

国 际 电 信 联 盟

ITU-T

国际电信联盟
电信标准化部门

X.1521

(04/2011)

X系列：数据网、开放系统通信和安全性
网络空间安全 – 反垃圾信息

共同漏洞评分系统（CVSS）

ITU-T X.1521建议书

ITU-T

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	
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。

摘要

有关共同漏洞评分系统（CVSS）的ITU-T X.1521建议书提供一个开放框架，以便于对通信网络、最终用户装置或其它有能力运行软件的信息通信技术（ICT）设备中使用的商业或开放源代码软件中的信息通信技术（ICT）漏洞的特性和影响进行通信沟通。本建议书的目的方便ICT管理人员、漏洞公告提供商、安全厂商、应用厂商和研究人员以通用语言对ICT漏洞予以评分。

沿革

版本	建议书	批准日期	研究组
1.0	ITU-T X.1521	2011-04-20	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/>。

© 国际电联 2012

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

1	范围	1
2	参考文献	1
3	定义	1
3.1	他处定义的术语	1
3.2	本建议书定义的术语	1
4	缩写词和首字母缩略语	2
5	惯例	2
6	CVSS的使用	2
6.1	对CVSS的描述	3
6.2	CVSS工作原理	4
6.3	CVSS评分	4
6.4	CVSS用户	4
6.5	度量组 – 基本度量指标	5
6.6	时间度量指标	8
6.7	环境度量指标	10
6.8	基本、时间、环境矢量	12
6.9	打分 – 导则	13
6.10	公式	14
7	更多资源	16
附录I – CVSS的使用示例		17
I.1	CVE-2002-0392	17
I.2	CVE-2003-0818	18
I.3	CVE-2003-0062	20
附录II – 更多资源		22
参考资料		23

引言

ICT管理人员必须对诸多各自为政的硬件和软件平台确定并评估相关漏洞，之后，他们需要排定这些漏洞的轻重缓急，并首先补救将带来最大风险的漏洞。由于需要排除的漏洞诸多，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ICT管理人员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CVSS对描述漏洞特性的方式实行标准化，因此CVSS用户可启动时间和环境度量指标（metrics）来应用能够更加准确地反映其独特环境风险的语境（contextual）信息。这将在他们试图缓解其独特环境中不可知的厂商漏洞造成的风险方面做出更佳的知情决策。

本建议书在技术上等同于“第2版本共同漏洞评分系统（CVSS）”并与之相兼容（2007年6月20日）。可在下列网站上查阅该出版物：<http://www.first.org/cvss>。

共同漏洞评分系统（CVSS）

1 范围

本建议书提供一种标准化方式，以便通过采用语境信息的时间和环境度量指标对ICT的漏洞特性和影响进行通信沟通，从而更准确地反映每一用户独特环境的风险。

本建议书在技术上等同于“第2版本共同漏洞评分系统（CVSS）”并与之相兼容（2007年6月20日）。可在下列网站上查阅该出版物：<http://www.first.org/cvss>。

2 参考文献

下列ITU-T建议书和其他参考文献的条款，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。所有的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。

[CVSS Guide] CVSS（2007），共同漏洞评分系统指南大全2.0版。

<<http://www.first.org/cvss/cvss-guide.pdf>>

3 定义

3.1 他处定义的术语

3.1.1 漏洞 [b-ITU-T X.1500]：所有可用于破坏系统或其中信息的弱点。

3.2 本建议书定义的术语

本建议书定义了下列术语：

3.2.1 接入（Access）：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。

3.2.2 可用性（Availability）：经授权的个人对数据和资源的可靠和及时的接入。

3.2.3 保密性（Confidentiality）：旨在确保信息不被披露给未经授权的主体的安全原则。

3.2.4 完整性（Integrity）：确保信息和系统不被恶意或意外修改的安全原则。

3.2.5 风险（Risk）：被利用的漏洞将对用户环境产生的相对影响。

3.2.6 威胁（Threat）：有害事件出现的可能性或频次。

4 缩写词和首字母缩略语

本建议书使用下列缩写词和首字母缩略语：

A	可用性影响
AC	接入复杂性
AR	可用性要求
Au	认证
AV	接入矢量
C	保密性影响
CDP	潜在附带损害
CR	保密性要求
CVSS	共同漏洞评分系统
DMA	内存直接接入
DNS	域名系统
E	可利用性影响
I	完整性影响
ICT	信息通信技术
IM	即时信息
IR	完整性要求
JVN	日本漏洞公告
NVD	国家漏洞数据库
RC	报告把握性
RL	补救程度
RPC	远程程序调用
SLA	服务水平协议
TD	目标分布
USB	通用串行总线

5 惯例

无。

6 CVSS的使用

目前，ICT管理人员需要为诸多各自为政的硬件和软件平台确定和评估漏洞，之后需要排定这些漏洞的轻重缓急并对风险最大的漏洞予以排除。但当需排除的漏洞数量极大、且每一个都采用不同的数值范围得到评分时，ICT管理人员难以将这些堆积如山的漏洞数据转化为可采取行动的信息。“共同漏洞评分系统（CVSS）”是一个旨在解决这一问题的开放式框架，它具有下列益处：

- 标准化的漏洞评分：当一个组织能够将其所有软件和硬件平台的漏洞评分规范化时，则该组织可充分实现漏洞统一管理政策的优势。该政策可以与服务水平协议（SLA）类似，明确规定必须以何种速度证实和补救特定漏洞。
- 开放框架：如果随意对漏洞进行评分，用户会感到困惑。“评分以何特性为基础？这一评分与昨天公布的评分有何不同？”通过CVSS，任何人都可以明确无误地了解得出评分的具体特性。
- 排定风险的轻重缓急：在计算环境评分时，漏洞具有了语境背景。也就是说，漏洞评分代表着组织实际面临的风险，用户知道一个特定的漏洞相对于其它漏洞究竟有多么重要。

6.1 对CVSS的描述

CVSS由三个度量指标组组成：基本组、时间组和环境组。如图1所示，每一组均含有一套度量指标。

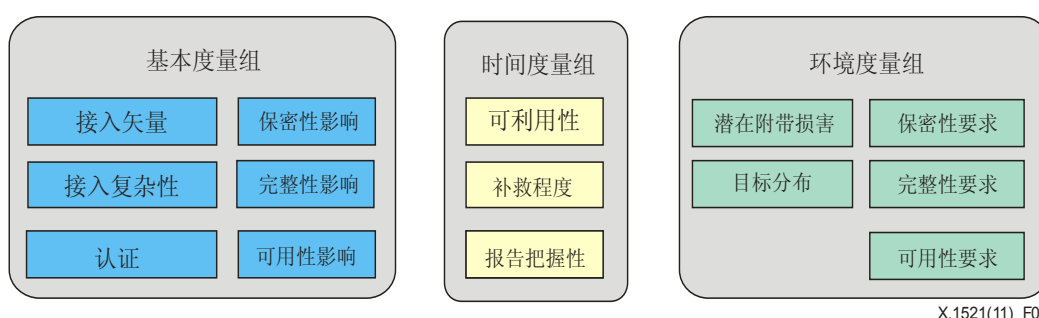


图1 – CVSS度量指标组

这些度量指标组的描述如下：

- 基本组：代表随时间和在用户环境中不断出现的漏洞的固有和根本特性。第6.5节具体讨论基本度量组。
- 时间组：代表随时间但不随用户环境变化的漏洞的特性。第6.6节讨论时间度量组。
- 环境组：代表与特定用户环境有关的、独特的漏洞特性。第6.7节探讨环境度量组。

CVSS基本组的目的是定义并沟通漏洞的根本特性。这一客观的描述漏洞特性的方式能够向用户清楚和直观地呈现漏洞，之后用户可启动时间和环境组来提供更加准确地反映其独特环境所面临的风险的语境信息，从而方便他们在试图缓解漏洞造成的风险时做出更佳的情决策。

6.2 CVSS工作原理

当为基本度量指标分配数值后，基本公式计算范围为零至十的评分分数，并创建一个矢量（如以下图2所示）。矢量为该框架的“开放性”提供了便利，该矢量包含为每一度量指标所分配数值的文本字符，并用于准确沟通每一个漏洞的评分是如何得出的。因此，应永远随漏洞评分显示该矢量。第7.4节进一步对矢量做出解释。

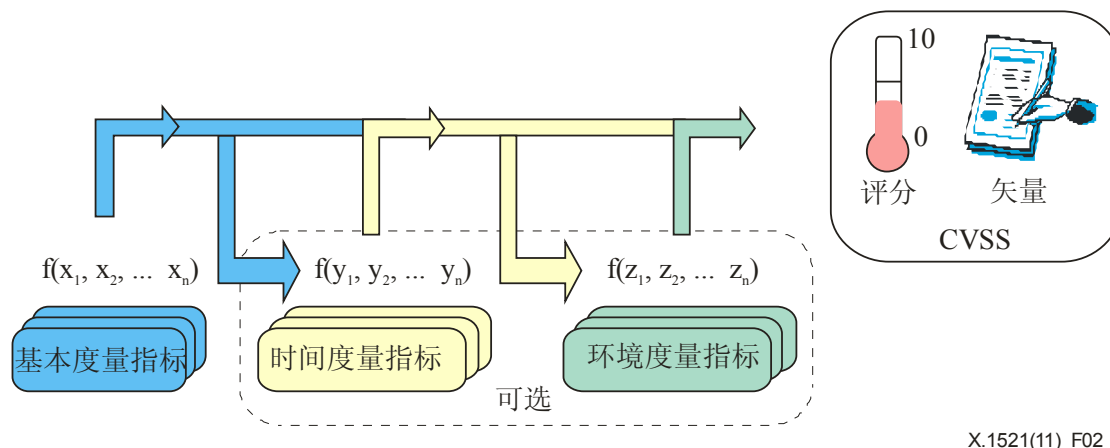


图2 – CVSS度量指标和公式

必要时可通过分配时间和环境度量指标数值改善基本评分，为提供漏洞的更多语境、以便更准确地反映漏洞对用户环境造成的风险，这样做是十分有益的。然而，并不存在这方面的要求。根据各方的不同目的，基本评分及矢量可能已足矣。

如需要时间评分，则时间公式将对时间度量指标与基本评分进行合并，以产生从0至10的时间评分分数。同样，如需要环境评分，则环境公式将对环境度量指标与时间评分进行合并，以产生从0至10的环境评分分数。第8.2节详细和充分地阐释基本、时间和环境公式。

6.3 CVSS评分

通常而言，基本和时间度量指标由漏洞公告分析人员、安全产品厂商或应用厂商予以明确，因为通常他们比用户更了解有关漏洞特性的信息。然而，环境度量指标却由用户予以明确，因为他们最有能力评价其自身环境中漏洞带来的潜在影响。

6.4 CVSS用户

诸多组织都在使用CVSS，且每一个组织都以不同方式找到了该系统的价值。现举例如下：

- 漏洞公告提供商：非盈利和商业性机构都在其免费的漏洞公告中公布CVSS基本和时间评分及矢量。这些公告提供诸多信息，包括发现日期，受到影响的系统以及指向有关厂商的链接，以了解补丁建议。
- 软件应用厂商：软件应用厂商在为其消费者提供CVSS基本评分和矢量，这有助于他们正确沟通其产品存在的漏洞严重程度并有助于其消费者有效管理其ICT风险。

- 用户组织：许多私营部门组织都在内部使用CVSS，以做出更好的有关漏洞管理的知情决策。他们首先采用扫描或监视技术确定主机和应用的漏洞，然后将这些数据与CVSS基本、时间和环境评分加以结合，以得到与语境更加有关的风险信息，并对对其系统造成最大风险的漏洞予以弥补。
- 漏洞扫描和管理：漏洞管理组织对网络扫描以找出ICT漏洞。他们为每台主机的每个漏洞提供CVSS基本评分。用户组织利用这些关键数据流减少故障并保护其系统免受恶意和意外ICT威胁的影响，从而更加有效地管理其ICT基础设施。
- 安全（风险）管理：安全风险公司将CVSS评分作为输入来计算组织的风险或威胁程度。这些公司采用往往与组织网络拓扑、漏洞数据和资产数据库相集成的尖端应用来为其消费者提供更加清晰明了的有关其面临风险程度的信息。
- 研究人员：CVSS的开放框架有助于研究人员对漏洞和漏洞特性做出统计分析。

6.5 度量组 – 基本度量指标

基本度量组捕获随时间在整个用户环境中出现的漏洞的特性。接入矢量、接入复杂性和认证度量指标捕获漏洞得到获取的方法以及是否要求有额外条件来对其加以利用。三个影响度量指标（如得到采用）则衡量漏洞将如何直接影响到ICT资产，其中影响被单独定义为保密性、完整性和可用性的损失程度。例如，漏洞可能导致完整性和可用性的部分丢失，但不会造成保密性损失。

6.5.1 接入矢量（AV）

该度量指标反映漏洞如何被利用。表1列出了该度量指标打分的可能数值。攻击者对主机实施的攻击越遥远，漏洞的评分越高。

表1 – 接入矢量打分评估

度量指标值	描述
本地（L）	仅可通过本地接入利用的漏洞要求攻击者具有对存在漏洞的系统的实际接入或本地（壳（shell））账户。有关可本地利用的漏洞示例包括外设攻击，如防火墙/USB DMA攻击以及本地特权升级（如sudo）。
相邻网络（A）	可通过相邻网络接入利用的漏洞要求攻击者能够接入存在漏洞的软件的广播或冲突域。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。
网络（N）	可通过网络接入利用的漏洞意味着存在漏洞的软件被绑定在网络堆栈上，且攻击者不要求进行本地网络接入或本地接入。此类漏洞通常被称为“远程利用漏洞”。网络攻击的示例之一是RPC缓冲溢出。

6.5.2 接入复杂性 (AC)

该度量指标衡量一旦攻击者获得了目标系统的接入所需的、利用漏洞进行攻击的复杂程度。例如，我们可以考虑互联网服务的缓冲溢出：一旦找到目标系统，则攻击者可随意开始利用。

但其它漏洞可能要求采取额外步骤才能被利用。例如，电子邮件客户机中的漏洞只有在用户下载并打开一个受到污染的附件后才能被利用。表2列出了该度量指标的可能数值。所要求的复杂程度越低，漏洞的评分越高。

表2 – 接入复杂性打分评估

度量指标数值	描述
高 (H)	存在专门的接入条件，例如： - 在大多数配置中，发起攻击的一方必须已提高了特权，或除实行攻击的系统外还欺骗 (spoof) 更多系统（如DNS劫持）。 - 攻击取决于可被十分熟悉情况的人轻而易举识破的社交工程方法。例如，受害者必须从事若干次可疑或不同寻常的行动。 - 实践中存在漏洞的配置被视为十分罕见。 - 如果存在竞赛 (race) 条件，则窗口十分狭窄。
中 (M)	接入条件有些专业化，以下为一些示例： - 攻击方限于某一组具有一定程度授权的系统或用户，很可能不受信任。 - 在成功开始攻击前必须收集某些信息。 - 受影响的配置为非默认配置，且不是常用配置（如，当服务器通过特定机制进行用户账户认证时会出现漏洞，但用另一种认证机制时不会出现漏洞）。 - 攻击仅要求少量的可能偶尔会使谨慎用户上当的社交工程（如，修改网络浏览器状态条、以显示虚假链路的网上钓鱼攻击在发送IM利用信息前必需存在于某人的好友名单 (buddy list) 上。
低 (L)	不存在专业化的接入条件或情有可原的环境，相关示例列举如下： - 受影响的产品通常要求接入广泛的系统和用户，可能是匿名和不受信任的系统和用户（如，面对互联网的网站或邮件服务器）。 - 受影响的配置为默认配置或无所不在的配置。 - 可人工进行攻击且要求的技能或收集的额外信息少之又少。 - 竞赛条件十分宽松（即，技术上是一种竞赛，但可轻而易举地获胜）。

6.5.3 认证 (Au)

该度量指标衡量攻击者必须与目标进行认证、以利用漏洞的次数。该度量指标并不衡量认证程序的力度或复杂性，仅要求攻击者在利用出现前提供证书。表3列出了该度量指标的可能数值。所要求的认证次数越低，漏洞评分越高。

表3 – 认证打分评估

度量指标数值	描述
多次 (M)	利用漏洞要求攻击者即使在每次使用相同证书时都要认证两次或更多次。其中示例之一是攻击者除提供证书以接入托管在相关系统上的应用外，还需与操作系统进行认证。
单次 (S)	该漏洞要求攻击者登录系统（如在命令行，或通过桌面会话或网络界面）。
无 (N)	不需要进行认证来利用漏洞。

应根据攻击者在发起攻击之前要求的认证来使用该度量指标。例如，如果邮件服务器可能受到用户认证之前即可发出的命令的影响，则该度量指标应打分为“无”，因为攻击者可以在要求提供证书之前开始进行利用。如果易于受到攻击的命令仅在成功认证之后才提供，则根据在发出命令前需进行的认证次数将漏洞打分为“单次”或“多次”。

6.5.4 保密性影响 (C)

该度量指标衡量被成功利用的漏洞对保密性产生的影响。保密性系指将信息接入和披露仅限于得到授权的用户，以及避免由未得到授权的用户获得信息或向其披露信息。表4列出了该度量指标的可能数值。保密性影响越大，漏洞评分越高。

表4 – 保密性影响打分评估

度量指标数值	描述
无 (N)	对系统保密性没有影响。
部分 (P)	信息披露数量可观，可能接入某些系统文档，但攻击者对所获得的信息无法控制，或损失范围有限。其示例之一是漏洞仅使数据库中的某些表遭到破坏。
完全 (C)	信息被完全披露，导致所有系统文档泄漏。攻击者能够读到所有系统数据（内存、文档等）。

6.5.5 完整性影响 (I)

该度量指标衡量被成功利用的漏洞产生的完整性影响。完整性系指信息的可信程度和得到保证的精确性。表5列出了该度量指标的可能数值。完整性影响越大，漏洞评分越高。

表5 – 完整性影响打分评估

度量指标数值	描述
无 (N)	对系统完整性没有影响。
部分 (P)	可能修改系统的某些文档或信息，但攻击者无法控制将修改的内容，或攻击者可影响的范围有限。例如，系统和应用文档可能被覆盖或修改，但攻击者无法控制将影响哪些文档，或攻击者只能在有限的语境或范围内修改文档。
完全 (C)	系统完整性被彻底破坏，系统保护完全丢失，导致整个系统遭受破坏。攻击者能够修改目标系统的任何文档。

6.5.6 可用性影响 (A)

该度量指标衡量被成功利用的漏洞造成的可用性影响。可用性系指对信息资源的接入性。消耗网络带宽、处理周期或硬盘空间的攻击都会影响到系统的可用性。表6列出了该度量指标的可能数值。可用性影响越大，漏洞评分越高。

表6 – 可用性影响打分评估

度量指标数值	描述
无 (N)	对系统可用性没有影响。
部分 (P)	性能降低或资源可用性受到干扰。示例之一是基于网络的泛洪攻击，它允许对互联网服务进行有限的成功连接。
完全 (C)	受到影响的资源完全瘫痪。攻击者可使资源完全不能被使用。

6.6 时间度量指标

漏洞造成的威胁可随时间的变化而改变。CVSS捕获的三种此类因素为：确认漏洞的技术细节、漏洞的补救状况、利用代码或技术的可用性。由于时间度量指标是可选的，因此每一个度量指标均含有一个对评分没有任何影响的度量指标数值，该数值在用户感到特定度量指标不适用、且希望“略过”该指标时加以使用。

6.6.1 可利用性 (E)

该度量指标衡量利用技术或代码可用性的现状。公开提供的、便于使用的利用代码加大了潜在攻击者的数量，因为其中包括了并非技能娴熟的攻击者，从而增加了漏洞的严重性。

开始时，现实生活中的利用可能仅仅是理论上的。此后可能会公布概念代码验证、实际运行的利用代码或利用漏洞所需的足够的技术细节。此外，可用的利用代码可从概念验证演示进步为利用代码，后者在不断利用漏洞方面十分成功。在严重情况下，它可能作为基于网络的蠕虫或病毒的有效荷载加以提供。表7列出了该度量指标的可能数值。漏洞越易于被利用，漏洞评分越高。

表7 – 可利用性影响打分评估

度量指标数值	描述
未证实（U）	不存在可用的利用代码，或利用完全是理论上的利用。
概念验证（POC）	存在对多数系统并不切实可行的概念验证利用代码或攻击演示。该代码或技术不能在所有情况下都运行如常，可能需要技能娴熟的攻击者进行大量的实质性修改。
实际运行（F）	存在实际运行的利用代码。在漏洞存在的情况下该代码在大多数情况下有效。
高（H）	漏洞可被实际运行的移动自治代码利用，或不要求利用（人工触发），且大范围提供细节。该代码在任何情况下均有效，或通过移动自治代理（如蠕虫或病毒）被大量提供。
未定义（ND）	为度量指标分配该数值不会影响评分，它只是向公式表明略过该度量指标。

6.6.2 补救程度（RL）

对于排定轻重缓急而言，漏洞的补救程度是一项重要因素。最初公布时，典型的漏洞是不被修补的，只是提供变通措施或热修复（hotfixes）手段，以便进行临时补救，直到发布正式补丁或升级软件。这当中的每一阶段均对时间评分进行下调，反映出随着补救的最终敲定，急迫程度也在下降。表8列出了该度量指标的可能数值。修复措施越不正式或固定，漏洞评分越高。

表8 – 补救程度打分评估

度量指标数值	描述
正式修复（OF）	存在完整的厂商解决方案。厂商或已发布了正式补丁，或提供升级（软件）。
临时修复（TF）	存在正式的临时修复，其中包括厂商发布临时的热修复、工具或变通措施。
变通措施（W）	存在非正式的非厂商解决方案。在某些情况下，受影响技术的用户可自行创建关键补丁或提供变通步骤，或用其它方法缓解漏洞。
未提供（U）	未提供解决方案或无法应用解决方案。
未定义（ND）	为度量指标分配该数值不会影响评分，它旨在向公式表明略过该度量指标。

6.6.3 报告把握性（RC）

该度量指标衡量人们对漏洞存在的相信程度以及已知技术细节的可信程度。有时，相关方面仅公开漏洞存在的事实，但不提供具体细节，之后漏洞可能被广泛宣传并由作者或受影响技术的厂商的承认予以确认。当十分确定漏洞存在时，漏洞的紧迫性更高。此外该度量指标还就可能发起攻击行动的攻击者可用的技术知识水平做出建议。表9列出了该度量指标的可能数值。漏洞越能被厂商或其它知名渠道证实，评分越高。

表9 – 报告把握性打分评估

度量指标数值	描述
未确认（UC）	存在单一的未经确认的渠道，或多项相互间可能十分矛盾的报告。报告真实性的可信度极低，示例之一是由地下黑客发出的传言。
未经证实（UR）	存在多种非正式渠道，可能包括独立的安全公司或研究组织。此时，可能存在相互矛盾的技术细节或其它持续性的模棱两可情况。
确认（C）	漏洞已得到厂商或受影响技术作者的承认。如果通过外部事件（如公布实际运行或概念验证利用代码或出现广泛利用）确认漏洞的存在时也可对漏洞予以确认。
未定义（ND）	为度量指标分配该数值不影响评分，它只向公式说明略过该度量指标。

6.7 环境度量指标

不同环境会极大地影响到机构及其利益攸关方的漏洞风险。CVSS环境度量组旨在捕获与用户ICT环境相关的漏洞特性。由于环境度量指标是可选的，因此每一项指标均含有一个对评分没有影响的度量数值。该数值在用户感到特定度量指标不适用并希望“略过”该指标时得到使用。

6.7.1 潜在附带损害（CDP）

该度量指标衡量损害或财产或设备失窃造成的生命或物理资产的潜在损失，它还衡量在生产方面产生的经济损失或收入损失。表10列出了该度量指标的可能数值。显而易见，潜在损害越大，漏洞评分越高。

表10 – 潜在附带损害打分评估

度量指标数值	描述
无（N）	不存在潜在的生命、物理资产、生产力或收入损失。
低（L）	成功利用该漏洞可能会造成轻微的物理或财产损失。或者机构会出现轻微的收入或生产力损失。
低 – 中（LM）	成功利用该漏洞可能会造成中度物理或财产损失。或者机构会出现中度收入或生产力损失。
中 – 高（MH）	成功利用该漏洞可能会导致大量的物理或财产破坏或损失。或者会出现极大的收入或生产力损失。
高（H）	成功利用该漏洞会为物理或财产造成灾难性破坏或损失。或者会有灾难性的收入或生产力损失。
未定义（ND）	为度量指标分配该数值不影响评分，它旨在向公式表明略过该度量指标。

显而易见，每一个组织均必须为自己确定“轻微、“中度、极大和灾难性”的确切含义。

6.7.2 目标分布 (TD)

该度量指标衡量出现漏洞系统的比例，其目的是作为一个具体针对环境的指标加以使用，以便获得可能受到漏洞影响的系统的近似百分比。表11列出了该度量指标的可能数值。产生漏洞的系统的比例越大，评分越高。

表11 – 目标分布打分评估

度量指标数值	描述
无 (N)	不存在目标系统，或者目标系统及其专业化，仅存在于实验室环境之中。事实上处于风险的环境为0%。
低 (L)	目标存在于环境内部，但规模很小，只有整体环境的1% - 25%处于风险中。
中度 (M)	目标存在于环境内，但规模为中度，整体环境的26% - 75%处于风险中。
高 (H)	目标存在于环境内，规模可观，整体环境的76% - 100%被视为处于风险中。
未定义 (ND)	为度量指标分配该数值不影响评分，它旨在向公式表明略过该度量指标。

6.7.3 安全要求 (CR、IR、AR)

这些度量指标有助于分析人员按照受影响的ICT资产对用户组织的重要程度为用户定制 (customize) CVSS评分体系，并从安全性、完整性和可用性方面加以衡量。也就是说，如果ICT资产支持的业务功能中可靠性是最重要的，则分析人员可相对于保密性和完整性为可用性分配更大的数值。每一个安全要求均有三个可能的数值：低、中或高。

对环境评分的总体影响取决于相应的基本影响度量指标（请注意，基本保密性、完整性和可用性影响度量指标本身未改变）。也就是说，这些度量指标通过重新对（基本）保密性、完整性和可用性影响度量指标予以加权而对环境评分做出修改。例如，如果保密性要求（CR）很高，则保密性影响（C）度量指标的权重增加。同样，如果保密性要求低，则保密性影响度量指标的权重减轻。如果保密性要求为中等，则保密性影响度量指标的加权为中等。同样的逻辑也适用完整性和可靠性要求。

如果（基本）保密性影响设为无，则保密性要求不会影响环境评分。此外，将保密性要求由中提高到高，在（基本）影响度量指标设为完全时也不会改变环境评分。这是因为影响子评分（计算影响的基本评分的一部分）已经为最大值10。

表12列出了安全性要求的可能数值。为简化工作，该表用于所有三个度量指标。安全性要求越高，评分越高（请牢记中等要求被视为是默认要求）。这些度量指标会将评分改变多达正2.5或负2.5。

表12 – 安全性要求打分评估

度量指标数值	描述
低 (L)	[保密性 完整性 可用性]损失可能仅对机构或与机构有关的个人（如雇员、客户）产生有限负面影响。
中 (M)	[保密性 完整性 可用性]损失可能对机构或与机构相关的个人（如雇员、客户）带来严重负面影响。
高 (H)	[保密性 完整性 可用性]损失可能对机构或与机构相关的个人（如雇员、客户）产生灾难性负面影响。
未定义 (ND)	为度量指标分配该数值不影响评分，它仅向公式表明略过该度量指标。

在诸多组织中，ICT资源按照网络地点、业务功能及潜在的收入或生命损失得到关键程度评级。例如，美国政府将每一个不保密的ICT资产分配给称作“系统”的一组资产。每一个系统均必须分配有三个“潜在影响”评级，以表明，根据三个安全性目标，在系统受到破坏时组织遭受的潜在影响：保密性、完整性和可用性。因此，美国政府中每一个不保密的ICT资产均在保密性、完整性和可用性的安全目标方面具有低、中或高的潜在影响评级。该评级体系在美国199“联邦信息处理标准（FIPS）”中得到了阐述。CVSS遵循了FIPS 199的总体模式，但并不要求组织使用特定体系来做出低、中或高的影响评级。

6.8 基本、时间、环境矢量

矢量的每一个度量指标均包含度量名称简称，其后为a“:”（冒号），再后为度量指标数值简称。矢量以预先确定的顺序列出这些度量指标，并采用“/”（斜线）符号将度量指标隔开。如某一时间或环境度量指标不会得到使用，则为其分配“ND”（未定义）数值。以下的表13列出这些基本、时间和环境矢量。

表13 – 基本、时间和环境矢量

度量指标数值	描述
基本	AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C]
时间	E:[U,POC,F,H,ND]/RL:[OF,TF,W,U,ND]/RC:[UC,UR,C,ND]
环境	CDP:[N,L,LM,MH,H,ND]/TD:[N,L,M,H,ND]/CR:[L,M,H,ND]/IR:[L,M,H,ND]/AR:[L,M,H,ND]

例如，具有“接入矢量：低、接入复杂性：中、认证：无、保密性影响：无、完整性影响：部分、可用性影响：完全”的基本度量数值的漏洞将具有下列基本矢量：“AV:L/AC:M/Au:N/C:N/I:P/A:C。”

6.9 打分 – 导则

以下是有助于分析人员对漏洞进行打分的导则。

6.9.1 综述

打分技巧1: 漏洞打分不应考虑与其它漏洞的相互影响, 也就是说, 应单独为每一个漏洞进行打分。

打分技巧2: 在为漏洞打分时, 应仅考虑对目标主机的直接影响。例如, 在跨址脚本漏洞方面, 对用户系统的影响可能会大大超过对目标主机的影响, 然而这是间接影响。在为跨址脚本漏洞打分时应不计保密性或可用性的影响, 以及完整性的部分影响。

打分技巧3: 诸如网络服务器等诸多应用可与多种不同特权进行运行, 因此对影响进行打分会涉及到对所用特权的设想。有鉴于此, 应根据得到最常使用的特权对漏洞进行打分。这可能不会反映出安全性方面的最佳做法, 特别是常常与根级特权运行的客户应用。在不明确哪些特权为最常用特权时, 进行打分的分析人员应设想一种默认配置。

打分技巧4: 在为具有多个利用方法(攻击矢量)的漏洞影响打分时, 分析人员应选择产生最大影响的利用方法, 而非最常用或最易于实施的方法。例如, 如果一个平台而非另一个平台存在实际运行的利用代码, 则“可利用性”应被设为“实际运行”。如果在并行开发一个产品的两个单独变量(如PHP 4.x和PHP 5.x), 且其中一个变量具有修复手段, 另一个变量没有, 则“补救程度”应设为“不存在”。

6.9.2 基本度量指标

6.9.2.1 接入矢量

打分技巧5: 当漏洞既可从本地又可从网络利用时, 应选择“网络”数值。当漏洞既可从本地也可从相邻网络利用、但不能从远程网络利用时, 应选择“相邻网络”数值。当漏洞既可由相邻网络又可由远程网络利用时, 应选择“网络”数值。

打分技巧6: 诸多客户应用或实用程序均存在可被远程利用或通过用户串通的行动或通过自动处理程序利用的本地漏洞。例如, 解压缩实用程序和病毒扫描装置可对来向电子邮件信息自动扫描。此外, 帮助应用程序(办公套件、图像浏览器、媒体播放器等)可通过电子邮件或在网站上下载内容时交换恶意文档的手段被利用。因此, 分析人员应将这些漏洞的接入矢量作为“网络”进行打分。

6.9.2.2 认证

打分技巧7: 如果认证机制本身(如PAM、Kerberos)或匿名服务(如公共FTP服务器)存在漏洞, 则该度量指标应被打分为“无”, 因为攻击者可以在无需提供有效证书的情况下利用漏洞。默认用户账户的存在可以被视为是“单次”或“多次”认证(酌情), 但如果证书公开, 则“可利用性”为“高”。

打分技巧8: 非常值得注意的是, 认证度量指标与接入矢量不同。在此, 一旦系统被接入, 就会考虑认证要求。具体而言, 对于可本地利用的漏洞而言, 如果认证超出了登录该系统的要求时, 则该度量指标仅应被设为“单次”或“多次”。要求认证的可被本地利用的漏洞示例为影响在Unix域名座(或其它非网络接口)上进行倾听的数据库引擎的漏洞。如果用户为利用该漏洞必须作为有效数据库用户进行认证时, 则该度量指标应设为“单次”。

6.9.2.3 保密性、完整性、可用性影响

打分技巧9：能够导致根层接入的漏洞应打分为完全损失保密性、完整性和可用性的漏洞，而导致用户层接入的漏洞应被打分为仅造成保密性、完整性和可用性部分损失的漏洞。例如，由于违反完整性规定而使攻击者修改了操作系统的密码文件的情况应被打分为完全影响了保密性、完整性和可用性的漏洞。

打分技巧10：造成部分或全部完整性损失的漏洞可能也会为可用性带来影响。例如，有能力修改记录的攻击者可能也能删除这些记录。

6.10 公式

以下描述基本、时间和环境度量组的打分公式和算法。下列网站提供有关这些公式的来源和测试的更多说明<http://www.first.org/cvss>。附录A提供这些公式的三种使用情况示例。

6.10.1 基本公式

基本公式是CVSS评分的基础。基本公式（2.10版本公式）为：

```
BaseScore = round_to_1_decimal(((0.6*Impact)+(0.4*Exploitability)-1.5)*f(Impact))
Impact = 10.41*(1-(1-ConfImpact)*(1-IntegImpact)*(1-AvailImpact))
Exploitability = 20*AccessVector*AccessComplexity*Authentication
f(impact) = 0 if Impact=0, 1.176 otherwise
AccessVector      = case AccessVector of
                        requires local access: 0.395
                        adjacent network accessible: 0.646
                        network accessible: 1.0
AccessComplexity = case AccessComplexity of
                        high: 0.35
                        medium: 0.61
                        low: 0.71
Authentication    = case Authentication of
                        requires multiple instances of authentication: 0.45
                        requires single instance of authentication: 0.56
                        requires no authentication: 0.704
ConfImpact        = case ConfidentialityImpact of
                        none: 0.000
                        partial: 0.275
                        complete: 0.660
IntegImpact       = case IntegrityImpact of
                        none: 0.000
                        partial: 0.275
                        complete: 0.660
AvailImpact       = case AvailabilityImpact of
                        none: 0.000
                        partial: 0.275
                        complete: 0.660
```

6.10.2 时间公式

使用时，时间公式将时间度量指标与基本评分合并，以产生从0至10的时间评分范围。此外，时间评分产生的时间打分不会高于基本打分，且不会比基本打分低33%以上。时间公式为：

```
TemporalScore = round_to_1_decimal(BaseScore*Exploitability
                                   *RemediationLevel*ReportConfidence)
Exploitability  = case Exploitability of
    unproven:          0.85
    proof-of-concept:  0.90
    functional:        0.95
    high:              1.00
    not defined:       1.00

RemediationLevel = case RemediationLevel of
    official-fix:      0.87
    temporary-fix:     0.90
    workaround:        0.95
    unavailable:       1.00
    not defined:       1.00

ReportConfidence = case ReportConfidence of
    unconfirmed:       0.90
    uncorroborated:    0.95
    confirmed:         1.00
    not defined:       1.00
```

6.10.3 环境公式

使用时，环境公式将环境度量指标与时间评分合并，以产生从0至10的环境评分范围。此外，该公式产生的打分不会高于时间打分。环境公式为：

```
EnvironmentalScore = round_to_1_decimal((AdjustedTemporal+
(10-AdjustedTemporal)*CollateralDamagePotential)*TargetDistribution)
AdjustedTemporal = TemporalScore recomputed with the BaseScores Impact
sub-equation replaced with the AdjustedImpact equation
AdjustedImpact = min(10,10.41*(1-(1-ConfImpact*ConfReq)*(1-IntegImpact*IntegReq)
                    *(1-AvailImpact*AvailReq)))
CollateralDamagePotential = case CollateralDamagePotential of
    none:          0.0
    low:           0.1
    low-medium:    0.3
    medium-high:   0.4
    high:          0.5
    not defined:   0.0

TargetDistribution    = case TargetDistribution of
    none:            0.00
    low:             0.25
    medium:          0.75
    high:            1.00
    not defined:     1.00

ConfReq              = case ConfReq of
    low:             0.5
    medium:          1.0
    high:            1.51
    not defined:     1.0

IntegReq             = case IntegReq of
    low:             0.5
    medium:          1.0
    high:            1.51
    not defined:     1.0

AvailReq             = case AvailReq of
    low:             0.5
```

medium:	1.0
high:	1.51
not defined:	1.0

7 更多资源

附录II包含一份可能对所有CVSS实施者有帮助的资源列表。该列表列出了漏洞公告指标和若干CVSS计算器。漏洞公告有助于搜索有关特定漏洞的详细信息。CVSS计算器则可帮助您计算自己的基础、时间或环境的评分。

附录I

CVSS的使用示例

（本附录不构成本建议书的组成部分）

以下介绍将CVSS用于三种不同漏洞的示例。

I.1 CVE-2002-0392

CVE-2002-0392: Apache区块编码（Chunked-Encoding）内存损坏漏洞。2002年6月，在Apache网络服务器处理用区块编码的请求编码手段中发现了漏洞。Apache基金会报告说，成功利用该漏洞在某些情况下会导致拒绝服务，在其它情况下则会导致执行网络服务器特权的任意代码。

由于该漏洞可被远程利用，因此接入矢量为“网络”。接入复杂性为“低”，因为成功利用该漏洞不需要更多的背景情况，攻击者仅需向Apache网站倾听器发送适当的利用信息，触发漏洞也不需要认证（任何互联网用户均可与网络服务连接），因此认证度量指标为“无”。

由于可用多种方法利用该漏洞，并会产生不同后果，因此应为每种方法都制定评分，并使用其中最高分数。

如果漏洞被用来执行在网络服务器允许下的任意代码，从而改变网站内容并可能浏览到本地用户或配置信息（包括连接设置和连向后台数据库的密码），则保密性和完整性影响度量指标应设为“部分”。这些度量指标共同形成6.4的基本评分。

如果利用该漏洞造成拒绝服务，则可用性影响应设为“完全”。这些度量指标共同产生7.8的基本评分。由于这是各种利用方案的最高可能基本评分，因此被作为基本评分使用。

由此，该漏洞的基本矢量为：AV:N/AC:L/Au:N/C:N/I:N/A:C。

现已知存在利用代码，因此可利用性被设为“实际运行”。Apache基金会已发布了该漏洞的补丁（既可用于1.3，又可用于2.0），因此补救程度为“正式修复”。显而易见，报告把握性为“确认”。这些度量指标对基本评分做出调整，从而形成6.4的时间评分。

假设对目标系统而言可用性比平常更为重要，且根据潜在附带损害和目标分布数值的不同，环境评分可介于0.0（“无”、“无”）和9.2（“高”、“高”）之间。现将相关结果总结如下。

BASE METRIC	EVALUATION	SCORE
Access Vector	[Network]	(1.00)
Access Complexity	[Low]	(0.71)
Authentication	[None]	(0.704)
Confidentiality Impact	[None]	(0.00)
Integrity Impact	[None]	(0.00)
Availability Impact	[Complete]	(0.66)
BASE FORMULA		BASE SCORE
Impact = 10.41*(1-(1)*(1)*(0.34)) == 6.9		
Exploitability = 20*0.71*0.704*1 == 10.0		
f(Impact) = 1.176		
BaseScore = ((0.6*6.9) + (0.4*10.0) - 1.5)*1.176 == (7.8)		
TEMPORAL METRIC	EVALUATION	SCORE
Exploitability	[Functional]	(0.95)
Remediation Level	[Official-Fix]	(0.87)
Report Confidence	[Confirmed]	(1.00)
TEMPORAL FORMULA		TEMPORAL SCORE
round(7.8 * 0.95 * 0.87 * 1.00) == (6.4)		
ENVIRONMENTAL METRIC	EVALUATION	SCORE
Collateral Damage Potential	[None - High]	{0 - 0.5}
Target Distribution	[None - High]	{0 - 1.0}
Confidentiality Req.	[Medium]	(1.0)
Integrity Req.	[Medium]	(1.0)
Availability Req.	[High]	(1.51)
ENVIRONMENTAL FORMULA		ENVIRONMENTAL SCORE
AdjustedImpact = min(10,10.41*(1-(1-0*1)*(1-0*1)* *(1-0.66*1.51)) == (10.0)		
AdjustedBase = ((0.6*10)+(0.4*10.0) - 1.5)*1.176 == (10.0)		
AdjustedTemporal == (10*0.95*0.87*1.0) == (8.3)		
EnvScore = round((8.3+(10-8.3)*{0-0.5})*{0-1}) == (0.00 - 9.2)		

I.2 CVE-2003-0818

CVE-2003-0818: 微软视窗ASN.1数据库整数处理漏洞。2003年9月发现了针对微软所有操作系统的ASN.1数据库的漏洞。成功利用该漏洞将会导致缓冲器溢出的情况，从而方便攻击者在行政管理（系统）特权方面执行任意代码。

该可远程利用的漏洞不要求进行认证，因此接入矢量为“网络”，“认证”为“无”，接入复杂性为“低”，因为不需要有更多的接入和专业化的背景情况就可以成功利用该漏洞。每一个影响度量指标均被设为“完全”，因为整个系统均可能被破坏。这些度量指标共同产生最大的10.0基本评分。

由此，该漏洞的基本矢量为：AV:N/AC:L/Au:N/C:C/I:C/A:C。

该漏洞确实存在已知的被利用手段，因此可利用性为“实际运行”。2004年2月，微软发布了MS04-007补丁，使补救程度成为“正式修复”，报告把握性为“确认”。这些度量指标对基本评分做出调整，从而产生8.3的时间评分。

假设对目标系统而言，可用性比平常更不重要，且根据潜在附带损害和目标分布的不同，环境评分可介入0.0（“无”、“无”）和9.0（“高”、“高”）之间。相关结果总结如下。

BASE METRIC	EVALUATION	SCORE
Access Vector	[Network]	(1.00)
Access Complexity	[Low]	(0.71)
Authentication	[None]	(0.704)
Confidentiality Impact	[Complete]	(0.66)
Integrity Impact	[Complete]	(0.66)
Availability Impact	[Complete]	(0.66)
FORMULA		BASE SCORE
Impact = 10.41*(1-(0.34*0.34*0.34)) == 10.0		
Exploitability = 20*0.71*0.704*1 == 10.0		
f(Impact) = 1.176		
BaseScore = ((0.6*10.0)+(0.4*10.0) - 1.5)*1.176 == (10.0)		
TEMPORAL METRIC	EVALUATION	SCORE
Exploitability	[Functional]	(0.95)
Remediation Level	[Official-Fix]	(0.87)
Report Confidence	[Confirmed]	(1.00)
FORMULA		TEMPORAL SCORE
round(10.0 * 0.95 * 0.87 * 1.00) ==		(8.3)
ENVIRONMENTAL METRIC	EVALUATION	SCORE
Collateral Damage Potential	[None - High]	{0 - 0.5}
Target Distribution	[None - High]	{0 - 1.0}
Confidentiality Req.	[Medium]	(1.0)
Integrity Req.	[Medium]	(1.0)
Availability Req.	[Low]	(0.5)
FORMULA		ENVIRONMENTAL SCORE
AdjustedImpact = 10.41*(1-(1-(1-0.66*1)*(1-0.66*1)* *(1-0.66*0.5)) == (9.6)		
AdjustedBase = ((0.6*9.6)+(0.4*10.0) - 1.5)*1.176 == (9.7)		
AdjustedTemporal == (9.7*0.95*0.87*1.0) == (8.0)		
EnvScore = round((8.0+(10-8.0)*{0-0.5})*{0-1}) == (0.00 - 9.0)		

I.3 CVE-2003-0062

CVE-2003-0062: NOD32反病毒缓冲器溢出。NOD32是由Eset开发的一个反病毒软件应用。2003年2月，在1.013之前的Linux和Unix版本中发现了缓冲器溢出漏洞，有利于本地用户在用户执行NOD32时在特权方面执行任意代码。要触发缓冲器溢出，攻击者必需等待（或欺骗）另一个用户（可能是根用户）来对目录路径进行超长时间扫描。

由于该漏洞仅可由在本地登录系统的用户利用，因此接入矢量为“本地”，接入复杂性为“高”，因为该漏洞无法由攻击者随意加以利用。此间复杂性又多了一层，因为攻击者必须等待另一个用户运行病毒扫描软件。认证设为“无”，因为攻击者不需要对任何额外系统进行认证。如果行政管理用户运行病毒扫描，导致缓冲器溢出，则可能导致整个系统的彻底瘫痪。因为必须考虑最有害的情况，因此三个影响度量指标的每一个均被设为“完全”。这些度量指标共同产生6.2的基本评分。

由此，该漏洞的基本矢量为：AV:L/AC:H/Au:N/C:C/I:C/A:C。

目前已公布了部分利用代码，因此可利用性度量指标被设为“概念验证”。Eset已发布了经更新的软件，因此补救程度为“正式修复”，报告把握性为“确认”。这三个度量指标对基本评分做出调整，从而产生4.9的时间评分。

假设对目标系统而言，保密性、完整性和可用性约同样重要，同时根据潜在附带损害和目标分布值的不同，环境评分可介于0.0（“无”、“无”）和7.5（“高”、“高”）之间。相关结果总结如下。

```

-----
BASE METRIC                                EVALUATION                                SCORE
-----
Access Vector                             [Local]                             (0.395)
Access Complexity                         [High]                              (0.35)
Authentication                           [None]                              (0.704)
Confidentiality Impact                   [Complete]                          (0.66)
Integrity Impact                        [Complete]                          (0.66)
Availability Impact                     [Complete]                          (0.66)
-----
FORMULA                                BASE SCORE
-----
Impact = 10.41 * (1 - (0.34*0.34*0.34)) == 10.0
Exploitability = 20*0.35*0.704*0.395 == 1.9
f(Impact) = 1.176
BaseScore = ((0.6*10)+(0.4*1.9) - 1.5)*1.176 == (6.2)
-----
TEMPORAL METRIC                          EVALUATION                          SCORE
-----
Exploitability                          [Proof-Of-Concept]                 (0.90)
Remediation Level                      [Official-Fix]                    (0.87)
Report Confidence                      [Confirmed]                       (1.00)
-----
FORMULA                                TEMPORAL SCORE
-----
round(6.2 * 0.90 * 0.87 * 1.00) == (4.9)
-----
ENVIRONMENTAL METRIC                    EVALUATION                    SCORE
-----
Collateral Damage Potential [None - High] {0 - 0.5}
Target Distribution        [None - High] {0 - 1.0}
Confidentiality Req.      [Medium]      (1.0)
Integrity Req.            [Medium]      (1.0)
Availability Req.         [Medium]      (1.0)
-----
FORMULA                                ENVIRONMENTAL SCORE
-----
AdjustedTemporal == 4.9
EnvScore = round((4.9+(10-4.9)*{0-0.5})*{0-1})
== (0.00 - 7.5)
-----

```

附录II

更多资源

（本附录不构成本建议书的组成部分。）

以下我们提供对实施CVSS的任何人可能都将十分有益的资源清单。漏洞公告对于搜寻详细的有关特定漏洞的信息十分有益。在计算自身的基本、时间或环境评分时，CVSS计算器将十分有益。

漏洞公告：

- 国家标准与技术研究院（NIST）设立并维护着国家漏洞数据库（NVD）和包括CVSS基本评分的漏洞公告网站。NIST除免费提供XML提要（feeds）外，也提供这些基于网络的公告。可分别通过下列网站对上述进行查询：
<http://nvd.nist.gov/nvd.cfm>和<http://nvd.nist.gov/download.cfm#XML>。
- IBM网络安全系统（ISS）公布供免费使用的X-Force漏洞公告，其中包括CVSS基本和时间评分。可通过下列网站查询：<http://xforce.iss.net/xforce/alerts>。
- Qualys公布包括CVSS基本和时间评分的漏洞参考资料。可通过下列网站查询：
<http://www.qualys.com/research/alerts/>。
- 思科公司公布的漏洞网站包括CVSS基本和时间评分，可通过下列网站查询：
<http://tools.cisco.com/MySDN/Intelligence/home.x>。（注：需要有思科在线连接账户）。
- Tenable网络安全机构公布Nessus漏洞扫描工具的相关插件，这些插件包括CVSS基本评分。可通过下列网站查询：<http://www.nessus.org/plugins/>。
- JPCERT/CC和IPA负责编制和发布日本漏洞公告（JVN），以及包括CVSS基本评分的漏洞公告网站。JVN除提供XML提要外还提供供免费使用的这些基于网络的公告。可分别通过下列网站查询：<http://jvndb.jvn.jp/en/> 和
<http://jvndb.jvn.jp/en/apis/>。

CVSS计算器：

- NIST CVSSv2计算器：
<http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2>
- 日本信息技术推进局：
<http://jvndb.jvn.jp/en/cvss/index.html>

参考资料

- [b-1] Mike Schiffman, Gerhard Eschelbeck, David Ahmad, Andrew Wright, Sasha Romanosky, *CVSS: A Common Vulnerability Scoring System*, National Infrastructure Advisory Council (NIAC), 2004.
- [b-2] Microsoft Corporation. *Microsoft Security Response Center Security Bulletin Severity Rating System*. November 2002 [cited 16 March 2007]. Available from URL:
<http://www.microsoft.com/technet/security/bulletin/rating.msp>
- [b-3] United States Computer Emergency Readiness Team (US-CERT). US-CERT Vulnerability Note Field Descriptions. 2006 [cited 16 March 2007]. Available from URL: <http://www.kb.cert.org/vuls/html/fieldhelp>
- [b-4] SANS Institute. SANS Critical Vulnerability Analysis Archive. Undated (cited 16 March 2007).
- [b-ITU-T X.1500] Recommendation X.1500 (2011), *Overview of Cybersecurity information exchange (CYBEX)*.

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