国 际 电 信 联 盟

ITU-T X.1520

(01/2014)

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

常见漏洞和暴露风险

ITU-T X.1520 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
云计算安全	
云计算安全概况	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和导则	X.1640–X.1659
云计算安全实施	X.1660–X.1679
其他云计算安全	X.1680–X.1699

欲了解更详细信息，请查阅 ITU-T建议书目录。

ITU-T X.1520 建议书

常见漏洞和暴露风险

摘要

本建议书的内容涉及常见漏洞和暴露风险（CVE），为就信息安全漏洞和暴露风险交换信息提供了一种结构化的方法，希望能够为商用或开放源软件中已发现的问题提供一些通用名称。上述软件用于通信网、最终用户装置或其它能够运行软件的信息通信技术（ICT）产品。本建议书的目的是定义CVE的使用，利用这些通用命名方式，为在不同漏洞能力（工具、数据库和服务）之间共享数据提供便利。本建议书定义CVE的使用以便提供将漏洞数据库与其它能力连接在一起的机制方便安全工具与服务之间的对比。CVE不包含风险、影响、修理信息或其它详细的技术信息。CVE仅包含配有状态指标的标准标识符编号，简要的描述以及相关漏洞报告和数据库的参考。CVE标识符库见[cve.mitre.org/cve/cve.html]。

本建议书定义了CVE的使用。CVE的目的是全方位提供所有公众已知的漏洞和暴露风险信息。尽管CVE旨在提供成熟的信息，但其工作重点仍放在目前已被安全工具检测出的漏洞和暴露风险以及所有已公开的新问题，接下来才是处理那些需要验证的早期安全性问题。

沿革

版本	建议书	批准日期	研究组	唯一ID号*
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

* 要获取该建议书，请在您网页浏览器的地址栏中输入以下URL：“http://handle.itu.int/”以及建议书的唯一ID号。例如：http://handle.itu.int/11.1002/1000/11830-en。

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

本建议书的内容涉及常见漏洞和披露（CVE）的使用，为就信息安全漏洞和披露交换信息提供了一种结构化的方法，希望能够为商用或开放源软件中已发现的问题提供一些通用名称。上述软件用于通信网、最终用户装置或其它能够运行软件的ICT产品。本建议书的目的是定义CVE的使用，利用这些通用命名方式，为在不同漏洞能力（工具、数据库和服务）之间共享数据提供便利。本建议书可将漏洞数据库与其它能力一起使用，方便安全工具与服务之间的对比。因此，CVE不包含风险、影响、修理信息或其它详细的技术信息。CVE仅包含配有状态指标的标准标识符编号，简要的描述以及相关漏洞报告和数据库的参考。CVE标识符库见：http://cve.mitre.org/cve/cve.html。

本建议书定义的CVE旨在全方位提供所有公众已知的漏洞和披露信息。尽管CVE旨在提供成熟的信息，但其工作重点仍放在目前已被安全工具检测出的漏洞和披露以及所有已公开的新问题，接下来才是处理那些需要验证的早期安全性问题。

本建议书所属的ITU-T建议书类别是基于一个规模庞大的全球开发用户群起草并不断完善的开放性规范。从规范已提交ITU-T批准，并与ITU-T达成共识，即该规范的修改或更新应确保全面的技术一致性和兼容性，其中有关变更和完善的讨论将通过原用户群实施，并包括对该用户群相应版本的明确引用。

ITU-T X.1520 建议书

常见漏洞和暴露风险

1 范围

有关常见漏洞和暴露风险的本建议书为在全球交流已为公众所知的成熟漏洞和暴露风险信息提供了一种结构化方式。这些漏洞和暴露风险或是通过安全工具检测出来或以其它方式被公之于众。这种“结构化方式”往往被看作“CVE兼容性”并对CVE的正确使用做出规定。信息安全漏洞是指软件中的错误，可被黑客直接用于获取对系统或网络的接入。信息安全暴露风险是指一种软件错误，它允许黑客使用某些信息或能力，将其作为进入系统或网络的垫脚石。CVE标识符的指配不在本建议书的讨论范围之内。

在ITU-T X.1520 建议书与MITRE公司协作编制，念念不忘尽可能保持ITU-T X.1520 建议书与2013年6月“CVE兼容性要求和建议”之间技术兼容性的重要性，后者在下列网站提供：https://cve.mitre.org/compatible/Requirements_for_CVE_Compatibility_V1.3.pdf。

2 参考文献

无。

3 定义

3.1 其它地方定义的术语

无。

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 准确率：引用正确CVE标识符的安全要素在审核抽样中的比例。

3.2.2 能力：可提供安全漏洞或暴露风险标识功能的安全工具、数据库、网站、报告或服务。

3.2.3 暴露风险：信息安全暴露风险是指一种软件错误，它可被黑客利用来获取信息或能力，将其作为进入某系统或网络的垫脚石。

3.2.4 映射：数据库中安全元素与相关CVE名称间关系的规范。

3.2.5 所有者：负责能力的监护人（实际的人或企业）。

3.2.6 数据库：支持某项能力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。

3.2.7 审核：判定某项能力是否与CVE兼容的过程。

3.2.8 审核机构：任何进行审核的实体。

注 – MITRE是唯一的审核机构。

3.2.9 审核日期：用于判定某种能力CVE兼容性的CVE内容的日期。

3.2.10 审核抽样：能力数据库中供审核机构评估精确性的安全要素组合。

3.2.11 抽样方法：审核机构确定审核抽样中安全要素的方法。

3.2.12 抽样规模：审核机构需要检查的安全要素比例和/或数量。

3.2.13 安全要素：与特定漏洞或暴露风险相关的数据库记录、电子邮件信息、安全报告、评估调查、签名等。

3.2.14 任务：使用工具进行的调查、检查、签名等，其操作会生成安全信息（即，安全要素）。

3.2.15 工具：一种软件应用或装置，负责检查主机或网络并生成与漏洞或暴露风险相关的信息或收集此类信息，例如漏洞扫描仪、入侵检测系统、风险管理、安全信息管理、合规报告工具或服务。

3.2.16 用户：能力的消费者或潜在消费者。

3.2.17 漏洞：软件中可被用来毁坏系统或系统所含信息的缺陷（基于[b-ITU-T X.1500]）。

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：

ASCII 美国信息交换标准代码
CVE 常见漏洞和暴露风险
GUI 图形用户接口
HTML 超文本标识语言
HTTP 超文本传输协议
IDS 入侵检测系统
PDF 便携文件格式
POC 联系人
URL 统一资源定位符
XML 可扩展标记语言

5 惯例

CVE在本建议书中作为名词使用。

6 高层要求

以下各项确定了与适当使用CVE标识符相关的概念、作用和责任，以便在不同漏洞能力（工具、数据库和服务）之间共用数据，使漏洞数据库和其他能力可以一起使用并为比较安全工具和服务提供便利。

前提

6.1 能力所有者必需是一个有效的法律实体，即一个组织或具体的个人，拥有有效的电话号码、电子邮件地址和街道邮寄地址。

6.2 除CVE自身（即姓名、说明、参考和相关数据）之外该能力应当提供附加的价值或信息。

6.3 能力所有者应为审核机构提供一名技术联系人，该联系人应有资格回答所有与映射和能力中与CVE功能相关的全部问题。

6.4 能力的商业版本应向大众或特定的消费者提供。

6.5 能力所有者应为审核机构提供一套完整的“CVE兼容性要求评估表”。

6.6 对配有数据库的能力，能力所有者应为审核机构提供免费数据库接入，这样该机构便可判定此数据是否满足所有相关要求。

6.7 针对拥有数据库的能力，能力所有者应允许审核机构使用该数据库，以确定那些必需加入CVE的漏洞。

6.8 能力所有者应同意遵守所有强制性CVE兼容要求，其中包括针对特定类型能力的强制要求。

功能

6.9 能力应允许用户使用CVE名称（“CVE-输出”）来定义安全要素。

6.10 当能力向用户介绍安全要素时，应允许用户获取相关的CVE名称（“CVE-输出”）。

6.11 对拥有数据库的能力，能力能力的映射应准确的将安全要素与相应的CVE名称（“映射精度”）连接在一起。

6.12 能力文档应准确的描述CVE、CVE兼容性以及能力中CVE相关功能的使用情况（“CVE-文档”）。

6.13 能力应指出CVE的更新日期（“日期使用”）。

6.14 能力应满足某种特定类型的补充要求，如附件A所述。

6.15 能力应满足其分配媒介的所有要求，如附件B所述。

6.16 不应对能力提出如下要求：

- 使用与CVE相同的说明或参考
- 在其数据库中包括所有CVE名称

其它事项

6.17 如果能力不能满足所有上述适用要求（6.1至6.16），则能力所有者不得宣布其为CVE兼容。

7 精确度

只有能力映射准确时，CVE兼容性才能促进数据共享。因此，CVE兼容性能力必需满足下文的最低精确度要求。

7.1 对于配有数据库的能力，该数据库的精确率应为90%或90%以上。

7.2 在审核期内，能力所有者应更正任何审核机构发现的映射错误。

7.3 审核期过后，能力所有者应当在该差错上报之后合理的时间段内更正映射差错，其期限对数据库而言为两（2）个版本，对于工具而言为六（6）个月，对网上能力和服务而言为三（3）个月。

7.4 对配有数据库的能力而言，能力所有者应当准备并签署一份声明，尽其所能确保映射中不存在差错。

7.5 如果某项能力是基于或使用了另一种CVE兼容能力（“源”能力），且所有者意识到源能力中存在映射差错，则该能力所有者应向源能力所有者报告这些差错。

7.6 报告档案的映射精度应针对档案数据库中的所有安全要素，其中包括档案首次在安全要素中使用CVE名称以及之后的使用。

7.7 能力应在三（3）个月内为在线功能和服务如实反映废弃的CVE名称的状态。

7.8 在CVE ID被弃用的三（3）个月内，能力不应在废弃CVE ID的描述说明更合适的ID时，输出废弃的CVE ID。

8 文档

下述要求适用于能力提供的文档。

8.1 文档的内容应包括CVE和CVE兼容性的简要描述，其内容可从CVE网站中的文件逐字照搬。

8.2 文档应当描述用户如何能够利用CVE名称从能力数据库中找到独立的安全要素。

8.3 文档应当描述用户如何能够从能力数据库中的独立要素中获得CVE名称。

8.4 如果文档包括索引，则该文档应在“CVE”术语项下包含CVE相关文档的参考。

9 CVE数据使用

用户必需能够确定能力数据库在CVE映射方面的“更新”程度。能力所有者需指出映射的更新程度，其方式是提供其最后一次CVE信息更新的日期并指出其使用那部分CVE内容及其采集CVE内容的位置。

9.1 各新版本的能力均应至少通过下述方法之一来标识创建、更新和映射所用CVE内容的最新日期：变更日志、新功能清单、帮助文件或其它机制。能力与此日期“保持一致”。

9.2 各新版本的能力均应与公布的CVE日期保持同步，该日期不会早于向用户提供此项能力之前三个月。如果某项能力无法满足这一要求，则可认为其按规定已“过期”。

9.3 能力所有者应当公布其更新能力数据库以纳入新CVE信息的频率。

9.4 能力所有者应当描述其选择将某类CVE信息纳入能力时所采用的标准和机制。

9.5 能力所有者应当描述其收集新CVE信息的来源。

10 不同版本CVE名称支持

无论采用老式四位数还是可变长度（四位或更多位数）的CVE-ID句法（在对2013年12月后采用的CVE-ID句法修改时使用），能力对CVE名称的使用应当独立于CVE名称在该能力中的表述格式。

10.1 如果用户使用YYYY-NNNN、YYYY-NNNNN、YYYY-NNNNNN或其它具有大量数位的有效ID进行搜索，则能力应当在其数据库中返回分别与CVE-YYYY-NNNN、CVE-YYYY-NNNNN、CVE-YYYY-NNNNNN或其它具有大量数位的有效ID相应的安全要素，而无论该CVE名称使用CVE还是CAN作为其名称的组成部分。

10.2 如果能力包含CVE名称CVE-YYYY-NNNN，但用户搜索时使用的是CVE名称的老格式，CVE-YYYY-NNNN（在2005年10月19日引入CVE命名方式变革之前），则能力应当返回CAN-YYYY-NNNN。

11 CVE兼容性的撤销

11.1 如果审核机构已经验证某能力为CVE兼容，但后来该审核机构有证据表明这些要求并未得到满足，则审核机构可撤销其批准。

11.1.1 审核机构应当指出未得到满足的具体要求。

11.2 审核机构应当判定能力所有者的行为或声明是否为“有意误导”。

11.2.1 审核机构可按照其意愿对“有意误导”一词做出解释。

11.3 除非有两个并无利益冲突的CVE编辑委员会成员提议，否则审核机构审议是否撤销某特定能力CVE兼容性的审查周期不得短于六（6）个月。

警告和评估

11.4 审核机构应当至少在取消计划实施日期之前两（2）个月，向能力所有者和技术联系人提出撤销警告。

11.4.1 如果审核机构发现能力所有者的行为或声明为故意误导，则审核机构可不提供警告期。

11.5 如果能力所有者坚信所有要求均得到了满足，则能力所有者可对撤销警告做出响应，提供详细信息指出因何其能力能够满足这些要求。

11.6 如果所有者对能力进行了修改，因此该能力能够在警告期内满足相关要求，则审核机构应当终止针对该能力的撤销行动。

撤销

11.7 审核机构可以推迟撤销的日期。

11.8 审核机构应当公布某项能力的CVE兼容性已被取消。

11.9 如果审核机构发现能力所有者在CVE兼容性要求方面所采取的行动是故意进行误导，则撤销至少应持续一年。

11.10 审核机构可以公布撤销的原因。

11.11 如果批准被撤销，能力所有者在撤销期内不得申请重新审核。

12 审核机构

针对审核机构开展的审核：

12.1 审核机构可针对具体的CVE内容日期，即审核日期，进行CVE兼容性审核。

12.2 审核机构应当明确指出用于判定能力兼容性的审核日期。

12.3 审核机构应当明确指出用于判定能力兼容性的、CVE兼容性要求文件的版本。

12.4 审核机构应当确定并公布抽样规模。

12.4.1 审核机构应当使用50个要素的抽样规模，再加上能力数据库的5%，其最大抽样规模可达到400个要素。

12.4.2 审核机构可对能力数据库中的各个要素进行审核。

12.5 审核机构应当公布抽样方法。

12.6 审核机构可使用非随机选择的审核抽样。

12.7 针对在相同时间段进行评估的各项能力，审核机构应当使用相同的抽样方法和抽样规模。

附件A

针对具体类型的要求

（此附件是本建议书不可分割组成部分）

由于许多能力均在使用CVE，因此某些类型的能力可能拥有特殊功能，需要对其CVE兼容性予以特别关注。

A.1 能力应当满足与特定类型相关的所有附加要求。

A.1.1 如果某项能力为漏洞评估扫描仪、入侵检测系统（IDS）或一种综合了一个或多个扫描仪和IDS检查结果的产品，则其须满足工具要求A.2.1 - A.2.8的规定。

A.1.2 如果能力是一项服务（例如受控的入侵检测和响应服务或远程扫描服务），则其须满足安全服务要求A.3.1 – A.3.5的规定。

A.1.3 如果能力是一项网络漏洞或签名数据库、网络档案或维护/补丁站点，则其须满足网络能力要求A.4.1 – A.4.3的规定。

A.1.4 如果能力是一种合成工具，例如安全信息管理器、合规报告工具或提供此类漏洞类型信息合成产品的服务，则其须满足合成能力要求A.5.1 - A.5.6的规定。

工具要求

A.2.1 工具应当允许用户使用CVE名称在工具内部定位相关的任务（“CVE-搜索”），其方式是至少提供下述功能之一：“查找”或“搜索”功能、该工具任务名称与CVE名称之间的映射或其它机制。

A.2.2 对确定独立安全要素的报告而言，该工具应当通过使用下述方式之一使用户能够判定这些要素的相关CVE名称（“CVE-输出”）：将CVE名称直接纳入报告、在工具任务名称与CVE名称之间提供映射或使用其它机制。

A.2.3 所有要求的报告或映射均应满足附件B中规定的媒体要求。

A.2.4 工具或所有者应当为用户提供与工具任务相关的所有CVE名称清单。

A.2.5 工具应当以提供包含CVE名称清单文件的方式，使用户能够选择任务级。

A.2.6 工具接口可以利用独立的CVE名称，使用户能够浏览，选择或取消任务集合。

A.2.7 如果工具中没有与用户指定的CVE名称相关的任务（在工具要求中的A.2.5或A.2.6），则工具应通知用户其无法执行相关任务。

A.2.8 能力所有者应当保证（1）误报率小于100%，即如果工具报告某特定安全要素，则其至少在某些时候是正确的，且（2）漏报率低于100%，即当与特定安全要素相关的事件发生时，有时工具会报告该时间。

安全服务要求

安全服务在工作时有时可能会使用CVE兼容的工具，但它们可能不会允许用户直接使用这些工具。因此，客户可能很难确定并比较不同业务的能力。安全业务要求旨在解决这一潜在限制。

A.3.1 安全业务应当能够使用CVE名称告诉用户该服务测试或检测了那些安全要素（“CVE-搜索”），其实现使用了下述一种或多种方式：为用户提供CVE名称的清单指出该业务测试或检测的要素、为用户提供业务要素与CVE名称之间的映射、以明确该业务测试或检测的CVE名称的方式对用户提交的CVE名称清单做出响应，或者使用一些其它机制。

A.3.2 对于确定单独安全要素的报告，服务应当通过下述一种或多种方式允许用户判定这些要素的相关CVE名称（“CVE-输出”）：允许用户将CVE名称直接纳入报告、为用户提供安全要素与CVE名称间的映射或使用其它机制。

A.3.3 服务提供的所有规定报告或映射均应满足附件B规定的媒体要求。

A.3.4 如果服务允许用户直接使用标识安全要素的产品，则该产品应为CVE兼容。

A.3.5 能力所有者应当保证（1）误报率小于100%，即如果工具报告某特定安全要素，则其至少在某些时候是正确的，且（2）漏报率低于100%，即当与特定安全要素相关的事件发生时，有时工具会报告该时间。

在线能力要求

A.4.1 在线能力通过提供下述功能，允许用户从在线能力数据库（“CVE-搜索”）中查找相关的安全要素：能够返回相关要素CVE名称的搜索功能、将各要素与相关CVE名称连接在一起的映射或其它机制。

A.4.1.1 在线能力应当提供一个URL“模板”，允许计算机程序能够方便的建立一个链接，从而能够使用A.4.1款在线能力要求中描述的搜索功能。

示例： `http://www.example.com/cgi-bin/db-search.cgi?cvename=CVE-YYYY NNNN`

```
http://www.example.com/cgi-bin/db-search.cgi?cvename=CVE-YYYY NNNNN
http://www.example.com/cgi-bin/db-search.cgi?cvename=CVE-YYYY NNNNNN
http://www.example.com/cve/CVE-YYYY-NNNN.html
http://www.example.com/cve/CVE-YYYY-NNNNN.html
http://www.example.com/cve/CVE-YYYY-NNNNNN.html
```

A.4.1.2 如果URL模板用于CGI程序，则该程序应当接受HTTP "GET"方法。

A.4.2 对于标识独立安全要素的报告，在线能力应当通过下述一种或几种方式允许用户判定这些要素的相关CVE名称（“CVE-输出”）：允许用户将CVE名称直接纳入报告、为用户提供安全要素与CVE名称之间的映射或通过其它机制实现。

A.4.3 如果在线能力不提供单独安全要素的详细信息，则在线能力应提供将各元素与相关CVE名称连接在一起的映射。

合成能力要求

A.5.1 合成能力以至少提供下述功能之一的方式允许用户使用CVE名称确定该能力中的相关要素（“CVE-搜索”）：“查询”或“搜索”功能，该能力名称与CVE名称之间的映射或审核机构批准的其它机制。

A.5.2 对于标识单独安全要素的报告，合成能力应当至少通过下述一种方式允许用户判定与这些要素相关的CVE名称（“CVE-输出”）：将CVE名称直接纳入报告、提供能力名称与CVE名称间的映射或使用其它机制。

A.5.3 所有必须提供的报告或映射均应满足附件B中的媒体要求。

A.5.4 工具或能力所有者应当为用户提供一份与工具任务相关的所有CVE名称清单。

A.5.5 该工具应当通过提供包含CVE名称清单的文件使用户能够选择任务集合。

A.5.6 该工具的接口应当允许用户通过使用独立的CVE名称对任务集合进行浏览、选择与取消。

附件B

媒体要求

（此附件是本建议书不可分割组成部分）

B.1 CVE兼容能力使用的传播媒体应采用本附件中包括的媒体格式。

B.2 媒体格式应当满足对该格式的具体要求。

电子文件（HTML、文字处理器、PDF、ASCII文本等）

B.3.1 文件应使用常用的格式，其阅读器支持“查找”或“搜索”功能（“CVE-搜索”），例如原始ASCII文本、HTML或PDF。

B.3.2 如果文件仅提供针对单独要素的短名称或标题，则其应列出与这些要素相关的CVE名称（“CVE-输出”）。

B.3.3 文件应当包括要素与CVE名称之间的映射，列出各要素的相应页数。

图形用户接口（GUI）

B.4.1 GUI应当为用户提供搜索功能，允许用户输入CVE名称并对相关要素进行检索（“CVE-搜索”）。

B.4.2 如果GUI列出了单独要素的详细内容，则其应当列出映射至该要素的CVE名称（或多个名称）（“CVE-输出”）。否则，GUI为用户提供的映射其格式应当满足B.3.1电子文件要求中的规定。

B.4.3 GUI应当允许用户使用能够满足B.3.1电子文件要求的格式导出或访问CVE相关数据。

附件C

媒体要求

（此附件是本建议书不可分割的组成部分）

本附件包含的CVE XML方案可通过下述网址获取：
http://cve.mitre.org/schema/cve/cve_1.0.xsd 下文复制了该方案的内容。

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns="http://cve.mitre.org/cve/downloads/1.0"
    targetNamespace="http://cve.mitre.org/cve/downloads/1.0"
    elementFormDefault="qualified" attributeFormDefault="unqualified" version="1.0">

  <!--  ********************************************************************** -->
  <!--  Changelog: 1.0 - Initial version -->
  <!--  ********************************************************************** -->
  <xsd:annotation>
    <xsd:documentation xml:lang="en">
      Simple schema that defines the format of the CVE List provided by MITRE
    </xsd:documentation>
  </xsd:annotation>

  <!--  ********************************************************************** -->
  <!--  Start Item Element Definition -->
  <!--  ********************************************************************** -->
  <xsd:element name="cve">
    <xsd:annotation>
      <xsd:documentation xml:lang="en">
        cve is the top level element of the CVE List provided by MITRE.
        It represents holds all CVE Items.
      </xsd:documentation>
    </xsd:annotation>
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element name="item" type="ItemType" minOccurs="1" maxOccurs="unbounded"/>
      </xsd:sequence>
      <xsd:attribute name="schemaVersion" type="xsd:token" use="optional"/>
    </xsd:complexType>
  </xsd:element>

  <!--  ********************************************************************** -->
  <!--  Simple Types -->
  <!--  ********************************************************************** -->
  <!-- CUSTOM TYPE DEFINITIONS-->
  <xsd:simpleType name="typeEnumType">
    <xsd:restriction base="xsd:token">
      <xsd:enumeration value="CAN"/>
      <xsd:enumeration value="CVE"/>
    </xsd:restriction>
  </xsd:simpleType>

  <xsd:simpleType name="statusEnumType">
    <xsd:restriction base="xsd:token">
      <xsd:enumeration value="Entry"/>
      <xsd:enumeration value="Candidate"/>
    </xsd:restriction>
  </xsd:simpleType>

  <!-- need to verify enumeration -->
  <xsd:simpleType name="simplePhaseEnumType">
    <xsd:restriction base="xsd:token">
      <xsd:enumeration value="Proposed"/>
      <xsd:enumeration value="Interim"/>
      <xsd:enumeration value="Modified"/>
      <xsd:enumeration value="Assigned"/>
```

```
  </xsd:restriction>
</xsd:simpleType>

<!--  ********************************************************************** -->
<!--  Complex Types -->
<!--  ********************************************************************** -->
<xsd:complexType name="ItemType">
  <xsd:sequence>
    <xsd:element name="status" type="statusEnumType" minOccurs="1" maxOccurs="1"/>
    <xsd:element name="phase" type="specificPhaseType" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="desc" type="xsd:string" minOccurs="1" maxOccurs="1"/>
    <xsd:element name="refs" type="refsType" minOccurs="1" maxOccurs="1"/>
    <xsd:element name="votes" type="votesType" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="comments" type="commentsType" minOccurs="0" maxOccurs="1"/>
  </xsd:sequence>
  <!--Need to Verify Enumeration-->
  <xsd:attribute name="type" type="typeEnumType" use="required"/>
  <xsd:attribute name="name" type="xsd:token" use="required"/>
  <xsd:attribute name="seq" type="xsd:token" use="required"/>
</xsd:complexType>

<xsd:complexType name="commentsType">
  <xsd:sequence>
    <xsd:element name="comment" minOccurs="0" maxOccurs="unbounded">
      <xsd:complexType>
        <xsd:simpleContent>
          <xsd:extension base="xsd:string">
            <xsd:attribute name="voter" type="xsd:token" use="required"/>
          </xsd:extension>
        </xsd:simpleContent>
      </xsd:complexType>
    </xsd:element>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="votesType">
  <xsd:sequence>
    <xsd:element name="accept" minOccurs="0" maxOccurs="1">
      <xsd:complexType>
        <xsd:simpleContent>
          <xsd:extension base="xsd:string">
            <xsd:attribute name="count" type="xsd:token" use="required"/>
          </xsd:extension>
        </xsd:simpleContent>
      </xsd:complexType>
    </xsd:element>
    <xsd:element name="modify" minOccurs="0" maxOccurs="1">
      <xsd:complexType>
        <xsd:simpleContent>
          <xsd:extension base="xsd:string">
            <xsd:attribute name="count" type="xsd:token" use="required"/>
          </xsd:extension>
        </xsd:simpleContent>
      </xsd:complexType>
    </xsd:element>
    <xsd:element name="noop" minOccurs="0" maxOccurs="1">
      <xsd:complexType>
        <xsd:simpleContent>
          <xsd:extension base="xsd:string">
            <xsd:attribute name="count" type="xsd:token" use="required"/>
          </xsd:extension>
        </xsd:simpleContent>
      </xsd:complexType>
    </xsd:element>
    <xsd:element name="recast" minOccurs="0" maxOccurs="1">
      <xsd:complexType>
        <xsd:simpleContent>
          <xsd:extension base="xsd:string">
            <xsd:attribute name="count" type="xsd:token" use="required"/>
          </xsd:extension>
        </xsd:simpleContent>
```

```
        </xsd:complexType>
      </xsd:element>
      <xsd:element name="reject" minOccurs="0" maxOccurs="1">
        <xsd:complexType>
          <xsd:simpleContent>
            <xsd:extension base="xsd:string">
              <xsd:attribute name="count" type="xsd:token" use="required"/>
            </xsd:extension>
          </xsd:simpleContent>
        </xsd:complexType>
      </xsd:element>
      <xsd:element name="reviewing" minOccurs="0" maxOccurs="1">
        <xsd:complexType>
          <xsd:simpleContent>
            <xsd:extension base="xsd:string">
              <xsd:attribute name="count" type="xsd:token" use="required"/>
            </xsd:extension>
          </xsd:simpleContent>
        </xsd:complexType>
      </xsd:element>
      <xsd:element name="revote" minOccurs="0" maxOccurs="1">
        <xsd:complexType>
          <xsd:simpleContent>
            <xsd:extension base="xsd:string">
              <xsd:attribute name="count" type="xsd:token" use="required"/>
            </xsd:extension>
          </xsd:simpleContent>
        </xsd:complexType>
      </xsd:element>
    </xsd:sequence>
  </xsd:complexType>

  <xsd:complexType name="specificPhaseType">
    <xsd:simpleContent>
      <xsd:extension base="simplePhaseEnumType">
        <xsd:attribute name="date" type="xsd:token" use="optional"/>
      </xsd:extension>
    </xsd:simpleContent>
  </xsd:complexType>

  <xsd:complexType name="refsType">
    <xsd:annotation>
      <xsd:documentation>holds all hyperlink elements</xsd:documentation>
    </xsd:annotation>
    <xsd:sequence>
      <xsd:element name="ref" type="refType" minOccurs="0" maxOccurs="unbounded"/>
    </xsd:sequence>
  </xsd:complexType>

  <xsd:complexType name="refType">
    <xsd:annotation>
      <xsd:documentation>Holds individual hyperlink element</xsd:documentation>
    </xsd:annotation>
    <xsd:simpleContent>
      <xsd:extension base="xsd:string">
        <xsd:attribute name="source" type="xsd:token" use="required"/>
        <xsd:attribute name="url" type="xsd:anyURI" use="optional"/>
      </xsd:extension>
    </xsd:simpleContent>
  </xsd:complexType>
</xsd:schema>
```

参考资料

[b-ITU-T X.1500] ITU-T X.1500建议书（2011） – 网络安全信息交换概述。

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
2014年，日内瓦