国 际 电 信 联 盟

ITU-T X.1526

(04/2013)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

网络安全信息交换 – 脆弱性/状态信息交换

开放漏洞和评估语言

ITU-T X.1526 建议书

国际电信联盟

ITU-T X 系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
报文处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定安全	X.1080–X.1099
安全应用和服务	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
计算网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1339
网络安全信息交换	
网络安全概述	X.1500–X.1519
脆弱性/状态信息交换	**X.1520–X.1539**
事件/事故/探索法信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
探索法和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589

欲了解更详细信息，请查阅 ITU-T建议书目录。

ITU-T X.1526 建议书

开放漏洞和评估语言

摘要

ITU-T X.1526 建议书--开放漏洞和评估语言（OVAL），标准化了评估过程中的三个主要步骤：表示用于测试的系统配置信息；分析系统存在的特定机器状态(脆弱性、配置、补丁状态等)；以及报告评估的结果。OVAL的目标是提供一个国际化的，信息安全领域的社区标准来促进开放和公布可行的安全内容，同时规范这些信息内容在整个安全工具和服务范围的传输。OVAL包括用于对系统细节进行编码的语言，以及整个社区持有的各类内容资料库。

沿革

版本	建议书	批准日期	研究组
1.0	ITU-T X.1526	2013-04-26	17

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

引言

有关开放漏洞和评估语言（OVAL）使用的ITU-T X.1526 建议书描述了一项促进公开提供安全内容的国际化、信息安全领域的社区标准，同时规范了这些信息内容在整个安全工具和服务范围的传递。OVAL包括用于对系统细节进行编码的语言，以及整个社区持有的各类内容资料库。该语言标准化了评估过程的三个主要步骤：表示用于测试系统的配置信息；分析系统存在的特定机器状态（脆弱性、配置、补丁状态等）；以及报告评估的结果。资料库是使用OVAL语言的一系列公开和开放的内容。

OVAL社区已经用可扩展标记语言（XML）开发出三种方案，作为OVAL语言的框架和词汇组成。这些方案对应于评估过程中的三个步骤：描述系统信息的OVAL系统特征方案，表达特定机器状态的OVAL定义方案和报告评估结果的OVAL结果方案。

使用OVAL语言编写的内容位于社区内的众多资料库之一。其中一个资料库称之为OVAL资料库。它是OVAL社区讨论、分析、存储和传播OVAL定义的集中会晤地点。OVAL资料库的每个定义确定了指定的软件是否有漏洞、配置问题、系统程序或补丁。

信息安全领域人士通过参与OVAL开发人员论坛的OVAL语言创建和通过在OVAL社区论坛为OVAL资料库书写定义，为OVAL的发展做出相应贡献。OVAL委员会由来自世界各地的工业界、学术界和政府组织代表组成，它负责批准OVAL语言以及监管OVAL网站托管的定义的发布。这意味着，OVAL反映了世界范围内最为广泛的安全和系统管理专业人士的真知灼见和专业技术知识。起草ITU-T X.1526建议书在最大程度上考虑到了保持该建议书与2011年1月20日由MITRE出版的《OVAL采纳与使用的要求和建议》间技术兼容的重要性。[https://oval.mitre.org/adoption/requirements_v1.0.html]

ITU-T X.1526 建议书

开放漏洞和评估语言

1 范围

ITU-T X.1526建议书提供了一种结构化的方法用于全球交换公共的可行的安全性内容，并规范这些信息内容在整个安全工具和服务范围的传递。OVAL包括用于对系统细节进行编码的语言，以及整个社区持有的各类内容资料库。

2 参考文献

以下ITU-T建议书和其他参考文献所包含的规定，通过本文件的引用，构成本建议书的规定。在本标准出版时，标明的版本是有效的。所有的建议书和其他参考文献都会被修订；因此本建议书的用户被鼓励探讨采用最新版本的建议书和下面列出的其他参考文献的可能性。当前有效的ITU-T建议书列表将会定期公布。引用本建议书的文件未给出，因为本建议书是一份独立的文件。

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

3 定义

3.1 其它地方定义的术语

本建议书采用了其它文献中定义的以下术语：

3.1.1 审查机构[b-ITU-T X.1520]：实施审查的任何机构。

注 – MITRE 是目前唯一的审查机构。

3.1.2 用户[b-ITU-T X.1520]：具有该功能的消费者或潜在消费者。

3.2 本建议书中定义的术语

本建议书中定义了如下术语：

3.2.1 创建工具：帮助新 OVAL 文件创建过程的产品（包括整合现有 OVAL 定义至一个文件的产品）。

3.2.2 能力：产品、服务或资料库的功能集合或特定功能。

3.2.3 正确性测试：确定产品、服务或资料库是否正确采用 OVAL 的过程。

3.2.4 定义评估器：产品采用 OVAL 定义来指导评估和产生 OVAL 输出结果（全部结果）。

3.2.5 定义资料库：OVAL定义资料库，用于提供给社区（免费或付费）。

3.2.6 所有者（基于[b-ITU-T X.1520]中给出的定义）：负责能力（见本建议书中的定义）的监护人（实际的人或企业）。

3.2.7 产品：有一种或多种能力的安全应用程序、设备或安全数据库。

3.2.8 **数据库**（基于[b-ITU-T X.1520]中给出的定义）：支持某项能力（如本建议书中的定义）的明示或暗示安全要素集合，例如，漏洞数据库、报告、入侵检测系统（IDS）中的系列签名或网站。

3.2.9 **结果用户：**产品接受OVAL结果作为输入，要么显示这些结果给用户，要么使用这些结果来执行某些操作（纠正，SIM等）。

3.2.10 **系统特征生成者：**基于系统的细节，生成一个有效的OVAL系统特征文件的产品。

3.2.11 **测试结果：**表示正确性测试结果的数据。

4 缩略语和首字母缩写

本建议书使用下述缩略语和首字母缩写：

CCE 通用配置枚举

CPE 通用平台枚举

CVE 通用漏洞和披露

OVAL 开放漏洞和评估语言

SIM 安全信息管理

XML 可扩展标记语言

5 惯例

本建议书中的关键词“需”、“须”、“不得”、“应”、“不应”、“建议”、“可以”和“可选”按照《ITU-T作者指南》进行解释。

6 高层要求

以下条目定义了五种不同能力相关的概念、角色和责任，每个定义都指向OVAL语言的不同用途，从而构成如何恰当使用OVAL语言。这些能力使得OVAL社区成员能够很容易理解一个给定的产品如何使用OVAL语言以及它如何满足他们的需求。

以下要求适用于所有正在实施的支持OVAL的能力，以及将要实施的能力。如果产品、服务、或资料库符合所有适当的要求，能力所有者将会收到正确使用OVAL的正式认证。

前提

6.1 能力所有者应当是有效的法律实体，例如一个组织或一个特定的个体，拥有一个有效的电话号码、电子邮件地址和街道邮箱地址。

6.2 能力所有者应该同意遵守所有的OVAL使用的强制性要求，其中包括特定能力的强制性要求。

6.3 能力所有者应提供与审查机关沟通的技术联络点，其具有资格回答任何OVAL相关的产品、服务或资料库功能的问题，并协调产品准备、服务或资料库的正确性测试。

6.4 能力所有者须提供一份完整的“OVAL使用问卷调查表”给审查机构。该问卷一旦满足声明过程就会被发送。请参阅“如何声明你的产品、服务或资料库是OVAL的使用者”部分（见http://oval.mitre.org/adoption/requirements.html）以获取更多信息。

6.5 能力所有者应该为审查机构提供项目的自由获取权限以便执行正确性测试，包括测试结果和/或资料库等，以确定是否符合相关组织的要求。

6.6 能力所有者应该与审查机构合作，以确保产品、服务或资料库可供执行正确性测试使用。

6.7 作为接收到正确使用OVAL的正式认可的一部分，能力所有者应同意支持审查机构的后续测试活动，同时将与尝试证明其产品、服务或资料库正确性的其他组织交换适当类型的文件。这将由审查机构进行管理，并将所有参与者的努力保持在一个合理的等级上。

6.8 产品应提供超出OVAL自身的价值或信息。因此，为其他人创建的单一来源的OVAL定义提供或转发参考，尚不足以作为正确使用OVAL的正式认证。

6.9 产品、服务或资料库应该能够提供给公众或消费者。

6.10 产品、服务或资料库应该清晰地注明方案和它们兼容的版本。

杂项

6.11 如果能力不能满足上述的所有适用要求（6.1至6.10），则能力所有者不得声明它是OVAL使用者。

7 正确性

如果能力所有者使用OVAL是正确的，其仅仅有利于互操作性。因此，OVAL使用者的能力必须满足下述的最低正确性要求。

7.1 能力所有者应该具有一种方法，使得用户能够提交在OVAL使用过程中，以及产品、服务或资料库正在产生的OVAL内容中发现的关于正确性的错误。

7.2 能力所有者须制定计划处理任何关于正确性的错误报告。

7.3 正确性的错误被报告后，能力所有者须在一个合理的时间间隔内处理它们。

8 文件

以下要求适用于OVAL使用者的产品、服务或资料库的相关文件。

8.1 产品应在其文档中包括一个OVAL和OVAL使用的简短描述，其中可以包括来自OVAL网站文件的完整部分。

8.2 产品须在其文档中清晰罗列组件的方案或不支持的单个测试。例如，如果某产品申请获得作为“定义评估器”正确使用OVAL的正式认证且不支持特定商用产品功能测试，则在产品、服务或资料库的文件中须说明这些不兼容。

8.3 产品、服务或资料库应该在其文件中清晰说明过程，即用户提交产品中关于OVAL内容的正确性相关错误时须遵守的步骤。

8.4 如果产品、服务或资料库包含的文件包括一个索引，那么它应该包括术语“OVAL”下的OVAL相关文档的引用。

9 合法性

OVAL使用者要求使用合法的文件。这将有助于确保信息被正确格式化，且文件的结构遵守OVAL语言。

9.1 产品、服务或资料库须验证所有的OVAL内容(包括生产和使用)，对于其声明遵守的OVAL语言版本使用W3C XML方案进行验证。

9.2 产品、服务或资料库应向用户报告任何W3C XML方案验证的错误。

9.3 产品、服务或资料库应验证所有的OVAL内容(包括生产和使用)，对于其声明遵守的OVAL语言版本使用Schematron [ISO/IEC 19757-3]进行验证。

9.4 产品、服务或资料库须向用户报告所有Schematron验证错误。

10 特定能力的要求

以下是特定应用能力的相关要求，并只适用于希望获得正确使用OVAL的正式认证的产品、服务或资料库的特定能力。

系统特征生成者

这些要求适用于所有的使用OVAL系统特征方案格式生成特殊设备信息的产品或服务。

10.1 产品或服务须为每个收集的特定系统特征的条目使用一个唯一的条目ID（每份文件保持唯一）。

10.2 产品或服务须生成系统的特征条目，其包含产品或服务在系统执行时收集的精确系统配置参数。

10.3 产品或服务使用OVAL定义文件来生成系统特征条目，须包括一个collected_objects小节，其中输入OVAL定义文件中所收集的对象内应包含系统特征对象。

定义资料库

这些要求适用于所有的资料库，用于提供使用OVAL定义方案格式的信息的收集。

10.4 所有的OVAL定义、测试集、对象、状态和变量应包含一个唯一的ID，与OVAL社区的所有其他OVAL定义、测试集、对象、状态和变量对应。

10.5 每个资料库的部分ID应该在所有的OVAL上下文中使用它唯一的常量命名空间。

10.6 每个OVAL定义、测试集、对象、状态和变量须在其生命周期内保持同一ID。这使得用户可以基于稳定的ID参考这些条目。现有的项目不应该被改写用于其他目的，例如用户可能会在他们自己的内容中引用该项目。

10.7 每次资料库内的OVAL定义、测试集、对象、状态或变量的更新或修改须导致该条目的版本增加。同样地，每个引用更新或修改条目也应增加其版本。这种引用条目的级联式版本更新并不需要扩展超出引用的OVAL定义，因为OVAL定义提供了一个逻辑单元。

10.8 OVAL定义的元数据应该符合OVAL定义的内容（例如，假如测试正在检查‘白平台’，受影响的家庭不应该是‘平台A’）。另外，元数据须反映所有的OVAL定义的内容，当OVAL定义适用于一个以上的家庭时，此时意味着元数据可能需要对每一个受影响的家庭都有章节描述。

10.9 包含OVAL定义的资料库用于覆盖一个特定的漏洞时须包含，有可能的话，一个通用漏洞和披露（CVE）名称作为其参考。

10.10 包含OVAL定义的资料库用于检测一个特定配置状态时须包含，有可能的话，一个通用配置（CCE）ID作为其参考。

10.11 包含OVAL定义的资料库用于检测一个特定平台时须包含，有可能的话，一个通用平台枚举（CPE）名称作为其参考。

10.12 能力所有者须记录下用户检索内容更新的过程。

创建工具

这些要求适用于所有的产品或服务，旨在帮助和促进OVAL内容的创建或修改。

10.13 创建工具须提供一个搜索界面，允许用户通过ID搜索OVAL定义、测试集、对象、状态和变量。

10.14 创建工具应鼓励重复使用现有的OVAL定义、测试集、对象、状态和变量。

10.15 创建工具应允许用户在文件里面引用其是由OVAL语言编写的验证，并报告所有的W3C XML方案和Schematron错误给用户。

10.16 创建工具须允许用户导入和编辑现有的OVAL内容。

10.17 创建工具须允许用户导出工具创建的内容，作为有效的OVAL语言文件。

10.18 创建工具须向用户报告重复的内容。

10.19 创建工具须提供超出XML编辑器的价值和能力。

定义评估器

这些要求适用于所有的用于评估一个指定系统的产品或服务，而作为输入，信息以OVAL定义方案的格式给出。一旦评估完成，结果必须采用可用的OVAL结果方案格式。

10.20 用户须能够决定正在被评估的OVAL定义。

10.21 用户须能够检查每个正在被评估的OVAL定义的细节。此要求确保OVAL定义对于用户是开放的，允许他们看到一个特定问题如何被测试。

10.22 如果产品或服务在运行时不使用OVAL定义，能力所有者须记录下该过程，通过它用户可以提交OVAL定义给能力所有者用于产品的解释。这包括说明如何快速定义提交给能力所有者的产品。

10.23 产品或服务须能使用每个OVAL定义来解释所有的逻辑，同时按照状态逻辑运算符执行随后的OVAL测试。

10.24 产品或服务须基于OVAL定义中规定的细节，确定目标系统的评估结果。

10.25 用户须能够确定所有在目标系统评估中使用的OVAL定义的结果。

10.26 当使用一组特定的OVAL定义和系统状态信息时，产品或服务须生成精确的、可预测和可重复的结果。

10.27 产品或服务所生成的结果须可采用纯粹的OVAL结果格式。这使得其他想利用详细评估信息的产品或服务，能够获得所需的信息。或可提供精简的结果，但完整的结果不可或缺。

10.28 当一个OVAL定义在同一个系统中不止一次地被评估，每次采用不同的变量值，OVAL结果文件应包括每种情况下唯一的变量实例值。

10.29 产品或服务须对所有的OVAL定义使用“未评估”的结果作为原始OVAL定义文件的一部分，但不马上报告。给定的OVAL定义满足要求10.25的规定。

10.30 任何使用或将OVAL定义翻译为内部语言的产品或服务，须反映与原来的OVAL定义相同的逻辑。

结果处理者

这些要求适用于所有的产品或服务，用于处理OVAL结果方案格式的信息。

10.31 对于每个在被使用的OVAL结果文件中定义的系统，用户须能确定正在报告的特定的OVAL定义。

10.32 用户须能够检查正在使用的OVAL结果文件的细节。这可以简单到允许用户打开XML文件。这项要求的重点是为了确保OVAL结果是对用户开放的，允许他们检查报告的数据。

10.33 如果产品或服务在运行时不使用OVAL结果文件，能力所有者须记录下该过程，通过它用户可以将OVAL结果提交给能力所有者，用于产品或服务的解释。这包括说明产品或服务如何快速提供文件给能力所有者。

11 审查机构的要求

以下是关于审查机构在OVAL使用过程中必须坚持的要求。

11.1 审查机构须清晰地区分使用的版本，需求文档的版本，以及OVAL语言的版本，用于确定每个产品、服务或资料库是否正式遵守OVAL的使用要求。

11.2 审查机构须定义和发布测试材料的样例。

11.3 审查机构应公布如何参加正确性测试的信息，以使各组织可以提前做好准备。

11.4 审查机构须提供联络点，用于安排已完成“OVAL使用问卷调查表”，并声明支持OVAL能力的正确性测试。

11.5 审查机构可能会重新测试已经被其正式认证使用OVAL的产品、服务或资料库。

11.6 一旦任何希望启动OVAL使用进程的有效能力所有者发出请求，审查机构必须提供一份OVAL使用声明的副本。

11.7 一旦已提交填妥“OVAL使用声明表”的任何能力所有者发出请求，审查机构必须提供一份“OVAL使用问卷调查表”的副本。

12 废止

如果审查机构已证实产品、服务或资料库正确使用了OVAL，但是在稍后的时刻审查机构有证据表明其要求不再满足，那么审查机构可以废止其批准，以及不再正式认可产品、服务或资料库正确使用了OVAL。以下是审查机构在取消其认可时必须遵循的要求。

12.1 至少在废止发生的两个月前，审查机构须对能力所有者发出废止警告。

12.2 审查机构可能推迟废止日期。

12.3 如果审查机关发现能力所有者存在有意误导的行为或声明，那么审查机构可能跳过警告期。审查机构可能按照其意愿来解释短语“有意误导”。

12.4 如果审查机构发现能力所有者对要求实施的行为存在故意误导，则废止须持续至少一年。

12.5 审查机构须确定未满足的特定要求。

12.6 如果能力所有者认为要求都得到了满足，那么能力所有者须对废止警告作出回应，通过提供细节表明产品、服务或资料库为何满足要求。

12.7 在警告期间，如果所有者修改产品、服务或资料库使其符合问题的要求，那么审查机构应该结束关于产品、服务或资料库的废止行动。

12.8 审查机关应该公布，废止相应的产品、服务或资料库正确使用OVAL的正式认证。

12.9 审查机关可能公开废止原因。

参考资料

[b-ITU-T X.1520] ITU-T X.1520建议书（2011年），《通用漏洞披露》。

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其它组件的结构、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	**数据网、开放系统通信和安全性**
Y系列	全球信息基础设施、互联网协议问题和下一代网络
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2013年，日内瓦