国 际 电 信 联 盟

ITU-T X.1525

国际电信联盟
电信标准化部门

(04/2015)

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

共同弱点评分系统

ITU-T X.1525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	X.1080–X.1099
安全应用和服务(1)	
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(1)	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
PITV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(2)	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1360–X.1369
智能交通系统（ITS）安全	X.1370–X.1389
分布式账簿技术安全	X.1400–X.1429
安全协议(2)	X.1450–X.1459
网络安全信息交换	
网络安全综述	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
探索法和信息要求	X.1560–X.1569
标示和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全综述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳实践和指导原则	X.1640–X.1659
云计算安全实现	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	X.1700–X.1729

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1525建议书

共同弱点评分系统

摘要

有关共同弱点评分系统的ITU-T X.1525建议书提供了一个开放框架，用于在软件能力开发中沟通信息通信技术（ICT）的特征和影响。本建议书旨在使ICT软件开发者、管理者、测试员、安全软件商、服务提供商、采购者、应用提供商和研究人员以共同的语言讨论ICT弱点评分，并在软件使用中以漏洞的形式予以反映。

历史沿革

版本	建议书	批准日期	研究组	唯一标识（ID）*
1.0	ITU-T X.1525	2015-04-17	17	11.1002/1000/12357

* 为获取本建议书，请在网页浏览器内键入URLhttp://handle.itu.int/，然后输入唯一ID。例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信和信息通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）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

本建议书为简要而使用的“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。“须”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/。

© 国际电联 2020

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

目录

页码

1 范围 1

2 参考文献 1

3 定义 1

3.1 在其它文件中定义的术语 1

3.2 本建议书定义的术语 2

4 缩略语和首字母缩写词 2

5 排印惯例 3

6 CWSS的使用 3

6.1 CWSS说明 3

6.2 CWSS的工作方式 4

6.3 CWSS评分 5

6.4 CWSS用户 6

7 度量指标组 7

7.1 度量指标组的各项要素 7

7.2 不确定性和灵活性的数值 7

7.3 基准查找度量指标组 8

7.4 攻击界面度量指标组 13

7.5 环境度量指标组 18

7.6 CWSS评分公式 22

7.7 CWSS矢量、评分示例和得分的可携带性 24

参考资料 28

引言

软件开发者经常要面对成百上千在编码中发现的弱点缺陷报告。在某些情况下，软件的弱点甚至可以导致可被人利用的漏洞。由于上报弱点数量很大，利益攸关方通常被迫要确定那些必须调查解决的问题的优先级。简言之，人们必须能够推断和通告不同弱点的相对重要性。尽管当今使用了不同种类的评分方法，但这些方法或者是专用方法或不适用于当前尚不精准的软件安全性评估。共同弱点评分系统（CWSS）为以一致、灵活、开放的方式对软件弱点进行优先级排序并使之适用于各类业务领域和目标软件用法提供了一种机制。这种以团队为基础的协作，旨在满足政府、学术界和行业利益攸关方的需求。

ICT软件开发者、管理者、测试员、安全软件商、服务提供商、采购者、应用提供商和研究人员，必须确定并评估在使用过程中会作为漏洞暴露出来的弱点。上述人员需具备为弱点进行优先级排序，并根据危险等级确定对哪些弱点采取补救行动的能力。由于需要排除的漏洞很多，且对每一个漏洞的评分均采用不同的数值范围，因此只能由各种ICT团体的成员、管理人员、测试员、采购者和开发者自己找出对零散漏洞做出比较的某种方法，并将其转化为可采取行动的信息。

由于CWSS对描述弱点特性的方式实行标准化，因此CWSS用户可启动“攻击界面和环境度量的指标（metrics）”，来应用语境（contextual）信息，这些信息能够更加准确地反映其操作所属独特商业环境下的软件能力风险，及其希望提供的独特业务能力面临的风险。这将使他们在试图缓解弱点造成的风险方面做出更佳的知情决策。

CWSS利用网络安全界的现有工作成果，例如有关常见漏洞和敞口（CVE）的[b-ITU-T X.1520]建议书提及的大量现实存在且为公众所知晓的不同漏洞，以及通过[b-ITU-T X.1521]建议书讨论已知漏洞严重性的公共弱点评分系统（CVSS）和软件架构、设计、编码或部署中的常见弱点枚举（CWE）清单。在构建CWSS时，应在允许未知领域使用合理缺省值的情况下，根据商业和技术背景提供定制。

CWSS属于ITU-T建议书当中的一个类别，来源于全球现有的大型开发和用户社团，由该社团编写并完善的开放性规范供ITU-T采用，为此达成的共识确保对规范的所有修改或更新都将确保充分的技术等效性和兼容性，同时将通过原有的用户社团程序开展有关修改充实的磋商，并在其中加入对用户社团保留的相应具体版本的明确引证。因此在最初通过ITU-T X.1525建议书时，将出现对等效性的应付努力确认和说明；随着用户社团进行的修改，之后版本的建议书将通过持续合作及时反映这些修改。

ITU-T X.1525建议书 – 共同弱点评分系统（CWSS）是在与MITRE公司协作基础上制定的，在此过程中，我们始终牢记尽可能保持ITU-T X.1525建议书 – 共同弱点评分系统（CWSS）和“共同弱点评分系统（CWSS）”版本1.0.1（2014年9月5日）间的技术兼容性十分重要[https://cwe.mitre.org/cwss/cwss_v1.0.1.html]。

ITU-T X.1525建议书

共同弱点评分系统

1 范围

本建议书提供了一种标准化方式，以便通过相关语境信息的攻击界面和环境度量指标介绍ICT软件能力开发过程中存在的漏洞特性及其影响，从而更准确地反映在用户执行功能的特定商业背景下和软件独特的业务能力下，相关软件功能用户面临的风险。

2 参考文献

下列ITU-T建议书和其它参考文献的条款，在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有建议书和其它参考文献均会得到修订，本建议书的使用者应查证是否有可能使用下列建议书或其它参考文献的最新版本。当前有效的ITU-T建议书清单定期出版。本建议书引用的文件自成一体时不具备建议书的地位。

无。

3 定义

3.1 在其它文件中定义的术语

本建议书使用以下他处定义的术语：

3.1.1 接入（Access）[b-ITU-T X.1521]：主体浏览、修改或与对象进行通信的能力。接入有助于主体和对象之间的信息流动。

3.1.2 可用性（Availability）[b-ITU-T X.1521]：经授权的个人对数据和资源的可靠和及时的接入。

3.1.3 攻击实例（attack instance）[b-ITU-T X.1544]：针对应用程序或系统，利用系统中的漏洞或薄弱环节进行有的放矢的进攻。

3.1.4 保密性（Confidentiality）[b-ITU-T X.1521]：旨在确保信息不被披露给未经授权的主体的安全原则。

3.1.5 完整性（Integrity）[b-ITU-T X.1521]：确保信息和系统不被恶意或意外修改的安全原则。

3.1.6 风险（Risk）[b-ITU-T X.1521]：被利用的漏洞将对用户环境产生的相对影响。

3.1.7 威胁（Threat）[b-ITU-T X.1521]：有害事件出现的可能性或频次。

3.1.8 漏洞（vulnerability）[b-ITU-T X.1500]：所有可能被用来破坏系统或它所含信息的缺陷。

3.1.9 弱点（weakness）[b-ITU-T X.1524]：软件代码、设计、架构或实施中的缺点或缺陷，在某些时候可能成为漏洞，或可能引入其他漏洞。

3.2 本建议书定义的术语

本建议书定义了如下术语：

3.2.1 小插图（vignette）：小插图为定义某种特定环境，软件在该环境中起到的作用以及某个组织在软件安全方面的工作重点，提供了一种可共用的正式方法。

4 缩略语和首字母缩写词

本建议书使用了如下缩略语和首字母缩写词：

AI	认证次数
AL	已获权限所在层
AP	获得的权限
AS	认证强度
ASLR	地址空间布局的随机化
AV	接入矢量
BI	商业影响
BVC	业务值的背景
CD	光盘
CIO	首席信息官
CSO	首席安全官
CSRF	跨网站请求伪造
CVSS	公共漏洞评分系统
CWE	常见弱点枚举
CWRAF	公共弱点风险分析框架
CWSS	共同弱点评分系统
DI	发现的可能性
DNS	域名系统
DS	部署范围
EC	外部控制的有效性
EX	被利用的可能性
FC	查找的置信度
FTP	文件传输协议
HTML	超文本标识语言
IC	内部控制的有效性
ICT	信息通信技术
IN	互动水平
IP	互联网协议
NIST	国立标准和技术学院

OS	操作系统
OWASP	开放网络应用安全项目
P	流行
PCI DSS	支付卡行业数据安全标准
RL	要求的权限所在层
RP	要求的权限
SAMATE	软件保障度量指标和工具评估
SANS	系统管理员、审计、连网和安全性
SQL	结构化查询语言
SSL	安全套接层
TI	技术影响
TLS	传输层安全性
USB	通用串型总线
XSS	跨网站脚本攻击

5 排印惯例

无。

6 CWSS的使用

当前，ICT软件开发者、管理者、测试员、安全软件商、服务提供商、采购者、应用提供商和研究人员，必须确定并评估在使用过程中会作为漏洞暴露出来的弱点。上述人员需具备为弱点进行优先级排序，并根据危险等级确定对哪些弱点采取补救行动的能力。由于需要排除的漏洞很多，且对每一个漏洞的评分均采用不同的数值范围，因此只能由各种ICT团体的成员、管理人员、测试员、采购者和开发者自己找出对零散漏洞做出比较的某种方法，并将其转化为可采取行动的信息。共同弱点评分系统（CWSS）是解决此问题的一个开放性框架。它可提供如下益处：

- 定量测量：CWSS可对某软件应用内可能出现的未确定弱点提供定量测量。
- 公共框架：CWSS可为软件应用中发现的安全错误（“弱点”）的优先级确定提供一种公共框架。
- 定制的优先级：CWSS可与公共弱点风险分析框架（CWRAF）[b-CWRAF]一起共用被消费者用于确定其业务领域内最重要类型的弱点，从而将在采购和实施相关保护活动时发出通知，作为确保软件安全的更高级别程序的一个组成部分。

6.1 CWSS说明

CWSS的由三个度量指标组构成：基准查找组、攻击界面组和环境组，请参见图1。各组包含多个度量指标 – 亦称为因子 – 用于计算某项弱点的CWSS得分。

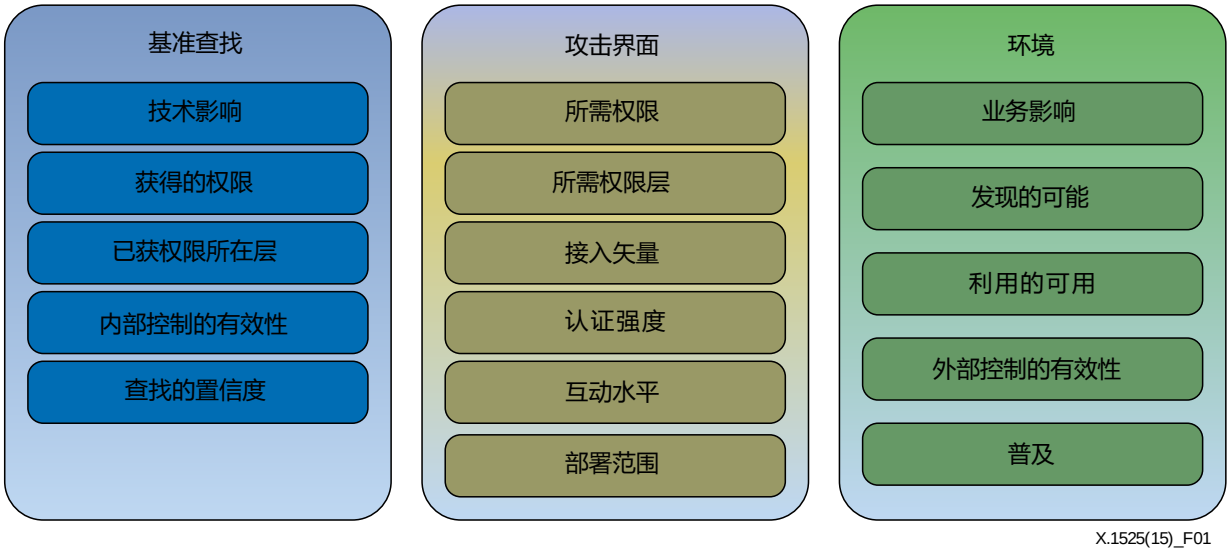

图 1 – CWSS 度量指标组

这些度量指标组的描述如下：

- 基准查找度量指标组：负责捕获弱点的内在风险，查找的准确性和控制的强度。基准查找度量指标组将在第7.3节探讨。
- 攻击界面度量指标组：负责指出为利用弱点攻击方必须克服的障碍。攻击界面度量指标组将在第7.4节探讨。
- 环境度量指标组：指出特定环境或操作背景下弱点的特性。环境度量指标组将在第7.5节探讨。

6.2 CWSS的工作方式

基准查找度量指标组的各项因子均指配有数值。这些数值被转换为相关的权重，并计算出基准查找分项的得分。基准查找分项得分的范围在0至100之间。同样的方法适用于攻击界面和环境度量指标组；其分项得分的范围在0至1之间。最后三项分项得分相乘，得出范围在0至100之间的CWSS得分，参见下文图2。

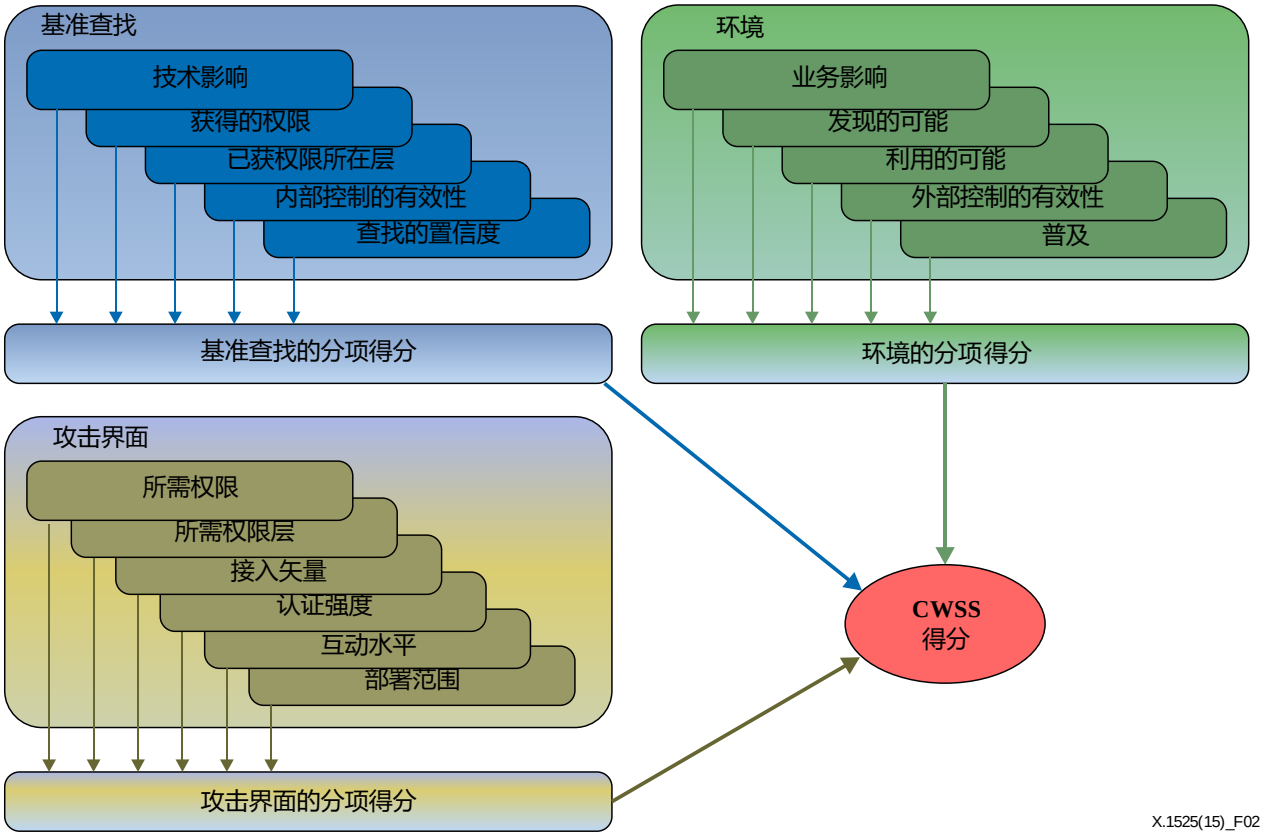

图 2 – CWSS评分

6.3 CWSS评分

利益攸关方团体目前正与MITRE协作调查可能需要在CWSS框架内为其提供支持的若干种不同评分方法。当前的四种评分方法如下：

定向评分法　对在特定（“定向”）软件包的设计或实施过程中发现的独立弱点进行评分，例如，某FTP服务器包内server.c 的第1234行，以及认证例行程序用户名出现的缓冲溢出。自动化工具和软件安全顾问在评估软件包的弱点时使用定向评分法。

通用评分法　对独立于任何具体软件包的弱点类别进行评分，以确定其相互之间的优先级（例如“缓冲溢出的优先级高于内存泄漏”）。此方法由CWE/SANS Top 25，OWASP Top Ten和类似工具使用，但同时亦为部分自动编码扫描程序所用。通常评分法可能与定向评分法大相径庭，需要对特定软件包内弱点类别单独出现的情况开展全面分析。例如，尽管缓冲溢出类别对众多开发商而言依然十分重要，但如果攻击者无法直接引起单独缓冲溢出缺陷，则可认为此类缺陷级别稍低，其影响会因操作系统（OS）层面保护机制 – 如地址空间布局随机化，而下降。

依背景面调整的评分法　依据诸如可能将业务/任务重点、威胁环境、风险容差等因素考虑在内的特定分析背景的需求，对评分做出调整。了解这些需求，使用了将弱点内在特性与高层业务考虑建立关联的vignette。此方法可同时适用于定向及通用评分。

集总评分法　将多个软件层级的弱点评分结合在一起，得出单一的总体得分（或“级别”）。虽然集总方式主要适用于定向评分法，但它亦可用于通用评分，如2010 CWE/SANS Top 25。

请注意，目前多数有关CWSS的讨论聚焦于定向评分法和根据背景进行调整的评分框架。集总评分法的关注度次之。通用评分法仍在独立开发，主要作为2011 Top 25和CWRAF的构成部分。

CWSS得分可自动计算，例如使用编码分析工具计算，同时亦可由软件安全顾问或开发者手动计算得出。鉴于自动分析不可能获取某些信息 – 例如应用的操作环境 – 因此可能实施多轮CWSS评分：首先由工具自动计算CWSS得分，然后由分析人员手动加入补充细节，并重新计算得分。

6.4 CWSS用户

为实现最高的效率，CWSS支持不同利益攸关方使用多种方法，鉴于软件弱点可能给其产品、系统、网络和服务带来风险，这些利益攸关方均有兴趣采用一种可将软件弱点优先级进行排序且表现一致的评分系统。下面介绍了一种主要利益攸关方的示例：

- 软件开发者：由于发布周期和资源的限制，软件开发者经常要在有限的时间内操作。因此，他们未能调查并解决所有上报的弱点。这些开发者可能会选择集中处理最严重、最易解决的问题。对于自动弱点查找，软件开发者可能会专注于出现误报概率最低的发现。
- 软件开发经理：软件开发经理负责制定优先级战略，将某些弱点类别从整个编码库中删除，或至少将最危险的部分删除，可以使用的方法包括定义“Top-N”的定制清单。他们必须了解集成可能存在自身弱点的第三方软件给安全造成的影响，且可能需要支持各生产线制定特有的安全要求和优先级。
- 软件采购者：包括采购人员在内的客户，希望采购的第三方软件具有合理水平的保障，且软件提供方已为删除或避免可能会给采购方业务和任务造成重大影响的弱点开展了尽职调查。此方面的利益攸关方包括首席信息官（CIO）、首席安全官（CSO）、系统管理员和软件最终用户。
- 企业安全经理：企业安全经理谋求尽量降低企业内部的风险，其中既包括第三方产品已为人熟知的漏洞，也包括其自身内部开发软件的漏洞（或弱点）。他们可能希望使用与其它安全管理程序集成的评分机制，例如将第三方漏洞扫描结果（针对已知的第三方漏洞）与定制的应用分析（针对内部软件）结合，用以帮助评估给某项资产造成的总体风险。
- 代码分析供应商和顾问：供应商和顾问通常具有自行定制的评分技术，但其希望为不同客户提供一种统一的、经相关团体审查的评分机制。
- 代码分析能力的评估者：评估者负责分析和衡量代码分析技术的能力（例如，NIST SAMATE）。他们可以使用统一的弱点评分机制，支持对结果上报机制实施抽检，同时还可了解这些发现的严重性，而无需依赖可能会因工具/技术上的巨大差异而导致不同结果的特别评分方法。
- 其它利益攸关方：其它利益攸关方可能包括漏洞研究者、安全开发的提倡者和以确保一致性为使命的分析人员（例如，PCI DSS）。

截至2014年6月（CWSS 0.8投入使用），已有多个投入实战的CWSS。其主要用户为代码分析供应商和软件安全顾问。

7 度量指标组

7.1 度量指标组的各项要素

CWSS包含以下按表1所示度量指标组划分的要素。后面各节更加详尽地描述了各项要素。

表 1 – 度量指标组的各项要素

组名	要素名称	摘要
基准查找	技术影响（TI）	在假设弱点可被成功发现并利用的情况下，该弱点可能产生的结果。
	获得的权限（AP）	攻击者获得的可成功利用软件弱点的权限类别。
	已获权限所在层（AL）	攻击者获得的、可成功利用软件弱点的权限类别所在的操作层。
	内部控制的有效性（IC）	使攻击者无法利用弱点的控制能力。
	查找的置信度（FC）	是否可相信上报问题是一种能被攻击者利用的弱点。
攻击界面	要求的权限（RP）	攻击者必须拥有的、用于获取含有弱点代码/功能的权限类型。
	要求的权限所在层（RL）	为实现攻击弱点的企图，攻击者必须拥有权限的操作层。
	接入矢量（AV）	攻击者必须通过其通信以获取相关代码或功能的通道。
	认证强度（AS）	负责保护包含弱点的代码/功能的认证例行程序的强度。
	互动水平（IN）	受害人要求采取的，为实施成功攻击开展的行动。
	部署范围（SC）	规定弱点是存在于所有可部署的软件实例，还是仅限于平台和/或配置的子集。
环境	业务影响（BI）	如果弱点被成功利用，可能会给业务或任务造成的潜在影响。
	发现的可能性（DI）	攻击者能够发现弱点的可能性。
	被利用的可能性（EX）	一旦弱点被发现，具备要求的权限/认证/接入水平的攻击者能够成功对其加以利用的可能性。
	外部控制的有效性（EC）	软件以外的控制或缓解能力，可增加攻击者获取和/或触发弱点的难度。
	流行程度（P）	此类弱点在软件中出现的频率。

7.2 不确定性和灵活性的数值

首先CWSS可在信息量很少的情况下使用，但信息的质量可随时间的推移提高。据预测，在许多使用案例中，随着更多信息的出现，CWSS针对单独弱点的评分可能会经常变化。不同实体或在不同时间点评估单独的因素。

由于上述原因，每项CWSS因素均有效地拥有“环境”或“时间”特性，因此采用与CVSS中所用度量指标组类型相同的度量指标组做用不大。

表2所述大多要素都具有四项共同值。

表 2 – 不确定性和灵活性的要素值

要素值	使用
未知	计算得分的实体没有为该要素提供要素值所需的足够信息。这可作为开展深入调查的信号。例如，自动代码扫描程序可找到某些弱点，但却无法检测到认证机制是否到位。 “未知”要素的使用强调评分并不完整或为估计值，可能有必要开展进一步分析。据此将为不完整的信息建模，使“业务值背景”可对由不完整信息生成的最终得分施加影响。 对所有要素而言，此值的权重为0.5，因此通常会生成更低的得分；增加新的信息（即将部分要素从“未知”改为其它值）将成为得分上下调整的依据。
不适用	计算得分的过程中明确规定要忽略此要素。这将切实有效地允许“业务值背景”决定某项要素是否与最终得分相关。例如，以客户为中心的CWSS评分方法可能会忽略为拯救而付出的努力，且具有高保障水平的环境可能会要求对所有上报的发现开展调查，即便其精度的置信度不高。 对于独立软件包的一系列弱点而言，预计所有研究的发现均为被忽略的要素设置了相同的“不适用”值。
定量	可使用连续范围在0.0 至1.0的定量值为该要素加权，而不使用该要素已定义的离散值集。并非所有要素均可以此种方式量化，但它可对度量进行更多定制。
缺省	该要素的权重可设置为缺省值。将该要素标记为缺省，为调查和今后可能的修改提供了余地。

7.3 基准查找度量指标组

基准查找度量指标组包含以下要素：

- 技术影响（TI）
- 获得的权限（AP）
- 已获权限所在层（AL）
- 内部控制的有效性（IC）
- 查找的置信度（FC）

技术影响、获得的权限和已获权限所在层等要素值的结合，为用户提供了看得到的权利。例如，用户可通过在“应用”层赋予“管理员”权限的方式描述“高”技术影响。

7.3.1 技术影响（TI）

技术影响是指假设弱点可被成功发现并利用的情况下，相关弱点可能产生的结果。此结果的表述使用了比保密性、完整性和可用性更详细的说明。

应根据获得的权限（AP）和已获权限所在层（AL）对技术影响做出评估。

表 3 – 技术影响的权重

值	代码	权重	说明
关键	C	1.0	完全控制受分析的软件，使各项操作无法执行。
高	H	0.9	在很高程度上控制了受分析的软件，或能获得访问关键信息的权利。
中	M	0.6	在中等程度上控制了受分析的软件，或能够获得访问中等重要信息的权利。
低	L	0.3	在最低程度上控制了受分析的软件，或仅能获得访问相对不重要信息的权利。
无	N	0.0	对受分析的软件不产生任何技术影响。换言之，这不会产生漏洞。
缺省	D	0.6	缺省权重是指“关键”、“高”、“中”、“低”和“无”的权重平均值。
未知	UK	0.5	没有足够的信息为此要素提供数值。可能需要进一步分析。将来可能需要选择不同的数值，并因此对得分产生影响。
不适用	NA	1.0	此要素被有意忽略，因为它与评分者如何确定弱点的优先级不相关。此要素可能不适用于有高保障要求的环境；用户可能希望调查每种令人感兴趣的弱点，无论其置信度如何。
定量	Q		此要素可通过定制的权重量化。

如果这些要素值不够精确，CWSS用户可使用其自己的定量方法推导出分项得分。此类方法之一涉及使用公共弱点风险分析框架（CWRAF）[b-CWRAF]定义一个vignette和技术影响得分卡。影响的权重计算可使用针对不同技术影响、按vignette划分的重要性评级，这些影响可能源自对弱点的利用，例如修改敏感数据、取得权限、资源消耗等。

7.3.2 获得的权限（AP）

获得的权限确定了攻击者获得的、可成功利用软件弱点的权限类别。

请注意这些数值与要求的权限使用的数值相同，但权重不同。

在某些情况下，获得的权限值可能与要求的权限使用的要素值相同，这意味着（1）“水平”权限的提升（例如从一个无权限的用户转给另一个）或（2）在同一沙盘软件内提升权限等级，例如文件传输协议（FTP）– 唯一能够逃离外壳程序的用户。

表 4 – 获得的权限所占权重

值	代码（注）	权重	说明
管理员	A	1.0	攻击者可用管理员、根、系统（SYSTEM）或其它相等的权限访问某实体，对受分析的软件拥有完全的控制；或攻击者可将其自身（较低）的权限提高为管理员权限。
拥有部分权限的用户	P	0.9	攻击者可用某些特殊权限访问某实体，但其权限还不够管理员权限；或攻击者可将其自身（较低）的权限提高、升级为拥有部分权限的用户。例如，某用户有权进行备份，但不能修改软件的配置或安装更新。
常规用户	RU	0.7	攻击者访问无特殊权限的常规用户（实体）；或攻击者可将其自身（较低）的权限提高为常规用户权限。
受限/ 访客	L	0.6	攻击者访问受限或具有“访客” 身份的实体，此类实体可开展的活动受到很大限制；或攻击者可将其自身（较低）的权限提高为访客权限。注：此数值并不指虚拟主机中的“访客操作系统”概念。
无	N	0.1	攻击者无法获得更多额外的权限。（请注意，此值在受限环境下有用，在此环境下攻击者可逃避沙盘软件或其它受限环境，但仍无法获得额外的权限，或作为其它用户取得接入。）
缺省	D	0.7	“无”、“访客”、“常规用户”、 “拥有部分权限的用户”和“管理员” 的权重平均值。
未知	UK	0.5	没有足够的信息为此要素提供数值。可能需要进一步分析。将来可能需要选择不同的数值，并因此对得分产生影响。
不适用	NA	1.0	此要素被有意忽略，因为它与评分者如何确定弱点的优先级不相关。此要素可能不适用于有高保障要求的环境；用户可能希望调查每种令人感兴趣的弱点，无论其置信度如何。
定量	Q		此要素可通过定制的权重量化。请注意，定量数值是完整的；但鉴于权限且用户为离散的实体，定量模式可发挥作用的环境可能有限。
注 – 此要素主要值的缩写为“RUNLAP”（即“常规用户”、“无”、“受限”、“管理员”和“部分权限”）。			

7.3.3 已获权限所在层（AL）

已获权限所在层确定了攻击者获得的、可成功利用软件弱点的权限类别所在的操作层。

表 5 – 已获权限所在层的权重

值	代码（注）	权重	说明
应用	A	1.0	攻击者在接受分析的软件内得到受支持的权限。（如果接受分析的软件是底层系统的基本组成部分，例如操作系统的核心，则系统值可能更为恰当。）
系统	S	0.9	攻击者获取了底层系统的权限或运行接受分析软件的物理主机的接入权限。
网络	N	0.7	攻击者获得了接入网络的权限。
企业基础设施	E	1.0	攻击者获得了接入某种关键企业基础设施的权限，例如路由器、交换机、域名系统（DNS）、域控制器、防火墙、身份服务器等。
缺省	D	0.9	“应用”、“系统”、“网络”和“企业基础设施”权重的平均值。
未知	UK	0.5	没有足够的信息为此要素提供数值。可能需要进一步分析。将来可能需要选择不同的数值，并因此对得分产生影响。
不适用	NA	1.0	此要素被有意忽略，因为它与评分者如何确定弱点的优先级不相关。 此要素可能不适用于有高保障要求的环境，因为此类环境希望严格执行权限分离，即使是在已取得权限的用户之间。
定量	Q		此要素可通过定制的权重量化。请注意，定量数值是完整的；但鉴于权限且用户为离散的实体，定量模式可发挥作用的环境可能有限。
注 – 此要素主要数值的缩写为“SANE”（即“系统”、“应用”、“网络”和“企业基础设施”）。			

7.3.4 内部控制的有效性（IC）

内部控制是一种控制和保护机制，或软件内构造的压力缓解措施（可通过构架、设计或实施实现）。内部控制的有效性衡量的是使攻击者无法利用弱点的能力。例如，将输入长度限制在15个字符以内的输入验证例行程序，通过减少XSS可尝试攻击的范围，在减少跨网站脚本攻击（XSS）方面发挥了中等效力。

若存在多种内部控制或可利用同一弱点的多个代码路径，则以下指南适用：

- 针对各代码路径，对代码路径上的各种内部控制加以分析，选择权重最低的值（即代码路径上最强的内部控制）。该值的名称为代码路径值。
- 收集所有代码路径值。
- 选择权重最高的代码路径值（即控制力最低的值）。

此方法从控制力最强的代码路径角度对各代码路径进行了评估（鉴于某攻击者必须避开控制），然后选择最弱的代码路径（即攻击者最容易使用的路径）。

表 6 – 内部控制的有效性权重

值	代码	权重	说明
无	N	1.0	不存在控制。
有限	L	0.9	使用简单或随机限制，或能防止偶然攻击者利用相关弱点。
中等	M	0.7	此保护机制被普遍使用，但其已知的限制可能为有经验的攻击者利用，用于避开保护。例如，使用超文本标识语言（HTML）实体编码防止XSS攻击，若输出被放入级联类型表格或HTML标记属性等其它背景之下，则此机制可能会被避开。
间接（深层保护）	I	0.5	此控制并不具体用于防止弱点被利用，而是间接降低成功攻击造成的影响，或增加构成功能性利用的难度。例如，验证例行程序可能间接限制输入的大小，从而可能提高攻击者构建XSS或结构化查询语言（SQL）插入式攻击净荷的难度。
最佳可用	B	0.3	此种控制遵循最佳现行做法，尽管它可能仍受到部分限制，会被高水平、有决心的攻击者攻克，但这可能需要存在其它弱点。例如，为防止跨网站请求伪造（CSRF）制定的双重提交法被认为是最强的可用方法之一，但若能同时利用可读取原始HTTP报头的某些功能，则该方法可能会失效。
完美	C	0.0	此控制能够完全控制各种弱点，即不存在缺陷或漏洞，且不会因利用产生不良后果。例如，缓冲拷贝操作可确保目的地的缓冲器永远大于源头的缓冲器（亦包括任何源头缓冲数量的间接扩容），因此不会产生溢出。
缺省	D	0.6	“完美”、“最佳可用”、“间接”、“中等”、“有限”和“无”等权重的平均值。
未知	UK	0.5	没有足够的信息为此要素提供数值。可能需要进一步分析。将来可能需要选择不同的数值，并因此对得分产生影响。
不适用	NA	1.0	此要素被有意忽略，因为它与评分者如何确定弱点的优先级不相关。
定量	Q		此要素可通过定制的权重量化。

7.3.5 查找的置信度（FC）

查找的置信度是指上报问题的可信程度：

1) 为一种弱点，且

2) 可被攻击者触发或使用。

表 7 – 查找的置信度权重

值	代码	权重	说明
真实性得到证实	T	1.0	攻击者可利用该弱点。
真实性得到部分证实	LT	0.8	相关弱点出现在某项功能或组件中，这些功能或组件的设计有赖于该功能的安全启动，但目前攻击者是否可利用该功能尚未可知或该功能尚不存在。例如，某实用功能可能在不对输入加密的情况下提出数据库查询，但如果仅使用恒定字符串调用，其发现的结果在局部具有真实性。
虚假性得到证实	F	0.0	发现存在错误（即发现为误报且不存在弱点），和/或不可能存在攻击者。
缺省	D	0.8	“真实性得到证实”、“真实性得到部分证实”和“虚假性得到证实”权重的平均值。
未知	UK	0.5	没有足够的信息为此要素提供数值。可能需要进一步分析。将来可能需要选择不同的数值，并因此对得分产生影响。
不适用	NA	1.0	此要素被有意忽略，因为它与评分者如何确定弱点的优先级不相关。 此要素可能不适用于有高保障要求的环境；用户可能希望调查每种令人感兴趣的弱点，无论其置信度如何。
定量	Q		此要素可通过定制的权重量化。有些代码分析工具拥有具体探测模式的精确测量值。

7.4 攻击界面度量指标组

攻击界面的度量指标组包括如下要素：

- 要求的权限（RP）
- 要求的权限所在层（RL）
- 接入矢量（AV）
- 认证强度（AS）
- 互动水平（IN）
- 部署范围（SC）。

7.4.1 要求的权限（RP）

要求的权限确定了攻击者必须拥有的、用于获取含有弱点代码/功能的权限类型。

表 8 – 要求的权限权重

值	代码（注）	权重	说明
无	N	1.0	不需要权限。例如，一种基于网络的搜索引擎在搜索术语并查看结果时，可能不需要相关实体具有任何权限。
受限/访客	L	0.9	该实体拥有有限或“访客” 权限，可大幅限制允许开展的活动；该实体或能够注册或创建新的账户，而无需为身份提供任何特殊的要求或证明。例如，网络博客可能允许博主在发表评论前创建一个用户名并提供有效的电子邮件地址。注：此数值并不指虚拟主机中的“访客操作系统”概念。
常规用户	RU	0.7	此实体为无特殊权限的常规用户。
拥有部分权限的用户	P	0.6	此实体为拥有部分特殊权限的有效用户，但其权限还不够管理员权限。例如，某用户有权进行备份，但不能修改软件的配置或安装更新。
管理员	A	0.1	此实体拥有管理员、根、系统（SYSTEM）或其它相等权限，这也意味着其对接受分析的软件或底层操作系统拥有完全的控制。
缺省	D	0.7	“无”、“受限”、“常规用户”、“拥有部分权限的用户”和“管理员”权重的平均值。
未知	UK	0.5	没有足够的信息为此要素提供数值。可能需要进一步分析。将来可能需要选择不同的数值，并因此对得分产生影响。
不适用	NA	1.0	此要素被有意忽略，因为它与评分者如何确定弱点的优先级不相关。 此要素可能不适用于有高保障要求的环境，因为此类环境希望严格执行权限分离，即使是在已取得权限的用户之间。
定量	Q		此要素可通过定制的权重量化。请注意，定量数值是完整的；但鉴于权限且用户为离散的实体，定量模式可发挥作用的环境可能有限。
注 – 此要素主要数值的缩写为“RUNLAP”（“常规用户”、“无”、“受限”、“管理员”和“拥有部分权限”）。			

7.4.2 要求的权限所在层（RL）

要求的权限所在层确定了为实现攻击弱点的企图，攻击者必须拥有权限的操作层。

表 9 – 要求的权限所在层的权重

值	代码（注）	权重	说明
应用	A	1.0	攻击者必须拥有在接受分析的软件内得到支持的权限。（如果接受分析的软件是底层系统的基本组成部分，例如操作系统的核心，则系统值可能更为恰当。）
系统	S	0.9	攻击者必须获取底层系统的权限或运行接受分析软件的物理主机的接入权限。
网络	N	0.7	攻击者必须已获得接入网络的权限。
企业基础设施	E	1.0	攻击者必须获得接入某种关键企业基础设施的权限，例如路由器、交换机、域名系统（DNS）、域控制器、防火墙、身份服务器等。
缺省	D	0.9	“应用”、“系统”、“网络”和“企业基础设施”的权重平均值。
未知	UK	0.5	没有足够的信息为此要素提供数值。可能需要进一步分析。将来可能需要选择不同的数值，并因此对得分产生影响。
不适用	NA	1.0	此要素被有意忽略，因为它与评分者如何确定弱点的优先级不相关。 此要素可能不适用于有高保障要求的环境，因为此类环境希望严格执行权限分离，即使是在已取得权限的用户之间。
定量	Q		此要素可通过定制的权重量化。请注意，定量数值是完整的；但鉴于权限且用户为离散的实体，定量模式可发挥作用的环境可能有限。
注 – 此要素主要数值的缩写为“SANE”（“系统”、“应用”、“网络”和“企业基础设施”）。			

7.4.3 接入矢量（AV）

接入矢量确定了攻击者必须通过其通信以获取相关代码或功能的通道。请注意，这些数值与CVSS中使用的值极为相似，但CWSS区分物理接入和本地（外壳/账户）接入。

尽管接入矢量与要求的权限所在层存在密切关系，但这两者有明显区别。例如，可获得路由器“物理”接入的攻击者，或许能够影响网络或企业层。

表 10 – 接入矢量的权重

值	代码	权重	说明
互联网	I	1.0	攻击者必须接入互联网才能利用弱点。
内部网	R	0.8	攻击者必须接入不与互联网直接相连（例如使用防火墙）的企业内部网，但内网可供企业大多数成员使用。
专网	V	0.8	攻击者必须接入仅供少数特定受信方使用的专网。
相邻网络	A	0.7	攻击者必须能够接入相关网络的物理接口，例如存在漏洞的软件广播或冲突域。本地网络示例包括本地IP子网、蓝牙、IEEE 802.11以及本地以太网部分。
本地	L	0.5	攻击者必须有互动、本地（外壳）账户与底层操作系统直接相连。
物理	P	0.2	攻击者必须能够物理接入运行软件的系统，或通过通用串型总线（USB）、光盘（CD）、键盘、鼠标等接口与系统互动。
缺省	D	0.75	相关值权重的平均值。
未知	U	0.5	
不适用	NA	1.0	此要素被有意忽略，因为它与评分者如何确定弱点的优先级不相关。
定量	Q		此要素可通过定制的权重量化。此要素可通过定制的权重量化。请注意，定量数值是完整的；但鉴于权限且用户为离散的实体，定量模式可发挥作用的环境可能有限。

7.4.4 认证强度（AS）

认证强度是指负责保护包含弱点的代码/功能的认证例行程序的强度。

如果认证例行程序达一个以上，或存在两个或多个代码路径，则应按下述方式评分：

若存在多种认证例行程序或可利用同一弱点的多个代码路径，则以下指南适用：

- 针对各代码路径，对代码路径上的各种认证例行程序加以分析，选择权重最低的值（即代码路径上最强的内部控制）。该值的名称为代码路径值。
- 收集所有代码路径值。
- 选择权重最高的代码路径值（即控制力最弱的例行程序）。

此方法从代码路径上最强的认证例行程序的角度对各代码路径进行了评估（鉴于某攻击者必须避开控制），然后选择最弱的代码路径（即攻击者最容易使用的路径）。

表 11 – 认证强度的权重

值	代码	权重	说明
强	S	0.7	此类弱点要求使用最强方法将相关实体与现实世界的身份联系在一起，例如基于硬件的令牌，和/或多要素认证。
中	M	0.8	此类弱点要求使用相对较强的方法认证，例如使用来自不受信任认证机构的证书、基于知识的认证或一次性口令。
弱	W	0.9	此类弱点要求使用简单、低强度的认证方法，通过欺诈、字典或重播攻击（例如静态口令）可轻易破解。
无	N	1.0	此类弱点无需任何认证。
缺省	D	0.85	“强”、“中”、“弱”和“无”等的权重平均值。
未知	UK	0.5	没有足够的信息为此要素提供数值。可能需要进一步分析。将来可能需要选择不同的数值，并因此对得分产生影响。
不适用	NA	1.0	此要素被有意忽略，因为它与评分者如何确定弱点的优先级不相关。 此值可能对谋求消除所有弱点的具有高保障要求的环境不适用。
定量	Q		此要素可通过定制的权重量化。

7.4.5 互动水平（IN）

互动水平定义了受害人要求采取的，实施成功攻击的行动。

表 12 – 互动水平的权重

值	代码	权重	说明
自动	A	1.0	无须操作者的互动。
典型/受限	T	0.9	攻击者必须让用户在典型产品操作过程中执行某项常见或被视作“正常” 的操作。例如，点击某网页上的链路或预览电子邮件正文均为常见行为。
中等	M	0.8	攻击者必须让用户执行一项使谨慎、有经验的用户觉得可疑的 操作。例如：用户必须接受攻击者净荷可能包含危险内容的提醒。
乐观	O	0.3	攻击者不能直接控制或影响受害方，只能被动地利用其错误或其它人的操作。
高	H	0.1	需要大量社会工程，其中可能包括受害者的无知与疏忽。
无互动	NI	0.0	没有进行互动的可能，甚至是偶然的互动；通常这会使弱点成为"缺陷"而不会形成漏洞。鉴于CWSS是用于安全，因此其权重为0。
缺省	D	0.55	“自动”、“受限”、“中等”、“乐观”、“高”和“无” 互动的平均值。
未知	UK	0.5	没有足够的信息为此要素提供数值。可能需要进一步分析。将来可能需要选择不同的数值，并因此对得分产生影响。

7.4.6 部署范围（SC）

部署范围确定了弱点是存在于所有可部署的软件实例，还是仅限于平台和/或配置的子集。例如，数字计算错误仅适用于在特定OS和64位架构下运行的软件，或路径遍历问题只会影响“\”为目录分隔符的操作系统。

表 13 – 部署范围权重

值	代码（注1）	权重	说明
全部	A	1.0	存在于所有平台和配置内
适量	M	0.9	存在于公共平台和配置内
罕见	R	0.5	仅存在于极少见的平台和配置内
有可能达到	P	0.1	有可能达到（注2），但所有代码路径目前都安全，且/或该弱点位于死码内
缺省	D	0.7	RAMP值权重的平均值
未知	UK	0.5	没有足够的信息为此要素提供数值。可能需要进一步分析。将来可能需要选择不同的数值，并因此对得分产生影响。
不适用	NA	1.0	此要素被有意忽略，因为它与评分者如何确定弱点的优先级不相关。
定量	Q		此要素可通过定制的权重量化。用户可能知晓包含此缺陷的已发货（或支持）软件所占比例。
注 1 – 此要素主要数值的缩写为“RAMP”（“罕见”、“全部”、“适量”和“有可能达到”）。 注 2 – “有可能达到”与查找的置信度（FC）要素中的“真实性得到部分证实”重叠。			

7.5 环境度量指标组

环境度量指标组包含以下要素：

- 业务影响（BI）
- 发现的可能性（DI）
- 被利用的可能性（EX）
- 外部控制的有效性（EC）
- 流行程度（P）。

7.5.1 业务影响（BI）

业务影响阐述了如果弱点被成功利用，可能会给业务或任务造成的潜在影响。

注 – 鉴于不同组织间的业务关切大不相同，CWSS 1.0无意提供更加精确的细分，例如从财务、声望、实体、法律或其它类型损害的角度进行细分。可以对此要素加以定量，以为外部定义的模型提供一切支持。

表 14 – 业务影响的权重

值	代码	权重	说明
关键	C	1.0	业务/任务可能会失败。
高	H	0.9	业务/任务的操作将受到严重影响。
中	M	0.6	业务/任务会受到影响，但不会给正常操作带来广泛影响。
低	L	0.3	对业务/任务产生最低级别的影响。
无	N	0.0	无影响。
缺省	D	0.6	“关键”、“高”、“中”、“低”和“无”的权重平均值。
未知	UK	0.5	没有足够的信息为此要素提供数值。可能需要进一步分析。将来可能需要选择不同的数值，并因此对得分产生影响。
不适用	NA	1.0	此要素被有意忽略，因为它与评分者如何确定弱点的优先级不相关。 此要素在业务影响不相关的背景下不适用，另一种不适用的情况为分析进程中评估和考虑的影响不在CWSS评分的范围内。
定量	Q		此要素可通过定制的权重量化。有些机构可能对资产业务价值有特定的测量方法，例如，哪些内容可纳入此测量之中。

7.5.2 发现的可能性（DI）

发现的可能性是指攻击者能够发现弱点的可能性。

注 – 曾考虑将此要素从CWSS 1.0中取消，因为它很难衡量且会受获得的权限、技术影响和流行程度等其它因素的影响。但是，目前仍然保留了这一要素意味着有些开发商将使用“发现的可能性”帮助确定解决某些问题的优先级。

表 15 – 发现的可能性所占权重

值	代码	权重	说明
高	H	1.0	攻击者很可使用简单的技术，轻易迅速地发现弱点，无需使用源代码或其它简化弱点探测的人工手段。
中	M	0.6	攻击者或许能够发现弱点，但可能需要某些技能，可能要求使用源代码接入或逆向工程的知识。发现问题可能需要一些时间。
低	L	0.2	没有高水平专业技能、访问源代码（或相应代码）和很长的时间，攻击者不可能发现弱点。
缺省	D	0.6	“高”、“中”、“低”的权重平均值。
未知	UK	0.5	没有足够的信息为此要素提供数值。可能需要进一步分析。将来可能需要选择不同的数值，并因此对得分产生影响。
不适用	NA	1.0	此要素被有意忽略，因为它与评分者如何确定弱点的优先级不相关。 如果评分者假设攻击者能够发现所有弱点，此可能不适用。
定量	Q		此要素可通过定制的权重量化。

7.5.3 被利用的可能性（EX）

被利用的可能性是指，一旦弱点被发现，具备要求的权限/认证/接入水平的攻击者能够成功对其加以利用的可能性。

表 16 – 被利用的可能性的权重

值	代码	权重	说明
高	H	1.0	某攻击者很可能利用易于开发且可靠的弱点利用机制，成功地攻击相关弱点。
中	M	0.6	攻击者可能成功攻击相关弱点，但成功的机率不同，或需要尝试多次方能成功。
低	L	0.2	攻击者可能不会攻击此弱点，或成功的概率很低。
无	N	0.0	攻击者不可能成功；即该问题是一个“缺陷”，因为它与攻击者并无关系且攻击者不会从中获益。
缺省	D	0.6	“高”、“中”、“低”的权重平均值。鉴于极少有弱点使用“无”值进行评分，因此该值被忽略，且将其纳入平均值的计算将把权重降低至非直观的水平。
未知	UK	0.5	没有足够的信息为此要素提供数值。可能需要进一步分析。将来可能需要选择不同的数值，并因此对得分产生影响。
不适用	NA	1.0	此要素被有意忽略，因为它与评分者如何确定弱点的优先级不相关。 例如，评分者可能希望假设攻击者能够利用能够找到的所有弱点，或希望投入大量资源消除可能阻碍其取得成功的障碍。
定量	Q		此要素可通过定制的权重量化。

请注意此要素受弱点的影响，因为攻击者经常以影响最为严重的弱点为目标。另外，他们亦可能以易于触发的弱点为目标。同时，它还受到内部和外部控制有效性等其它要素的影响。

似乎流行程度亦是一种影响因素，流行程度与发现的可能性的关系更为密切。

7.5.4 外部控制的有效性（EC）

外部控制的有效性是指软件以外的控制或缓解能力，可增加攻击者获取和/或触发弱点的难度。例如，地址空间布局随机化（ASLR）且类似的技术会降低，但不会彻底消除缓冲溢出攻击取得成功的可能性。但是，ASLR不会直接在软件内部显示。

若存在多种外部控制或可利用同一弱点的多个代码路径，则以下指南适用：

- 针对各代码路径，对代码路径上的各种外部控制加以分析，选择权重最低的值（即代码路径上最强的外部控制）。该值的名称为代码路径值。
- 收集所有代码路径值。
- 选择权重最高的代码路径值（即控制力最低的值）。

此方法从控制力最强的代码路径角度对各代码路径进行了评估（鉴于某攻击者必须避开控制），然后选择最弱的代码路径（即攻击者最容易使用的路径）。

表 17 – 外部控制有效性的权重

值	代码	权重	说明
无	N	1.0	不存在控制。
有限	L	0.9	使用简单或随机限制，或能防止偶然攻击者利用相关弱点。
中等	M	0.7	此保护机制被普遍使用，但其已知的限制可能被有经验的攻击者用于避开保护。
间接 （深层保护）	I	0.5	此控制并不具体用于防止弱点被利用，而是间接降低成功攻击造成的影响，或增加构成功能性利用的难度。例如，地址空间布局随机化（ASLR）且类似的技术会降低，但不会彻底消除缓冲溢出攻击取得成功的可能性。鉴于响应方式一般为退出进程，相关结果仍然是拒绝服务。
最佳可用	B	0.3	此种控制遵循最佳现行做法，尽管它可能仍受到部分限制，会被高水平、有决心的攻击者攻克，但这可能需要存在其它弱点。例如，传输层安全性（TLS）/安全套接层（SSL 3）在大部分网络范围内均可操作，且由于兼容性问题通常无法提供更强的方法。
完美	C	0.1	此控制能够完全控制各种弱点，即不存在缺陷或漏洞，且不会因利用产生不良后果。例如，沙盘环境可能会将文件接入操作限制到一个工作目录下，此做法可防止对路径遍历的利用。 非零权重用于反映将来外部控制可能被偶然取消的可能性，例如在软件环境发生变化的情况下。
缺省	D	0.6	“完美”、“最佳可用”、“间接”、“中等”、“有限”和“无”的权重平均值。
未知	UK	0.5	没有足够的信息为此要素提供数值。可能需要进一步分析。将来可能需要选择不同的数值，并因此对得分产生影响。
不适用	NA	1.0	此要素被有意忽略，因为它与评分者如何确定弱点的优先级不相关。
定量	Q		此要素可通过定制的权重量化。

7.5.5 流行程度（P）

某种发现的流行程度确定了此类弱点在软件内出现的频率。

注 – 请注意可能会考虑在将来的版本中取消此要素。但是，它与通用评分方法和CWRAF联系过于密切，难以从CWSS 1.0中删除。

此要素拟在弱点类别通用评分中使用，例如定制Top-N弱点清单的开发。在自动扫描背景下对单独的弱点发现进行评分时，此要素可能会使用“不适用”值。

表 18 – 流行程度的权重

值	代码	权重（注）	说明
广泛流行	W	1.0	此弱点存在于相关环境中的全部或多数软件内，在同一软件包内可能会出现多次。
高	H	0.9	此弱点会经常遇到，但并未广泛流行。
普通	C	0.8	此类弱点会定期遇到。
受限	L	0.7	此类弱点很少遇到。
缺省	D	0.85	“受限”、“普通”、“高”和“广泛流行”的平均权重。
未知	UK	0.5	没有足够的信息为此要素提供数值。可能需要进一步分析。将来可能需要选择不同的数值，并因此对得分产生影响。
不适用	NA	1.0	此要素被有意忽略，因为它与评分者如何确定弱点的优先级不相关。 针对某应用特定弱点的发现进行定向评分时，流行程度通常不相关，因为独立的应用和分析技术可判定弱点出现的频率，且诸多集总评分方法在弱点更多的情况下会生成更高的得分。
定量	Q		此要素可通过定制的权重量化。在有限的使用案例中，精确的流行程度数据或许可用，但前提是在低水平粒度的情况下对弱点数据进行跟踪。例如，软件开发者可能跟踪一系列产品的弱点，或代码审计厂商可衡量整个客户库内接受分析软件的流行程度。在上一版的CWSS中，流行程度的计算是基于针对2010年Top 25采集的原始投票数据，这些数据使用后被调整至1至10范围的离散值（原来为1-4）。
注 – 鉴于即便在只存在单一弱点的情况下仍能成功攻击该软件，选定的权重相互间并无明显的区别。			

7.6 CWSS评分公式

CWSS 1.0得分的范围在0至100之间。其计算公式如下：

BaseFindingSubscore * AttackSurfaceSubscore * EnvironmentSubscore

BaseFindingSubscore支持的值在0至100之间。AttackSurfaceSubscore和EnvironmentSubscore支持的数值都在0至1之间。

7.6.1 基准查找分项得分

基准查找分项得分（BaseFindingSubscore）的计算公式如下：

```
Base = [ (10 * TechnicalImpact + 5*(AcquiredPrivilege + AcquiredPrivilegeLayer)
+ 5*FindingConfidence) * f(TechnicalImpact) * InternalControlEffectiveness ] * 4.0

f(TechnicalImpact) = 0 if TechnicalImpact = 0; otherwise f(TechnicalImpact) = 1.
```

BaseFindingSubscore得分的最大值为100。

f(TechImpact）的定义在CVSS存在一个对等提法。此定义用于确保在技术影响为0的情况下，其它新增要素将不经意地生成非零得分。

TechnicalImpact和AcquiredPrivilege/AcquiredPrivilegeLayer组合的权重相同，各占BaseFindingSubscore的40%（每种组合所生成子值的最大数值为10）。查找的置信度会有一些调整，占基准值的20%（最大值为5）。InternalControlEffectiveness可向下调整得分，或者将其调整为0，但这要视应用的内部控制强度而定。应用InternalControlEffectiveness之后，结果可能的范围在0-25之间，因此要使用4.0的系数将BaseFindingSubscore调整到0至100范围内。

7.6.2 攻击界面的分项得分

攻击界面的分项得分（AttackSurfaceSubscore）的计算公式如下：

```
[ 20*(RequiredPrivilege + RequiredPrivilegeLayer + AccessVector) + 20*DeploymentScope + 15*LevelOfInteraction + 5*AuthenticationStrength ] / 100.0
```

要求的权限/接入占攻击界面分项得分的60%；部署范围占另外得分的20%；互动占15%；认证占5%。认证要求并未得到很高重视，其原因在于相关假设认为身份的严格认证不会明显遏制攻击者利用漏洞的企图。

此公式生成的值在0至100之间，之后再以100为除数求商。

7.6.3 环境分项得分

环境分项得分的计算公式如下：

```
[ (10*BusinessImpact + 3*LikelihoodOfDiscovery + 4*LikelihoodOfExploit + 3*Prevalence) * f(BusinessImpact) * ExternalControlEffectiveness ] / 20.0

f(BusinessImpact) = 0 if BusinessImpact == 0; otherwise f(BusinessImpact) = 1
```

BusinessImpact占环境得分的50%，且其可将最终得分变为0。ExternalControlEffectiveness总是非零（如果环境变化则其可对不经意取消的风险负责），但在其它方面该因素可对最终得分产生重大影响。LikelihoodOfDiscovery与LikelihoodOfExploit的组合占得分比例的35%，流行程度因素占15%。

7.6.4 该公式的其它特性

可表示的各类得分存在巨大的差异，尽管多种要素的组合与多种小数值权重的结合意味着潜在的得分范围在某种程度上向低值靠拢。

鉴于“不适用”的权重为1，该公式潜在的最高得分永远为100.0。在极为罕见的情况下，某些要素被作为不适用处理（例如，技术影响、业务影响和内部控制的有效性），此时最小的可能得分或者为非零值。

当缺省值被用于单一评分的众多要素时，如采用CWSS 1.0定义的平均权重，则得分将显著地向较低侧靠拢。某要素的平均权重并不一定会反映最可能使用的值，因此缺省权重的选择可能会在未来的版本中修改。理想条件下，该公式有一项属性内使用的多个缺省值会产生相对接近50的得分；选择非缺省值将向上或向下调整最终得分，从而增加精度。

使用“未知”值通常亦会得出向下靠拢的得分。这可能是一项有用特性，因为在没有具体信息的条件下，得分会偏高。

7.7 CWSS矢量、评分示例和得分的可携带性

使用为各要素制定的代码，CWSS得分可以一种压缩、机器分析且可人工读取的格式存储，提供有关评分产生的细节。这与CVSS矢量的构建十分类似。

与CVSS不同，并非CWSS要素均可用离散值加以象征性描述。所有要素均可使用连续权重定量，利用"Q" 值这些权重具有超越原始定义的缺省离散值的权限。在使用CWRAF计算时，影响要素是对32种独立技术影响和层面的有效表述，其中许多可能不适用于特定的弱点。将各种影响作为独立要素处理，几乎会使计算CWSS评分所需的要素加倍。此外，CWRAF使用“业务值背景”（BVC）调整针对具体业务的评分亦意味着CWSS得分及其矢量在“传送”至其它域或vignette的情况下，可能呈现出不一致。

考虑到这一关切，CWSS 1.0矢量应明确列出各要素的权重，尽管这会增大矢量呈现的尺寸。

CWSS矢量内单一要素的格式如下：

FactorName：值、权重

例如，"P:NA,1.0"为流行程度指定了“不适用”值，其权重为1.0。"AV:P,0.2"指示符指出了接入矢量的“物理”值，其权重为0.2。

各要素用正斜线分隔，例如：

```
AV:I,1.0/RP:G,0.9/AS:N,1.0
```

式中列出了“AV”（接入矢量）、“RP”（要求的权限水平）以及“AS”（认证强度）的值和权重。

如果一个CWSS矢量并未列出某值的实际权重，则实施应上报可能的差错或不一致，力求根据矢量要素的数值推导出CWSS版本，并根据推导出的版本重新计算CWSS得分，同时将其与原得分加以比较。如果得分前后并不一致，则实施应上报可能的差错或不一致。

7.7.1 示例：业务关键型应用

考虑到在上报的弱点中应用是相关公司的主要收入来源，因此该弱点具有关键的业务价值。该应用允许任意互联网用户仅用电子邮件地址签约账户。用户可利用相关弱点获得应用的管理员权限，但在管理员查看近期用户活动之前，攻击不可能取得成功-这是一种常见现象。攻击者不可能完全控制应用，但可能删除其用户和数据。进一步假设不存在可控制弱点的手段，但解决此问题很简单，且只需几行代码。

此情况可能出现在以下CWSS矢量中：

```
(TI:H,0.9/AP:A,1.0/AL:A,1.0/IC:N,1.0/FC:T,1.0/
RP:G,0.9/RL:A,1.0/AV:I,1.0/AS:N,1.0/IN:T,0.9/SC:A,1.0/
BI:C/0.9,DI:H,1.0/EX:H,1.0/EC:N,1.0/P:NA,1.0)
```

为实现可读性，该矢量已分解为多行。各行代表一个度量指标组。

相关要素和值如下文表19所示。

表 19 –业务关键型应用的要素和要素值示例

要素	值
技术影响	高
获得的权限	管理员
已获权限所在层	应用
内部控制的有效性	无
查找的置信度	真实性得到证实
要求的权限	访客
要求的权限所在层	应用
接入矢量	互联网
认证强度	无
互动水平	典型/受限
部署范围	全部
业务影响	关键
发现的可能性	高
被利用的可能性	高
外部控制的有效性	无
流行程度	不适用

此矢量的CWSS得分为92.6，其推导公式如下：

- BaseSubscore:
  - [(10 * TI + 5*(AP + AL) + 5*FC) * f(TI) * IC] * 4.0
  - f(TI) = 1
  - = [(10 * 0.9 + 5*(1.0 + 1.0) + 5*1.0) * 1 * 1.0] * 4.0
  - = [(9.0 + 10.0 + 5.0) * 1.0] * 4.0
  - = 24.0 * 4.0
  - = 96.0
- AttackSurfaceSubscore:
  - [20*(RP + RL + AV) + 20*SC + 15*IN + 5*AS] / 100.0
  - = [20*(0.9 + 1.0 + 1.0) + 20*1.0 + 15*0.9 + 5*1.0] / 100.0
  - = [58.0 + 20.0 + 13.5 + 5.0] / 100.0
  - = 96.5 / 100.0
  - = 0.965
- EnvironmentSubscore:
  - [(10*BI + 3*DI + 4*EX + 3*P) * f(BI) * EC] / 20.0
  - f(BI) = 1
  - = [(10*1.0 + 3*1.0 + 4*1.0 + 3*1.0) * 1 * 1.0] / 20.0
  - = [(10.0 + 3.0 + 4.0 + 3.0) * 1.0] / 20.0
  - = 20.0 / 20.0
  - = 1.0

最终得分为：

96.0 * 0.965 * 1.0 = 92.64 == 92.6

7.7.2 示例：业务关键性有限的Wiki

考虑此CWSS矢量。假设此软件为wiki软件，被中型企业用于跟踪社会活动。此矢量最重要的特性包括应用的常规用户会给应用管理员带来中等强度的技术影响，但该应用并非业务关键型应用，所以总体业务影响低。此外，亦请注意绝大多数环境要素被设置为“不适用”。

```
(TI:M,0.6/AP:A,1.0/AL:A,1.0/IC:N,1.0/FC:T,1.0/
RP:RU,0.7/RL:A,1.0/AV:I,1.0/AS:W,0.9/IN:A,1.0/SC:NA,1.0/
BI:L/0.3,DI:NA,1.0/EX:NA,1.0/EC:N,1.0/RE:NA,1.0/P:NA,1.0)
```

为实现可读性，该矢量已分解为多行。各行代表一个度量指标组。

相关要素和值如下文表20所示。

表 20 – 业务关键型应用的要素和要素值示例

要素	值
技术影响	中等
获得的权限	管理员
已获权限所在层	应用
内部控制的有效性	无
查找的置信度	真实性得到证实
要求的权限	常规用户
要求的权限所在层	应用
接入矢量	互联网
认证强度	弱
互动水平	自动
部署范围	不适用
业务影响	低
发现的可能性	不适用
被利用的可能性	不适用
外部控制的有效性	无
流行程度	不适用

此矢量的CWSS得分为51.1，其推导公式如下：

- BaseSubscore:
  - `[ (10 * TI + 5*(AP + AL) + 5*FC) * f(TI) * IC ] * 4.0`
  - `f(TI) = 1`
  - `= [ (10 * 0.6 + 5*(1 + 1) + 5*1) * f(TI) * 1 ] * 4.0`
  - `= 84.0`
- AttackSurfaceSubscore:
  - `[ 20*(RP + RL + AV) + 20*SC + 15*IN + 5*AS ] / 100.0`
  - `= [ 20*(0.7 + 1 + 1) + 20*1.0 + 15*1.0 + 5*0.9 ] / 100.0`
  - `= [ 54.0 + 20.0 + 15.0 + 4.5 ] / 100.0`

- = 93.5 / 100.0
- = 0.94 (0.935)

- EnvironmentSubscore:
  - [(10*BI + 3*DI + 4*EX + 3*P) * f(BI) * EC] / 20.0
  - f(BI) = 1
  - = [(10*0.3 + 3*1.0 + 4*1.0 + 3*1.0) * f(BI) * 1] / 20.0
  - = [(3.0 + 3.0 + 4.0 + 3.0) * 1.0 * 1.0] / 20.0
  - = [13.0 * 1.0] / 20.0
  - = 0.65

最终得分为：

```
84.0 * 0.935 * 0.65 = 51.051 == 51.1
```

7.7.3 实现CWSS得分便携性的其它方法

除记录CWSS矢量内各独立权重之外，还可采用其它方法。

一种可能性是扩展CWSS矢量，以记录不会影响得分但将反映版本或其它重要信息的补充元数据。相关元数据本身不必取得权重。例如，CWSS版本可用“要素”名称加数值表示CWSS的版本，例如“V:1.1”。这可能会给各CESS矢量增加约4个字节。但是，如果在矢量内对版本进行加密，则指配的权重便无需再记录（定量值除外），从而使最终矢量的尺寸大幅缩减。

另一种不同方法是将元数据随附在CWSS得分之后（例如，在使用CWRAF时提供技术影响得分卡），但此元数据与得分/矢量脱离十分容易。定量要素仍需在矢量中呈现，因为这些要素会因各弱点不同而异。

另一种方法是，当CWSS得分从一方传至另一方时，接收方可对给定CWSS矢量的得分进行重新计算，并将重新计算的得分与原得分加以对比。得分间的差异表明提供方与接收方使用了不同的机制，造成这一现象的原因可能是CWSS不同。

参考资料

[b-ITU-T X.1500] Recommendation ITU-T X.1500 (2011), *Overview of Cybersecurity information exchange*.

[b-ITU-T X.1520] Recommendation ITU-T X.1520 (2014), *Common vulnerabilities exposures*.

[b-ITU-T X.1521] Recommendation ITU-T X.1521 (2011), *Common vulnerability scoring system*.

[b-ITU-T X.1524] Recommendation ITU-T X.1524 (2012), *Common weakness enumeration.*

[b-ITU-T X.1544] Recommendation ITU-T X.1544 (2013), *Common attack pattern enumeration and classification.*

[b-CWRAF] Common Weakness Risk Analysis Framework
<http://cwe.mitre.org/cwraf/>

ITU-T 建议书系列

系列 A	ITU-T 工作的组织
系列 D	资费及结算原则和国际电信/ICT 的经济和政策问题
系列 E	综合网络运行、电话业务、业务运行和人为因素
系列 F	非话电信业务
系列 G	传输系统和媒介、数字系统和网络
系列 H	视听及多媒体系统
系列 I	综合业务数字网
系列 J	有线网络和电视、声音节目及其他多媒体信号的传输
系列 K	干扰的防护
系列 L	环境与 ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列 M	电信管理，包括 TMN 和网络维护
系列 N	维护：国际声音节目和电视传输电路
系列 O	测量设备的技术规范
系列 P	电话传输质量、电话设施及本地线路网络
系列 Q	交换和信令，以及相关联的测量和测试
系列 R	电报传输
系列 S	电报业务终端设备
系列 T	远程信息处理业务的终端设备
系列 U	电报交换
系列 V	电话网上的数据通信
系列 X	**数据网、开放系统通信和安全性**
系列 Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列 Z	用于电信系统的语言和一般软件问题

瑞士印刷
2020年，日内瓦