVAL definitions provide a logical unit.

**10.8** The OVAL Definition metadata shall be consistent with the OVAL Definition content (e.g., the affected family should not be 'platform A' if the tests are examining 'platform white'). Additionally, the metadata shall reflect all of the OVAL Definition's content, which means that the metadata may need to have sections for each affected family when an OVAL Definition applies to more than one family.

**10.9** A repository that contains an OVAL Definition to cover a specific vulnerability shall include, when available, a common vulnerabilities and exposures (CVE) name as a reference.

**10.10** A repository that contains an OVAL Definition to check for a specific configuration state shall include, when available, a common configuration enumeration (CCE) ID as a reference.

**10.11** A repository that contains an OVAL Definition to check for a specific platform shall include, when available, a common platform enumeration (CPE) name as a reference.

**10.12** The capability owner shall document the process by which a user can retrieve content updates.

**Authoring tool**

These requirements apply to all products or services that are designed to help facilitate the creation or modification of OVAL content.

**10.13** An authoring tool shall provide a search interface to allow the user to search for OVAL Definitions, Tests, Objects, States, and Variables by ID.

**10.14** An authoring tool should encourage the reuse of existing OVAL Definitions, Tests, Objects, States, and Variables.

**10.15** An authoring tool should allow the user to invoke validation on a document that is written for the OVAL Language and report all W3C XML schema and Schematron errors to the user.

**10.16** An authoring tool shall allow the user to import and edit existing OVAL content.

**10.17** An authoring tool shall allow the user to export the content, created by the tool, as valid OVAL Language documents.

**10.18** An authoring tool should report duplicate content to the user.

**10.19** An authoring tool shall provide value and capability above and beyond the capability of an XML editor.

**Definition evaluator**

These requirements apply to all products or services that intend to evaluate a specified system using, as input, information provided in the OVAL Definition schema format. Once evaluation has been performed, the results must be available in the OVAL results schema format.

**10.20** The user shall be able to determine which OVAL definitions are being evaluated.

**10.21** The user shall be able to examine the details of each OVAL Definition being evaluated. This requirement ensures that the OVAL definitions are open to the user allowing them to see how a specific issue is being tested.

**10.22** If the product or service does not consume OVAL definitions at runtime, the capability owner shall document the process by which a user can submit OVAL definitions to the capability owner for interpretation by the product. This includes stating how quickly definitions submitted to the capability owner are made available to the product.

**10.23** The product or service shall be capable of interpreting all of the logic within each OVAL Definition and subsequent OVAL tests in accordance with the stated logical operators.

**10.24** The product or service shall determine the result of evaluating the target system based on the details specified in the OVAL Definition.

**10.25** The user shall be able to determine the result of all OVAL definitions used in the evaluation of the target system.

**10.26** The product or service shall generate accurate, predictable, and repeatable results when using a specific set of OVAL definitions and system state information.

**10.27** The results generated by the product or service shall be available in the full OVAL Results format. This allows other products or services that want to leverage detailed evaluation information, to obtain the information as desired. Thin results may be available as well, but full results are required.

**10.28** When an OVAL Definition has been evaluated more than once on a single system, each time with different values for the variables, the OVAL results file shall include unique variable instance values for each individual case.

**10.29** A product or service shall use a result of "not evaluated" for all OVAL definitions that are part of the original OVAL Definition file, but are not being reported on. This satisfies requirement 10.25 for the given OVAL Definition.

**10.30** Any use or translation of an OVAL Definition into the internal language of the product or service shall reflect the same logic as the original OVAL Definition.

**Results consumer**

These requirements apply to all products or services that intend to consume information in the OVAL results schema format.

**10.31** For each system defined in the OVAL result file being consumed, the user shall be able to determine the specific OVAL definitions that are being reported on.

**10.32** The user shall be able to examine the details of the OVAL results file being consumed. This can be as simple as allowing the user to open the XML file. The point of this requirement is to make sure that the OVAL results used are open to the user allowing them to examine the data being reported.

**10.33** If the product or service does not consume OVAL results files at runtime, the owner shall document the process by which a user can submit OVAL results files to the capability owner for interpretation by the product or service. This includes stating how quickly files submitted to the capability owner are made available to the product or service.

## 11 Review authority requirements

The following are requirements pertaining to OVAL adoption that the review authority must adhere to.

**11.1** The review authority shall clearly identify the version of the adoption, the version of the requirements document, and the version of the OVAL Language that was used to determine formal adherence to the OVAL adoption requirements for each product, service, or repository.

**11.2** The review authority shall define and publish sample test materials.

**11.3** The review authority shall publicize information on how to participate in correctness testing so that organizations can prepare as much in advance as possible.

**11.4** The review authority shall provide a point of contact for arranging correctness testing for capabilities declaring support for OVAL that have completed the "OVAL Adoption Questionnaire Form".

**11.5** The review authority may re-test a product, service, or repository that has been formally acknowledged for adopting OVAL at the discretion of the review authority.

**11.6** The review authority must provide a copy of the OVAL Adoption Declaration Form upon request from any valid capability owner wishing to start the OVAL adoption process.

**11.7** The review authority must provide a copy of the OVAL Adoption Questionnaire Form upon request from any capability owner that has submitted a completed OVAL Adoption Declaration Form.

## 12 Revocation

If the review authority has verified that a product, service, or repository has correctly adopted OVAL, but at a later time the review authority has evidence that the requirements are no longer being met, then the review authority may revoke its approval and the product, service, or repository will no longer be formally acknowledged as correctly adopting OVAL. The following are the requirements that the review authority must follow in order to revoke the acknowledgement.

**12.1** The review authority shall provide the capability owner with a warning of revocation at least two (2) months before revocation is scheduled to occur.

**12.2** The review authority may delay the date of revocation.

**12.3** If the review authority has found that the actions or claims of the capability owner are intentionally misleading, then the review authority may skip the warning period. The review authority may interpret the phrase "intentionally misleading" as it wishes.

**12.4** If the review authority finds that the actions of the capability owner with respect to the adoption requirements are intentionally misleading, then revocation shall last a minimum of one year.

**12.5** The review authority shall identify the specific requirements that are not being met.

**12.6** If the capability owner believes that the requirements are being met, then the capability owner shall respond to the warning of revocation by providing specific details that indicate why the product, service, or repository meets the requirements under question.

**12.7** If the owner modifies the product, service, or repository so that it complies with the requirements in question, during the warning period, then the review authority should end the revocation action for the product, service, or repository.

**12.8** The review authority shall publicize that the formal acknowledgement of the correct adoption of OVAL has been revoked for the product, service, or repository.

**12.9** The review authority may publicize the reason for revocation.

# Bibliography

[b-ITU-T X.1520] Recommendation ITU-T X.1520 (2011), *Common vulnerabilities and exposures.*

## SERIES OF ITU-T RECOMMENDATIONS

| | |
|---|---|
| Series A | Organization of the work of ITU-T |
| Series D | General tariff principles |
| Series E | Overall network operation, telephone service, service operation and human factors |
| Series F | Non-telephone telecommunication services |
| Series G | Transmission systems and media, digital systems and networks |
| Series H | Audiovisual and multimedia systems |
| Series I | Integrated services digital network |
| Series J | Cable networks and transmission of television, sound programme and other multimedia signals |
| Series K | Protection against interference |
| Series L | Construction, installation and protection of cables and other elements of outside plant |
| Series M | Telecommunication management, including TMN and network maintenance |
| Series N | Maintenance: international sound programme and television transmission circuits |
| Series O | Specifications of measuring equipment |
| Series P | Terminals and subjective and objective assessment methods |
| Series Q | Switching and signalling |
| Series R | Telegraph transmission |
| Series S | Telegraph services terminal equipment |
| Series T | Terminals for telematic services |
| Series U | Telegraph switching |
| Series V | Data communication over the telephone network |
| **Series X** | **Data networks, open system communications and security** |
| Series Y | Global information infrastructure, Internet protocol aspects and next-generation networks |
| Series Z | Languages and general software aspects for telecommunication systems |

Printed in Switzerland
Geneva, 2013