国 际 电 信 联 盟

ITU-T X.1521

(03/2016)

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

共同漏洞评分系统（CVSS）3.0

ITU-T X.1521 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
PKI相关建议书	X.1340–X.1349
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	
云计算安全概述	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
云计算安全的落实工作	X.1660–X.1679
其他云计算安全问题	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.1521 建议书

共同漏洞评分系统3.0

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。本建议书的目的是方便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	唯一识别码*
1.0	ITU-T X.1521	2011-04-20	17	11.1002/1000/11062
2.0	ITU-T X.1521	2016-03-23	17	11.1002/1000/12614

关键词

共同漏洞评分系统、 CVSS、 CYBEX、度量

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/ ，随后输入建议书的唯一识别码，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

共同漏洞评分系统（CVSS）作为一个开放框架，用于对软件漏洞的特性和严重性进行通信沟通。CVSS包括三大度量组：基本组、时间组和环境组。基本组代表漏洞的固有特性，时间组反映随时间变化的漏洞特性，而环境组代表某用户环境所特有的漏洞特性。基本组的评分范围为0至10，可通过给时间组和环境组评分来对其进行修改。CVSS分数也可由矢量字符来表示，即数值的压缩文字形式，用于评分。本建议书是CVSS第3.0版本的官方技术规范。

CVSS第3.0版本在CVSS第2.0版本基础上做了重大改进，不可向后兼容。在使用CVSS第2.0版本时遇到了一些技术规范方面的限制，例如：虚拟环境中的漏洞评分、跨址脚本等“间接”漏洞、无法捕获同一系统内各应用之间的相互依赖性、以及捕获用户而非攻击者的行为。更多有关第3.0版本的改进信息，请参见附件I，第2条款。

在应对上述限制时，CVSS工作组意识到，不可能与CVSS第2.0版本实现向后兼容。缺乏兼容性将给使用和处理CVSS第2.0版本的现有系统带来一些问题。因此，我们相信，第3.0版本能够提供足够的价值，弥补这一问题。我们强烈建议还在生产和处理CVSS第2.0版本的用户和厂商改用CVSS第3.0版本。

虽然出于历史的目的，CVSS第2.0版本技术规范还会继续提供，但已不再有效。强烈鼓励工具和流程实施者在继续支持第2.0版本的同时采纳CVSS第3.0版本技术规范，以便处理第2.0版本技术规范中已打分的现有漏洞。

ITU-T X.1521 建议书

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3版本共同漏洞评分系统（CVSS）”并与之相兼容（2015年6月10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。

无。

3 定义

3.1 他处定义的术语

本建议书使用下列他处定义的术语：

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	攻击复杂性
AR	可用性要求
ARP	地址解析协议
AV	攻击矢量
C	保密性影响
CIA	保密性、完整性和可用性
CPU	中央处理器
CR	保密性要求
CVE	共同漏洞暴露
CVSS	共同漏洞评分系统
CWE	共同缺陷列表
DMA	内存直接接入
DNS	域名系统
DOM	文件对象模型
DoS	拒绝服务
E	利用代码成熟度
I	完整性影响
ICT	信息通信技术
ID	识别码
IP	互联网协议
IR	完整性要求
ISC	影响子评分
IT	信息技术
LAN	局域网
MA	修改后的可用性
MAC	修改后的攻击复杂性
MAV	修改后的攻击矢量
MC	修改后的保密性影响
MI	修改后的完整性
MPR	修改后的所需特权
MS	修改后的范围
MUI	修改后的用户交互
NIST	国家标准与技术研究院
OS	操作系统
OSI	开放系统互连

PCI DSS	支付卡行业数据安全标准
PR	所需特权
RC	报告把握性
RL	补救程度
RPC	远程程序调用
S	范围
SCAP	安全内容自动化协议
SQL	结构化查询语言
TCP	传输控制协议
UI	用户交互
USB	通用串行总线
VM	虚拟机
XSS	跨址脚本

5 惯例

无。

6 关于共同漏洞评分系统

共同漏洞评分系统（CVSS）作为一个开放框架，用于对软件漏洞的特性和严重性进行通信沟通。CVSS包括三大度量组：基本组、时间组和环境组。基本组代表漏洞的固有特性，时间组反映随时间变化的漏洞特性，而环境组代表某用户环境所特有的漏洞特性。基本组的评分范围为0至10，在给时间组和环境组评分后可对其进行修改。CVSS分数也可由矢量字符来表示，即数值的压缩文字形式，用于评分。本建议书是CVSS第3.0版本的官方技术规范。

6.1 简介

软件、硬件和固件漏洞会给任何一个运行计算机网络的组织带来重大的风险，且很难进行归类和缓解。而共同漏洞评分系统（CVSS）则为捕捉漏洞的主要特性提供了一种方法，通过评分的方式反映其严重性，并对数值进行文字描述。之后，会对分数进行定性分类（例如，低、中、高、严重），帮助组织合理评估其漏洞管理流程，排定轻重缓急。

总而言之，CVSS有三大益处。第一，标准化的漏洞评分。当一个组织用通用算法来对所有IT平台的漏洞进行评分时，该组织可充分实现漏洞统一管理政策的优势，确定某漏洞验证和补救的最长允许时间。其次，开放框架。如果由第三方随意对漏洞进行评分，用户会感到困惑。通过CVSS，得出评分的具体特性将变得透明。最后，CVSS有助于排定风险的轻重缓急。在计算环境评分时，漏洞对于每一个组织来说都具有了语境背景，可以更好地了解该漏洞给组织带来的风险。

本建议书是对CVSS第3.0版本官方技术规范的描述。

6.1.1 度量指标

CVSS由三个度量组组成：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。

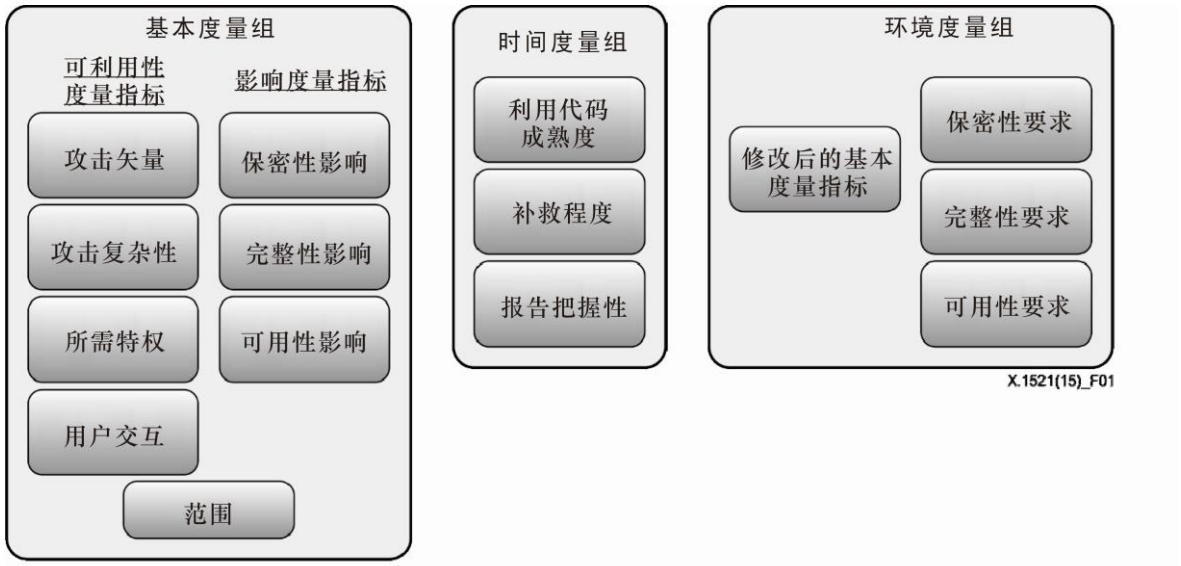


图1 – CVSS第3.0版本度量组

基本度量组代表随时间和在用户环境中不断出现的漏洞的固有特性。包括两套度量指标：可利用性度量指标和影响度量指标。

可利用性度量指标反映的是漏洞可被利用的难易程度和技术手段。即代表易于受到攻击的事物特性，我们将其称为*存在漏洞的组件*。另一方面，影响度量指标反映的是成功利用的直接后果，代表*受影响事物*所遭遇的后果，我们将其称为*受影响的组件*。

存在漏洞的组件通常为软件应用、模块、驱动等（或甚至可能是硬件设备），而受影响组件则可以是软件应用、硬件设备或网络资源。这种可以衡量漏洞而非存在漏洞组件的能力是CVSS第3.0版本的一个关键特性。该特性会在下面的范围这一度量指标中介绍和进一步讨论。

时间度量组反映随时间但不随用户环境变化的漏洞的特性。例如，简易利用工具可以提高CVSS评分，而创建正式布丁则会降低评分。

环境度量组代表与特定用户环境有关的、独特的漏洞特性。该度量指标可以使负责打分的分析人员纳入安全控制，缓解后果，并根据其业务风险加强或削弱存在漏洞的系统的重要性。

以上各度量指标会在后面进一步详细讨论。

6.1.2 评分

当分析人员为基本度量指标分配数值后，基本公式计算范围为0.0至10.0的评分分数，如图2所示。

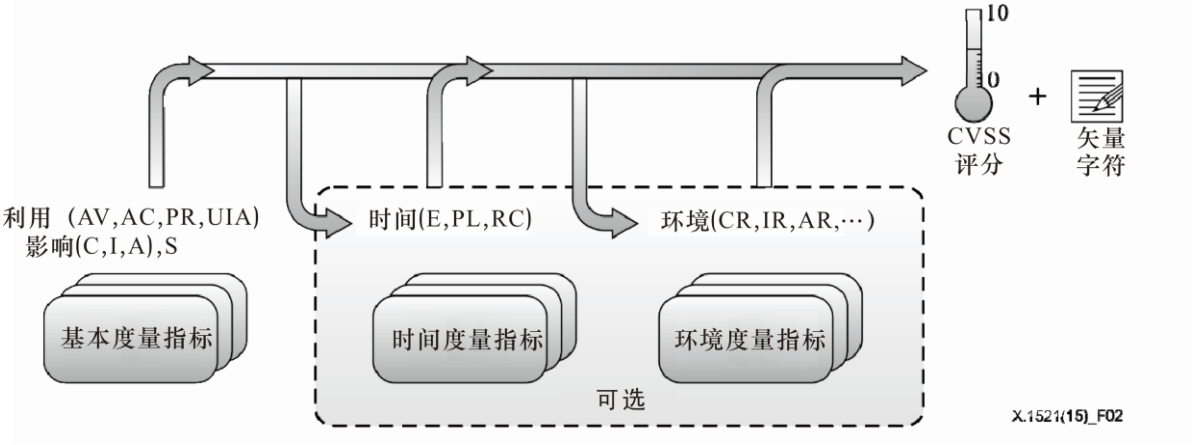


图2 – CVSS度量指标和公式

具体来说，基本公式来源于两个子公式：可利用性子评分公式和影响子评分公式。可利用子评分公式来源于基本可利用性度量指标，而影响子评分公式来源于基本影响度量指标。

之后，可通过给时间和环境度量指标打分的方式对基本分值进行改进，以更准确地反映用户环境所面临的漏洞风险。但并不要求对时间和环境度量指标进行打分。

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，因为通常他们掌握着有关漏洞特性的最准确信息。另一方面，环境度量指标由最终用户组织予以明确，因为他们最有能力评价其自身计算环境中漏洞所带来的潜在影响。

给CVSS度量指标评分还会产生一个矢量字符，即用于漏洞评分的度量指标数值的文字反映。该矢量字符包含为每一度量指标所分配数值的特定格式的文本字符，应永远随漏洞评分显示该矢量。

有关评分公式和矢量字符的更多信息如下。

请注意，在对所有度量指标进行评分时，应假设攻击者已经定位到并找到漏洞。即分析人员无需考虑漏洞是通过何种手段找到的。此外，很有可能还有很多其他的人会对漏洞进行评分（例如，软件厂商、漏洞公告分析人员、安全产品厂商等），然而应注意的是，漏洞评分并不打算被个人及其组织所知。

6.2 基本度量指标

6.2.1 可利用性度量指标

如前所述，可利用性度量指标反映的是易于受到攻击的事物特性，我们将其称为存在漏洞的组件。因此，以下列举的每一个可利用性度量指标均应相对于存在漏洞的组件来评分，反映会引发成功攻击的漏洞特性。

6.2.1.1 攻击矢量（AV）

该度量指标反映的是漏洞可能被利用的背景。攻击者（的逻辑和实际）距离越远，度量指标数值（以及之后的基本评分）则越高，以便利用存在漏洞的组件。假设从互联网另一端利用漏洞的潜在攻击者数量高于需要实际接入设备来利用漏洞的潜在攻击者数量，因此，评分会更高。表1列出了可能的数值。

表1 – 攻击矢量

度量指标值	描述
网络（N）	可通过网络接入利用的漏洞意味着存在漏洞的组件被绑定在网络堆栈上，且攻击者的路径经过开放系统互联（OSI）的第3层（网络层）。此类漏洞通常被称为“远程利用漏洞”，可以想成是一种距离一个或多个网络跃点之外的可利用的攻击（例如，从路由器跨越第3层边界）。网络攻击的示例之一是，攻击者从公共互联网另一端通过发送一个特制的传输控制协议（TCP）包来引发拒绝服务（例如，CVE-2004-0230）。
相邻（A）	可通过相邻网络接入利用的漏洞意味着存在漏洞的组件被绑定在网络堆栈上，但攻击仅限于同一个共享的实际（例如，蓝牙、IEEE 802.11）或逻辑（例如，本地IP子网）网络，无法在OSI第3层边界外操作（例如，路由器）。相邻攻击的示例之一是，地址解析协议（ARP）（IPv4）或邻居发现（IPv6）洪水攻击引起局域网段的拒绝服务。请参见CVE-2013-6014。
本地（L）	可通过本地接入利用的漏洞意味着存在漏洞的组件没有被绑定在网络堆栈上，且攻击者的路径通过读/写/执行能力实现。在某些情况下，攻击者可能会在本地登录，以便利用漏洞，否则就可能需要靠用户交互来执行恶意文件了。
实际（P）	可通过实际接入利用的漏洞需要攻击者实际触碰或操控存在漏洞的组件。实际交互既可以是短暂的（例如，邪恶女仆攻击[1]），也可以是长期的。这类攻击的示例之一是，冷启动攻击允许攻击者在实际接入系统后获取磁盘密钥，或外设攻击，如火线（Firewire）/通用串行总线（USB）内存直接接入攻击。

6.2.1.2 攻击复杂性（AC）

该度量指标描述了超出攻击者控制但必须存在的条件，以便利用漏洞。如下所述，此类条件可能需要收集更多与目标有关的信息、进行特定的系统配置设定或计算特例。重要的是，对本度量指标的评估不需要用户交互就可以利用漏洞（用户交互度量指标中有相关条件描述）。对于复杂性最低的攻击来说，其本度量指标值最大。表2列出了可能的数值。

1 有关邪恶女仆攻击的描述，请登录 https://www.schneier.com/blog/archives/2009/10/evil_maid_attac.html。

表2 – 攻击复杂性

度量指标值	描述
低（L）	不存在专业化的接入条件或情有可原的环境。攻击者可多次成功攻击存在漏洞的组件。
高（H）	成功的攻击取决于超出攻击者控制的条件。即成功的攻击无法随意完成，需要攻击者投入一定量的努力，在成功攻击之前针对存在漏洞的组件做好准备或执行工作。2例如，成功的攻击可能需要攻击者克服以下条件： • 攻击者必须进行针对性的勘察。例如，针对目标的配置设定、序列号、共享秘密等。 • 攻击者必须做好目标环境的准备，以便提高利用的可靠性。例如，通过重复利用来赢得竞赛（race）条件，或克服先进的利用缓解技术。 • 攻击者必须将其自身投入到目标和受害者所需资源之间的逻辑网络路径中，以便读取和/或修改网络通信（如，中间人攻击）。

6.2.1.3 所需特权（PR）

该度量指标描述了攻击者在成功利用漏洞之前必须享有的特权水平。当无需任何特权时，该度量指标最大。表 3 列出了可能的数值。

表3 – 所需特权

度量指标值	描述
无（N）	攻击者在攻击前未得到授权，因此也无需获取任何设置或文件来实施攻击。
低（L）	攻击者被授予（即需要）基本用户能力的特权，通常仅对用户的设置和文件有影响。而拥有低特权的攻击者则可能仅对非敏感性资源带来影响。
高（H）	攻击者被授予（即需要）对存在漏洞的组件执行重大（例如，行政管理）控制的特权，会对整个组件的设置和文件带来影响。

6.2.1.4 用户交互（UI）

该度量指标指出了用户而非攻击者参与成功破坏存在漏洞的组件的要求。该度量指标决定了漏洞是否可以完全按照攻击者的意愿随意被利用，或独立的用户（或用户发起的流程）是否必须以某种方式参与。当无需用户交互时，该度量指标值最大。表4列出了可能的数值。

2 请注意，我们并没有对所需的努力程度提出意见。我们只是觉得必须要多做一些努力，以便利用漏洞。

表4 – 用户交互

度量指标值	描述
无（N）	存在漏洞的系统无需任何用户交互即可被利用。
需要（R）	此类漏洞的成功利用需要用户在漏洞被利用之前采取一些行动。例如，只有在系统管理员安装应用期间才能被成功利用。

6.2.2 范围（S）

CVSS第3.0版本的一个重要特性是能够使一个软件组件的漏洞在超出其手段或特权的情况下对资源产生影响。此类后果用度量指标授权范围或只是范围来表示。

从正式意义上来说，范围指的是计算授权主体（如应用、操作系统或沙盘环境）在授予计算资源（如文件、中央处理器（CPU）、内存等）的获取权限时所定义的特权集合。此类特权通过认证和授权的方式进行分配。在某些情况下，授权可根据预定义的规则或标准被简单或随意控制。例如，当以太网流量发送至网络交换机时，交换机会接受到达其端口的流量，并作为一个授权主体对流向其他交换机端口的流量实行控制。

当某授权范围所管辖的软件组件漏洞影响到另一个授权范围所管辖的资源时，范围就发生了变化。

人们可能会直观地认为，范围的改变意味着脱离沙盘环境，例如虚拟机中的漏洞可以使攻击者删除主机操作系统（OS）上的文件（甚至可能是其自己的虚拟机（VM））。本例中有两个单独的授权主体：一个负责定义和执行虚拟机及其用户特权，另一个负责定义和执行虚拟机运行的主机系统特权。

例如，对于允许攻击者破坏主机操作系统所有系统文件的微软Word漏洞来说，范围不会发生变化，因为是同一个授权主体负责执行用户Word和主机系统文件的特权。

当范围发生变化时，基本分数也会随之提高。表5列出了可能的数值。

表5 – 范围

度量指标值	描述
不变（U）	被利用的漏洞仅能对同一个授权主体所管理的资源产生影响。在这样的情况下，存在漏洞的组件和受影响的组件是同一个组件。
已变（C）	被利用的漏洞可以对超出存在漏洞组件授权特权之外的资源产生影响。在这样的情况下，存在漏洞的组件和受影响的组件不是同一个组件。

6.2.3 影响度量指标

影响度量指标指的是受影响组件的特性。不论被成功利用的漏洞是否对一个或多个组件产生了影响，都会根据后果最严重的组件来对影响度量指标进行评分，此后果与成功攻击之间有着最为直接和可预测的联系。也就是说，分析人员应将影响控制在其相信攻击者能够实现的合理最终结果范围之内。

若范围未发生变化，则影响度量指标应反映出对存在漏洞的组件所产生的保密性、完整性和可用性（CIA）影响。然而，若范围发生了变化，则影响度量指标应反映出对存在漏洞的组件或受影响的组件产生的CIA影响，以遭受结果最为严重的组件为准。

6.2.3.1 保密性影响（C）

该度量指标衡量因漏洞被成功利用而产生的、对软件组件管理的信息资源保密性所产生的影响。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6列出了可能的数值。受影响组件损失越大，该度量指标值越高。

表6 – 保密性影响

度量指标值	描述
高（H）	保密性完全丧失，导致所有受影响组件中的资源泄漏给攻击者。虽然仅可以获取某些受限信息，但泄露的信息却会带来直接、严重的影响。例如，攻击者窃取了管理员的密码或网络服务器的专用密钥。
低（L）	丧失一定的保密性。可以获取某些受限信息，但攻击者对所获得的信息无法控制，或损失的数量或种类有限。信息泄露不会给受影响组件带来直接、严重损失。
无（N）	受影响组件内的保密性没有破坏。

6.2.3.2 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精确性。表7列出了可能的数值。受影响组件的后果越严重，该度量指标值越高。

表7 – 完整性影响

度量指标值	描述
高（H）	完整性被彻底破坏，或保护完全丢失。例如，攻击者能够修改被受影响组件保护的任何/所有文件。虽然仅有一些文件被修改，但恶意修改会给受影响的组件带来直接、严重的后果。
低（L）	可能对数据进行修改，但攻击者无法控制修改的结果，或修改的数量有限。数据修改不会给受影响的组件带来直接、严重的影响。
无（N）	受影响组件内的完整性没有破坏。

6.2.3.3 可用性影响（A）

该度量指标衡量因漏洞成功利用而给受影响组件的可用性造成的影响。保密性和完整性影响度量指标针对的是受影响组件所用数据（例如，信息、文件）的保密性或完整性破坏，而该度量指标指的是受影响组件本身的可用性丧失，例如网络服务（如网络、数据库、电子邮件）。由于可用性系指对信息资源的接入性，因此消耗网络带宽、处理周期或硬盘空间的攻击都会影响到受影响组件的可用性。表8列出了可能的数值。受影响组件的后果越严重，该度量指标值越高。

表8 – 可用性影响

度量指标值	描述
高（H）	可用性彻底丧失，造成攻击者能够完全拒绝对受影响组件资源的获取；该损失既可以是持续的（当攻击者持续发起攻击），也可以是长期的（即使攻击结束，情况仍然存在）。虽然攻击者有能力拒绝某些可用性，但可用性的丧失会给受影响组件带来直接、严重的后果（例如，攻击者无法中断现有的连接，但可以阻止新的连接；攻击者可以多次利用同一个漏洞，每次成功攻击时，仅泄露少量的内存，但多次利用后则会造成服务完全不可用）。
低（L）	性能降低或资源可用性受到干扰。即使可能多次利用漏洞，但攻击者不能完全向合法用户拒绝服务。受影响组件中的资源要么总是部分可用，要么在某些时间全部可用，但总体上来说不会给受影响组件带来直接、严重的后果。
无（N）	对受影响组件内的可用性没有影响。

6.3 时间度量指标

该度量指标衡量利用技术或代码可用性的现状、补丁或变通措施是否存在或对漏洞描述的把握。

6.3.1 利用代码成熟度（E）

该度量指标衡量漏洞被攻击的可能性，通常以利用技术、利用代码可用性或活跃、“自由”利用的现状为基础。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或其他自动攻击工具的有效荷载加以提供。

表9列出了可能的数值。漏洞越易于被利用，漏洞评分越高。

表9 – 利用代码成熟度

度量指标值	描述
未定义（X）	为度量指标分配该数值不会影响评分，它只是向评分公式表明略过该度量指标。
高（H）	存在实际运行的自治代码，或不要求利用（人工触发），且大范围提供细节。利用代码在任何情况下均有效，或通过自治代理（如蠕虫或病毒）被大量提供。联网系统可能遭遇扫描或利用的尝试。利用已经发展到可靠、广泛可用和便于使用的自动工具水平。

表9 – 利用代码成熟度

度量指标值	描述
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。
概念验证（P）	存在概念验证利用代码，或攻击演示对多数系统并不切实可用。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。
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。

6.3.2 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10列出了可能的数值。修复措施越不正式或固定，漏洞评分越高。

表10 – 补救程度

度量指标值	描述
未定义（X）	为度量指标分配该数值不会影响评分，它旨在向评分公式表明略过该度量指标。
未提供（U）	未提供解决方案或无法应用解决方案。
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。
临时修复（T）	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。
正式修复（O）	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）。

6.3.3 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。例如，影响可以被认为是不良的影响，但根源却可能是未知的。之后漏洞可能被研究证实，指出漏洞的位置，尽管研究也可能无法肯定。最后，漏洞可能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11列出了可能的数值。漏洞越能被厂商或其它知名渠道证实，评分越高。

表11 – 报告把握性

度量指标值	描述
未定义（X）	为度量指标分配该数值不影响评分，它只向评分公式说明略过该度量指标。
确认（C）	存在详细的报告或可能实际运行的副本（实际运行的利用可以提供）。有源代码来独立证实研究论断，或作者或受影响代码的厂商确认了漏洞的存在。
合理（R）	已公布了大量的细节，但研究人员要么对根源没有完全的把握，要么无法获得源代码来充分确认所有会引起后果的交互。然而，合理的信心是存在的，认为漏洞可以被复制，至少能证实一种影响（概念验证的利用可以提供）。示例之一是一份有关漏洞的详细研究报告，并附有相关解释（可能较为模糊或“留给读者思考”），确认结果的复制方式。
未知（U）	很多的影响报告指出，漏洞是存在的，且漏洞的原因未知，或各报告中的漏洞原因或影响各不相同。报告人员对于漏洞的真实本质并不肯定，对于报告的有效性或静态基本评分在存在上述差异的情况下是否能够得到应用也没有把握。示例之一是，漏洞报告注意到，当发生间歇性且不可复制的崩溃问题时，由于有证据证明内存被破坏，因此会造成拒绝服务或更严重的影响。

6.4 环境度量指标

这些度量指标有助于分析人员按照受影响的IT资产对用户组织的重要程度为用户定制（customize）CVSS评分体系，并从已实行的补充性/替代性安全控制、保密性、完整性和可用性方面加以衡量。该度量指标相当于对基本度量指标的修改，并在组织基础设施中的组件安置基础上分配度量指标值。

6.4.1 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信息技术（IT）资产对用户组织的重要程度为用户定制（customize）CVSS评分体系，并从保密性、完整性和可用性方面加以衡量。也就是说，如果IT资产支持的业务功能中可用性是最重要的，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修改后的基本影响度量指标。也就是说，这些度量指标通过重新对修改后的保密性、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，则修改后的保密性影响（C）度量指标的权重增加。同样，如果保密性要求低，则修改后的保密性影响度量指标的权重减轻。如果保密性要求为中等，则修改后的保密性影响度量指标的加权为中等。同样的流程也适用于完整性和可用性要求。

请注意，如果（修改后的基本）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（修改后的基本）影响度量指标设为高时也不会改变环境评分。这是因为修改后的影响子评分（计算影响的修改后基本评分的一部分）已经为最大值10。

表12列出了可能的数值。为简化工作，该表用于所有三个度量指标。安全要求越高，评分越高（请牢记中等要求被视为是默认要求）。

表12 – 安全要求

度量指标值	描述
未定义（X）	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。
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。
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。
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。

6.4.2 修改后的基本度量指标

此类度量指标有助于分析人员根据其环境内部的修改来调整基本度量指标。也就是说，如果环境对受影响的软件做了一般性改变，与影响其可利用性、范围或影响的方式不同，则环境可以通过一个合理修改的环境评分来对此加以反映。

对环境评分的总体影响取决于相应的基本度量指标。也就是说，这类度量指标在应用（环境）安全要求之前通过重新分配（基本）度量指标值来修改环境评分。例如，某漏洞组件的默认配置可能是在管理员特权的情况下运行倾听服务，对此，破坏可能会给攻击者带来高保密性、完整性和可用性影响。然而，在分析人员的环境下，同样的互联网服务则可能在更低的特权下运行；在这种情况下，修改后的保密性、修改后的完整性和修改后的可用性可能均应设为低。

为简化工作，仅提及修改后的基本度量指标的名称。每一个修改后的环境度量指标和其相应的基本度量指标具有同样的数值，再加一个未定义值。

该度量指标的目的在于对给定环境中已实行的缓解进行定义。可以使用修改后的度量指标来对提高基本评分的情况进行描述。例如，某组件的默认配置可能需要高特权（PR：高）来获得某功能，但在分析人员的环境下，可能不需要任何特权（PR：无）。分析人员可以把MPR设为无来反映其环境的更严重情况。

表13列出了可能的数值。

表13 – 修改后的基本度量指标

修改后的基本度量指标	相应的数值
修改后的攻击矢量（MAV）	与相应的基本度量指标（见上述基本度量指标）数值一样，再加上未定义（默认）
修改后的攻击复杂性（MAC）	
修改后的所需特权（MPR）	
修改后的用户交互（MUI）	
修改后的范围（MS）	
修改后的保密性（MC）	
修改后的完整性（MI）	
修改后的可用性（MA）	

6.5 定性严重性评级数值范围

出于某些目的，用文字来表示数值型基本、时间和环境评分很有用。所有的评分均可映射在表14的定性评级中。[3]

表14 – 定性严重性评级数值范围

评级	CVSS评分
无	0.0
低	0.1 – 3.9
中	4.0 – 6.9
高	7.0 – 8.9
严重	9.0 – 10.0

例如，4.0的CVSS基本评分相当于中级严重性评级。此类定性严重性评级并非强制性使用，在公布CVSS评分时无需将其纳入。评级的目的在于帮助机构合理地评估其漏洞管理流程，并排定轻重缓急。

6.6 矢量字符

CVSS第3.0版本是整套CVSS度量指标的文字体现。通常用于对CVSS度量指标信息的简明记录或转移。

第3.0版本的矢量字符以“CVSS：”开始，以及当前版本的数字型体现“3.0”。度量指标信息以一套度量指标的形式紧随其后，每一个度量指标前有一个正斜杠“/”，作为分隔符。每一个度量指标均为其缩写形式，一个冒号“：”，以及其相应度量指标值的缩写形式。本技术规范在前面的内容中已经对缩写形式进行了定义（每一个度量指标名称和度量指标值后的圆括号中），总结如下表。

[3] 请注意，定量和定性评分之间的这种映射适用于仅对基本度量组进行评分的情况，也适用于对所有基本、时间和环境度量组评分的情况。

度量指标在矢量字符中可以任何顺序体现，尽管表15展示的是推荐顺序。所有的基本度量指标必须都纳入矢量字符中。而时间和环境度量指标则不一定，省略的度量指标归入未定义（X）值。若需要，未定义值的度量指标也可明确纳入矢量字符中。程序读取第3.0版本矢量字符必须接受任何顺序的度量指标，并将未明确的时间和环境视为未定义。同一个度量指标不得在同一个矢量字符中出现两次。

表15 – 基本、时间和环境矢量

度量组	度量指标名称 与缩写形式	可能的数值	是否强制？
基本	攻击矢量，AV	[N,A,L,P]	是
	攻击复杂性，AC	[L,H]	是
	所需特权，PR	[N,L,H]	是
	用户交互，UI	[N,R]	是
	范围，S	[U,C]	是
	保密性，C	[H,L,N]	是
	完整性，I	[H,L,N]	是
	可用性，A	[H,L,N]	是
时间	利用代码成熟度，E	[X,H,F,P,U]	否
	补救程度，RL	[X,U,W,T,O]	否
	报告把握性，RC	[X,C,R,U]	否
环境	所需保密性，CR	[X,H,M,L]	否
	所需完整性，IR	[X,H,M,L]	否
	所需可用性，AR	[X,H,M,L]	否
	修改后的攻击矢量，MAV	[X,N,A,L,P]	否
	修改后的攻击复杂性，MAC	[X,L,H]	否
	修改后的所需特权，MPR	[X,N,L,H]	否
	修改后的用户交互，MUI	[X,N,R]	否
	修改后的范围，MS	[X,U,C]	否
	修改后的保密性，MC	[X,N,L,H]	否
	修改后的完整性，MI	[X,N,L,H]	否
	修改后的可用性，MA	[X,N,L,H]	否

例如，基本度量指标值为“攻击矢量：网络，攻击复杂性：低，所需特权：高，用户交互：无，范围：不变，保密性：低，完整性：低，可用性：无”的漏洞，且没有明确的时间或环境度量指标会产生如下矢量：

– CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N

同样的例子还可以再加上“可利用性：实际运行，补救程度：未定义”，且未遵循推荐顺序的度量指标会产生如下矢量：

– CVSS:3.0/S:U/AV:N/AC:L/PR:H/UI:N/C:L/I:L/A:N/E:F/RL:X

6.7 CVSS第3.0版本XML架构定义

CVSS XML架构定义（XSD）定义了包括CVSS度量指标值的XML文件结构，对于想要存储或转移XML格式的此类数据很有用。可在以下网址获取XSD：https://www.first.org/cvss/cvss-v3.0.xsd。

6.8 CVSS第3.0版本公式

CVSS第3.0版本的公式定义如下。

6.8.1 基本

基本评分是影响和可利用性子评分公式的函数。当基本评分定义为，

If (Impact sub score <= 0) 0 *else,*

Scope Unchanged [4] $Roundup(Minimum[(Impact + Exploitability), 10])$

Scope Changed $Roundup(Minimum[1.08 \times (Impact + Exploitability), 10])$

影响子评分（ISC）定义为，

Scope Unchanged $6.42 \times ISC_{Base}$

Scope Changed $7.52 \times [ISC_{Base} - 0.029] - 3.25 \times [ISC_{Base} - 0.02]^{15}$

当，

$$ISC_{Base} = 1 - \left[\left(1 - Impact_{Conf}\right) \times \left(1 - Impact_{Integ}\right) \times \left(1 - Impact_{Avail}\right)\right]$$

可利用性子评分为，

$$8.22 \times AttackVector \times AttackComplexity \times PrivilegeRequired \times UserInteraction$$

6.8.2 时间

时间评分定义为，

$$Roundup(BaseScore \times ExploitCodeMaturity \times RemediationLevel \times ReportConfidence)$$

6.8.3 环境

环境评分定义为，

If (Modified Impact Sub score <= 0) 0 else,

If Modified Scope is Unchanged *Round up(Round up (Minimum [× (M.Impact + M.Exploitability) ,10]) × Exploit Code Maturity × Remediation Level × Report Confidence)*

---

4 当“向上舍入”被定义为最小的数字并保留小数点后一位时，则等于或高于其输入。例如，（4.02）向上舍入为4.1；（4.00）向上舍入为4.0。

If Modified Scope is Changed *Round up(Round up (Minimum [1.08 × (M.Impact + M.Exploitability) ,10]) × Exploit Code Maturity × Remediation Level × Report Confidence)*

修改后的影响子评分定义为，

If Modified Scope is Unchanged $6.42 \times [ISC_{Modified}]$

If Modified Scope is Changed $7.52 \times [ISC_{Modified} - 0.029]$-$3.25 \times [ISC_{Modified} - 0.02]^{15}$

当

$$ISC_{Modified} = Minimum\left[\left[1 - \left(1 - M.I_{Conf} \times CR\right) \times \left(1 - M.I_{Integ} \times IR\right) \times (1 - M.I_{Avail} \times AR)\right], 0.915\right]$$

修改后的可利用性子评分为，

$$8.22 \times M.AttackVector \times M.AttackComplexity \times M.PrivilegeRequired \times M.UserInteraction$$

6.8.4 度量指标等级

度量指标值定义如表16所示。

表16 – 度量指标值

度量指标	度量指标值	数值
攻击矢量 / 修改后的攻击矢量	网络	0.85
	相邻网络	0.62
	本地	0.55
	实际	0.2
攻击复杂性 / 修改后的攻击复杂性	低	0.77
	高	0.44
所需特权 / 修改后的所需特权	无	0.85
	低	0.62（0.68若范围/修改后的范围发生了变化）
	高	0.27（0.50若范围/修改后的范围发生了变化）
用户交互 / 修改后的用户交互	无	0.85
	需要	0.62
C,I,A影响 / 修改后的C, I, A影响	高	0.56
	低	0.22

度量指标	度量指标值	数值
	无	0
利用代码成熟度	未定义	1
	高	1
	实际运行	0.97
	概念验证	0.94
	未证实	0.91
补救程度	未定义	1
	未提供	1
	变通措施	0.97
	临时修复	0.96
	正式修复	0.95
报告把握性	未定义	1
	确认	1
	合理	0.96
	未知	0.92
安全要求 – C, I, A要求（CR）	未定义	1
	高	1.5
	中	1
	低	0.5

6.8.5 关于CVSS第3.0版本公式和评分

CVSS第3.0版本方程为按严重性顺序排列的所有可能的度量指标组合提供了一种数学近似法（漏洞查询表）。为了得到CVSS第3.0版本的方程，SIG通过给真实漏洞分配第3.0版本度量指标值的方式制订了查询表（lookup table），和严重性分组（低、中、高、严重）。给每一个严重性层级定义了可接受的数字范围之后，SIG与德勤（Deloitte & Touche LLP）合作调整方程参数，使第3.0版本的度量指标组合与SIG提议的严重性评级保持一致。

鉴于数字结果有限（101个结果，范围从0.0至10.0），多个评分组合可能会产生同样的数字评分。此外，可能会省略一些数字评分，因为加权和计算来源于度量指标组合的严重性排序。另外，在某些情况下，度量指标组合可能会偏离期望的严重性阈值。这是不可避免的，现在也没有一个简单的纠正方法，因为为了修正偏差而调整某一个度量指标值或公式参数会引起其他潜在的更严重的偏差。

经一致同意，正如CVSS第2.0版本所做的那样，可接受的偏差值为0.5。也就是说，所有用于加权和计算的度量指标值组合会在其分配的严重层级之内或所分配层级的0.5偏差之内产生一个数字评分。例如，预期会评为“高”的组合可能会得到6.6和9.3之间的一个数字评分。最终，CVSS第3.0版本会保留0.0至10.0的范围用于向后兼容。

附录I

CVSS第3.0版本用户手册

（本附件不是本建议书的组成部分。）

I.1 引言

本手册作为CVSS第3.0版本官方技术规范文件的补充提供了更多的信息，强调与第2.0版本的不同，还提供了评分指南和评分流程图。

共同漏洞评分系统（CVSS）提供了一种捕获漏洞主要特性的方法，得出反映其严重性的数字评分以及该评分的文字表示。之后，数字评分可以转换为定性表达（如低、中、高和严重），帮助机构合理地评估其漏洞管理流程，并排定轻重缓急。

CVSS有三大益处：

– 标准化的漏洞评分。当一个组织用通用算法来对所有IT平台的漏洞进行评分时，该组织可充分实现漏洞统一管理政策的优势，确定某漏洞验证和补救的最长允许时间。

– 开放框架。如果由第三方随意对漏洞进行评分，用户会感到困惑。通过CVSS，得出评分的具体特性将变得透明。

– CVSS有助于排定风险的轻重缓急。在计算环境评分时，漏洞对于每一个组织来说都具有了语境背景，可以更好地了解该漏洞给组织带来的风险。

自2004年首次发布以来，CVSS已被广泛采纳。2007年9月，CVSS第2.0版本被支付卡行业数据安全标准（PCI DSS）采用。为了符合PCI DSS的要求，商家处理信用卡必须表明他们计算系统漏洞的CVSS评分均不大于等于4.0。2007年，国家标准与技术研究院（NIST）将CVSS第2.0版本纳入其安全内容自动化协议（SCAP）。[5] 2011年4月，CVSS第2.0版本作为国际漏洞评分标准被正式采纳（ITU-T X.1521）。[6]

I.2 CVSS第3.0版本中的变化

鉴于CVSS第2.0版本已被广泛采纳，我们也发现了很多可以改进的地方，并就此制定了第3.0版本。详细内容如下。

I.2.1 范围、存在漏洞的组件和受影响的组件

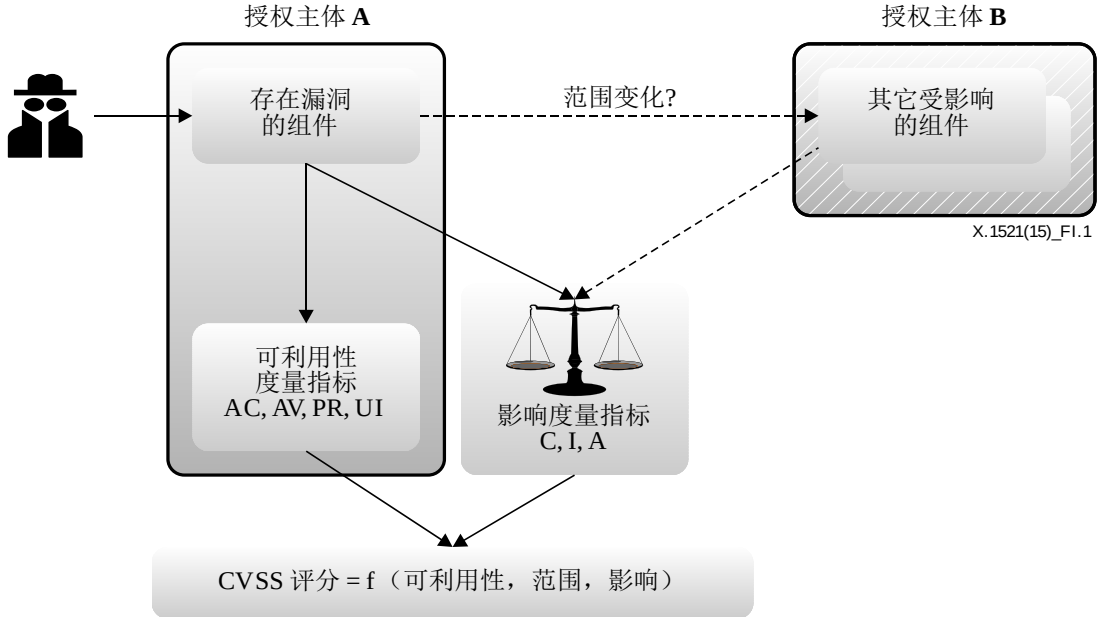
CVSS第2.0版本在给会完全破坏其软件的漏洞评分时给厂商造成了一些困难，但仅对主机操作系统产生部分影响。在第2.0版本中，漏洞在相对于主机操作系统的情况下进行评分，使应用厂商采用“部分+”影响度量指标惯例。[7] CVSS第3.0版本解决了这一问题，对影响度量指标的评分位置进行了更新，引入了范围这一新度量指标（详细内容如下）。因此，CVSS第3.0版本一个重要的概念性变化就是能够对存在于某软件组件（我们将其称为*存在漏*

5 请参见 http://scap.nist.gov/。

6 请参见 https://www.itu.int/rec/T-REC-X.1521-201104-I/en。

7 例如，请参见 http://www.oracle.com/technetwork/topics/security/cvssscoringsystem-091884.html。

洞的组件）、但却会影响另外一个软件、硬件或组网组件（我们将其称为受影响的组件）的漏洞进行评分，如图I.1所示。[8]



图I.1 – 范围变化

例如，虚拟机中有一个破坏主机操作系统的漏洞。那么存在漏洞的组件就是虚拟机，而受影响的组件则是主机操作系统。由于这两个组件分别独立管理计算资源特权，因此它们代表不同的（授权）主体。在图I.1中，虚拟机由“授权主体A”管理，而主机操作系统由“授权主体B”管理。当两大授权主体参与到漏洞利用中时，CVSS就会认为范围发生了变化。这种情况由新的度量指标来表示，即范围。

正如图I.1所示，在CVSS第3.0版本给漏洞评分时，可利用性度量指标是相对于存在漏洞的组件来进行评分的。也就是说，在评分时要考虑存在编码缺陷的组件。另一方面，影响度量指标是相对于受影响的组件来进行评分的。在某些情况下，存在漏洞的组件可能和受影响的组件是同一个组件，在这种情况下，则不会发生范围变化。然而，在其他情况下，可能对存在漏洞的组件和受影响的组件都有影响。这时，范围就会发生变化，且保密性、完整性和可用性影响度量指标应反映出对存在漏洞的组件或受影响的组件所产生的影响，以最为严重的一方为准。

在漏洞允许盗取密码文件的情况下，攻击者可能会采取后续行动来进入未授权账户，最直接的结果就是本地系统文件保密性的丧失。这种情况下，范围不会发生变化。然而，在漏洞允许路由器的ARP表被攻击者重写时，会带来两种影响。第一，路由器的系统文件（对存在漏洞组件的完整性带来影响）；第二，路由器所服务的互联网服务（对受影响系统的可用

8 请注意，存在漏洞的组件是软件程序（主机操作系统、互联网应用、设备驱动等），而受影响的组件则可以是另一个软件程序、硬件设备或网络资源。

性带来影响）。由于评分应反映最严重的结果，因此影响度量指标评分要么反映出存在漏洞组件的完整性损失，要么反映出互联网服务的可用性损失，以更严重的一方为准。[9]

I.2.2 接入矢量

接入矢量（来自第2.0版本）被重新命名为攻击矢量，但仍反映的是攻击者相对于存在漏洞组件的“远近”。也就是说，攻击者离存在漏洞的组件越远（逻辑和实际网络距离），基本评分越高。此外，该度量指标现在可以区分需要本地系统接入的本地攻击（如针对桌面应用的攻击）和需要实际接入平台的实际攻击，以利用漏洞（如火线（firewire），USB或越狱（jailbreaking）攻击）。

I.2.3 攻击复杂性

接入复杂性（来自第2.0版本）包含两个问题：为了成功利用漏洞而必须存在或发生的、超出攻击者控制的任何软件、硬件或组网条件（例如，软件竞赛条件或应用配置），以及人类交互的需求（例如，需要用户执行一个恶意可执行程序）。因此，接入复杂性分为两个度量指标，攻击复杂性（针对前一种情况）和**用户交互**（针对后一种情况）。

I.2.4 所需特权

所需特权这一新度量指标代替了第2.0版本中的认证度量指标。攻击者必须单独向系统认证，所需特权指的是成功攻击所需的接入等级，而非衡量次数。具体来说，高、低和无这几个度量指标值反映的是攻击者利用漏洞所需的特权。

I.2.5 影响度量指标

第2.0版本中无、部分和完全这几个**保密性、完整性和可用性影响**度量指标值已被无、低和高所代替。新的度量指标值反映的是攻击所造成的总体影响程度，而非攻击影响的总体系统百分比（比例）。例如，虽然心脏出血（Heartbleed）[10]漏洞仅造成少量信息丢失，但影响却很严重。在CVSS第2.0版本中，会被评为部分，而在CVSS第3.0版本中则会被评为高。

除此之外，在上述示例中，影响度量指标现在反映的是受影响组件的后果。而受影响组件与含有被利用漏洞的组件可以是、也可以不是同一个组件。

I.2.6 时间度量指标

相对于第2.0版本，第3.0版本中时间度量指标的影响有所下降。可利用性更名为利用代码成熟度，以便更好地表示度量指标所衡量的对象。

I.2.7 环境度量指标

环境度量指标的目标分布和潜在附带损害被修改后的因素所代替，包括缓解控制或控制存在于用户环境中的弱点，以免削弱或增强被成功利用的漏洞的影响。

---

9 更多信息，请参见本指南随附的示例文件。

10 见 http://heartbleed.com/。

I.2.8 定性评级数值范围

一些机构创建了系统，将CVSS第2.0版本的基本评分映射到定性评级中。现在，CVSS第3.0版本提供了一个标准化的方式，将数字评分映射到严重性评级中，包括无、低、中、高和严重这几个级别，具体信息请参见CVSS第3.0版本的技术规范文件。此类定性严重性评级并非强制性使用，在公布CVSS评分时无需将其纳入。

使用CVSS第3.0版本评分的同时还想要交替使用严重性评级系统的机构需使用不同的评级术语或明确指出其评级与CVSS第3.0版本技术规范不符，以避免混淆。

I.2.9 变化小结

这些变化的一个重要结果就是，第2.0版本和第3.0版本的评分可能并不总是具有可比性。例如，会造成彻底破坏的漏洞应用在第2.0版本中会被评为部分保密性、完整性和可用性影响度量指标值。而在第3.0版本中，同样的漏洞则会在同等的保密性、完整性和可用性影响度量指标值下被评为高。

第2.0版本变化总结如下表I.1所示。

表I.1 – CVSS第2.0版本到第3.0版本的变化

第2.0版本	第3.0版本
相对于主机平台的总体影响对漏洞进行评分。	现在是相对于受影响组件的影响对漏洞进行评分。
没有意识到某应用中的漏洞会影响到同一系统的其他应用。	当前新增的范围这一度量指标包含在*受影响事物*（受影响的组件）和*存在漏洞事物*（存在漏洞的组件）并非同一事物时的漏洞。
接入矢量可能将需要本地系统接入的攻击和实际硬件攻击进行了合并。	现在，攻击矢量度量指标将本地和实际值分开描述。
在某些情况下，接入复杂性将系统配置和用户交互进行了合并。	该度量指标分成了攻击复杂性（描述系统复杂性）和用户交互（描述用户在成功攻击中的参与）。
在实际情况下，认证度量指标评分会偏向于三个可能结果中的两个，无法有效捕获所期待的漏洞特性。	所需特权作为一项新的度量指标代替了认证，现在反映的是攻击者所需的最大特权，而不是攻击者必须认证的次数。
影响度量指标反映的是存在漏洞应用所遭受的影响百分比。	现在的影响度量指标值则反映的是影响的程度，并被重命名为无、低和高。
目标分布和潜在附带损害的环境度量指标并无用处。	目标分布和潜在附带损害被缓解因素所代替。
CVSS第2.0版本无法对用于同一攻击的多个漏洞评分。	虽然不是正式的度量指标，但漏洞串联为多漏洞评分提供了指南。
无正式的定性评分指南。	数字范围被映射到5分制的定性评级数值范围中。

I.3 评分指南

以下是给分析人员在用CVSS第3.0版本对漏洞进行评分时的一系列建议。

I.3.1 利用生命周期内的CVSS评分

分析人员在了解何时对漏洞的影响进行评分时应将影响限制在其相信攻击者能够实现的合理最终影响范围内。造成该影响的能力应得到最低可利用性子评分的支持，但也可以包括来自漏洞描述的细节信息。例如，思考以下两个漏洞：

在漏洞1中，远程未认证的攻击者可以向网络服务器发送一个微小的特制请求，使网络服务器泄露根（管理员）账户的纯文本密码。分析人员仅能从可利用性子评分度量指标和漏洞描述中得知攻击者可以向网络服务器发送特制请求，以便利用漏洞。影响应到此为止；虽然攻击者**可能**有能力将这些凭证用于此后以管理员身份执行代码，但无法得知攻击者是否能够获取登录提示或方法，以便用此类凭证来执行命令。获取该密码仅意味着保密性的直接、严重损失：

- 基本评分：7.5 [CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N]。

在漏洞2中，本地低特权用户可以向操作系统发送一个微小的特制请求，使其泄露根（管理员）账户的纯文本密码。分析人员能从可利用性子评分度量指标和漏洞描述中得知攻击者可以接入操作系统，可以本地低特权攻击者身份登录。获取该密码会给保密性、完整性和可用性带来直接、严重的损失，因为分析人员可以根/管理员账户合理地发出命令（假定攻击者可以从其自己的账户登出，再以根账户登录）：

- 基本评分：7.8 [CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H].

I.3.2 保密性和完整性与可用性的影响对比

保密性和完整性度量指标指的是对服务所用数据的影响。例如，被恶意篡改的网络内容，或被窃取的系统文件。可用性影响度量指标指的是服务的运行。也就是说，可用性度量指标针对的是服务本身的表现和运行 – 而非数据的可用性。可以思考一下，网络、电子邮件或域名系统（DNS）等互联网服务的漏洞允许攻击者修改或删除名录中的所有网络文件，这仅会对完整性产生影响，而非可用性。原因是网络服务仍然在正常运行 — 只是服务于修改后的内容。

I.3.3 被远程攻击者利用的本地漏洞

在CVSS第2.0版本中，打分技巧5指出：“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。”该指南有时会带来混淆，比如攻击者欺骗用户从远程网络服务器下载一份错误格式的文件，利用文件解析漏洞。在此情况下，使用CVSS第2.0版本的分析人员会将此类漏洞视为“网络”，其评分度量指标字符为：

- AV:N/AC:M/Au:N/C:P/I:P/A:P, or AV:N/AC:M/Au:N/C:C/I:C/A:C。

CVSS第3.0版本对该指南进行了改进，阐明了攻击矢量度量指标的网络和相邻值的定义。具体来说，只有当漏洞被绑定在网络堆栈上时，分析人员才应对网络或相邻评分。需要用户交互进行下载或接收恶意内容（也可通过本地提供，例如通过USB盘）的漏洞应被评为本地。

例如，不依赖网络即可被利用的文件解析漏洞通常应被评为本地值，不论使用何种方法分发该恶意文件（如可以是网站链接或通过USB盘）。

I.3.4 跨址脚本漏洞

在CVSS第2.0版本中，需要具体的指南来得出不为零的跨址脚本（XSS）漏洞评分，因为漏洞的评分是相对于含有漏洞的主机操作系统进行的。由于修改了网络服务器对客户的回应，通常情况下XSS漏洞的评分描述的是部分完整性影响：AV:N/AC:M/Au:N/C:N/I:P/A:N。这一点甚至适用于基于文档对象模型（DOM）的跨址脚本（XSS）漏洞，虽然可能因与服务器的交互而引发，但却在客户端被完全利用（例如，当服务器提供的JavaScript解析发送给服务器的请求字符时）。

这是范围设计时的关键场景之一 – 并不是存在漏洞的组件（例如，网络服务器，或网络服务器所提供的JavaScript）受到了影响，而是特权被单独授权主体所管理的组件受到影响（例如，客户的浏览器环境）。因此，在CVSS第3.0版本下，跨址脚本漏洞不一定要限制于给服务器造成的有限或不存在的影响，现在也可以对客户所受到的影响进行评分。对于允许攻击者向受害者提供恶意链接和在其浏览器中执行JavaScript的反射性XSS漏洞也可以进行评分：

– CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

I.3.5 中间人

现在，CVSS第3.0版本明确包含了对中间人攻击的评分。虽然在第2.0版本中并没有具体体现，但在第3.0版本中该类攻击是由攻击复杂性度量指标所表示的。

I.3.6 硬件漏洞

此外，虽然CVSS主要是针对软件的漏洞和影响进行评分的，但现在的第3.0版本也更适合于给包括硬件组件在内的影响和组网影响进行评分。

I.3.7 漏洞串联

CVSS主要对单个的漏洞进行分类和评级。然而，支持整个漏洞分析群体的需求也很重要，将在单一攻击破坏主机或应用过程中被利用的多个漏洞的情况纳入进来。这种对多个漏洞的评分就叫做漏洞串联。请注意，这并不是一个正式的度量指标，只是涵盖在内，为分析人员对这类攻击进行评分提供指南。

在对一系列漏洞进行评分时，分析人员有责任确定究竟要把哪些漏洞组合起来进行串联评分。分析人员应将串联评分与各个漏洞及其评分一并列举出来。例如，可以在网页上的漏洞泄露公告中进行告知。

此外，分析人员也可把其他可以与已评分漏洞串联起来的相关漏洞纳入进来。具体来说，分析人员可以把通常会串联在一起的普遍性（或类）相关漏洞列举出来，或进一步描述必须存在的所需前提。例如，可以描述一下某些种类的结构化查询语言（SQL）注射漏洞是如何引发跨址脚本（XSS）攻击的，或某种缓冲溢出是如何授予本地特权的。列举出一些普遍性或普遍类的漏洞能够作为最少的必要信息，向其他用户发出警告，且不会让攻击者得知新的利用机会。

另外，分析人员还可以（通过机器可读、可解析的漏洞列表形式，如共同漏洞暴露（CVE）识别码（ID）或共同缺陷列表（CWE））完整的列举出一些已知的、与（或者可能与）一个或多个已评分的串联漏洞相串联的具体漏洞，以便利用IT系统。若某漏洞只有在其他前提条件都满足的情况下才能被利用（如第一次利用另一个漏洞），则可以把两个或多个CVSS评分相结合，通过给最低限制的可利用性子评分度量指标和最大影响的影响子评分度量指标评分来描述漏洞串联。以下示例即利用了可利用性、范围和影响子评分来描述串联：

漏洞A：AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H，从矢量可见，需要本地低特权用户，以便利用。而对于漏洞B：AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L，使远程无特权攻击者能够在需要用户交互来完成攻击的情况下在低影响系统上执行代码。因此，鉴于A和B，串联C可以被描述为B -> A的串联：AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H，将B的可利用性和A的影响结合起来，两者的范围均为发生变化，因为如果可以利用B并作为本地用户从中获得代码执行，也就可以满足此后发布A的前提条件，使漏洞A产生影响。

I.4 术语表

授权主体：授予和管理资源特权的计算容器。授权主体的示例包括，数据库应用、操作系统和沙盘环境。

串联评分：给两个或多个串联漏洞评分所得出的基本分数。

串联漏洞：请参见漏洞串联。

组件：软件或硬件组件。

软件组件：包含待执行计算机指令的软件程序或模块。例如，操作系统、互联网应用、设备驱动。

硬件组件：实际计算设备。

受影响的组件：遭受被利用漏洞后果的（一个或多个）组件。可以与存在漏洞的组件是同一个组件，也可以在范围发生变化的情况下不是同一个组件。

特权：对接入计算资源进行定义的、授予用户或用户流程的（通常为读、写和执行）权利集合。

资源：计算设备所接入、修改或消耗的软件或网络对象。例如，计算机文件、内存、CPU 周期或网络带宽。

范围：在授予计算资源的接入时由授权主体定义和管理的特权集合。

漏洞：软件（或硬件）组件的弱点或缺陷。

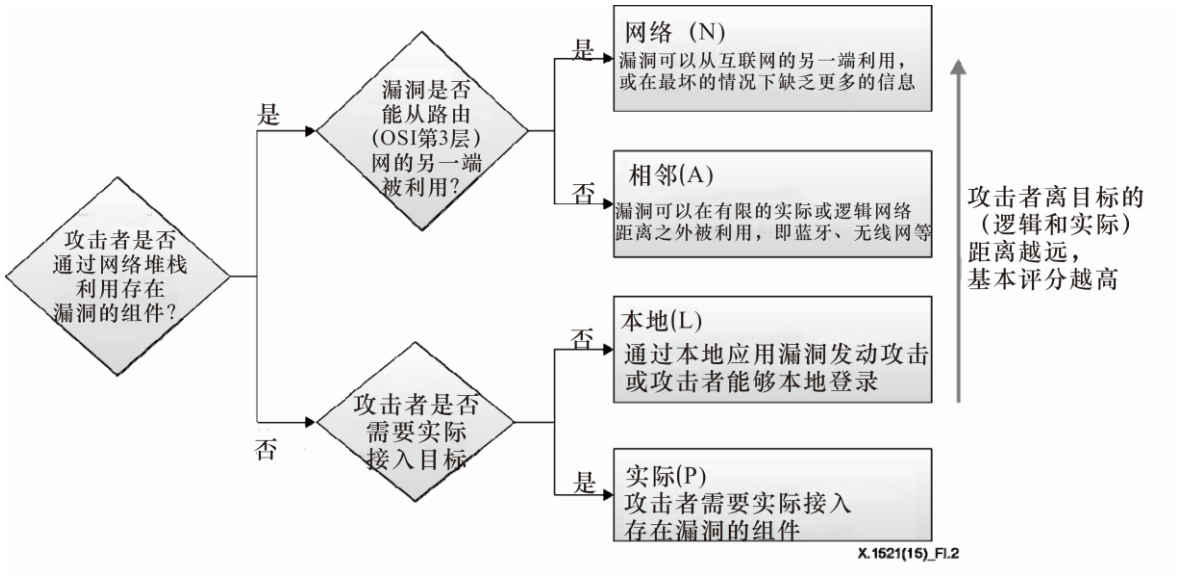
漏洞串联：为攻击 IT 系统而对多个漏洞的有序利用，串联尾端的一个或多个利用需要在之前的利用成功完成之后才能实现。定义还可参见以下网址 http://cwe.mitre.org/documents/glossary/#Chain。

存在漏洞的组件：含有漏洞并将被修补的软件（或硬件）组件。

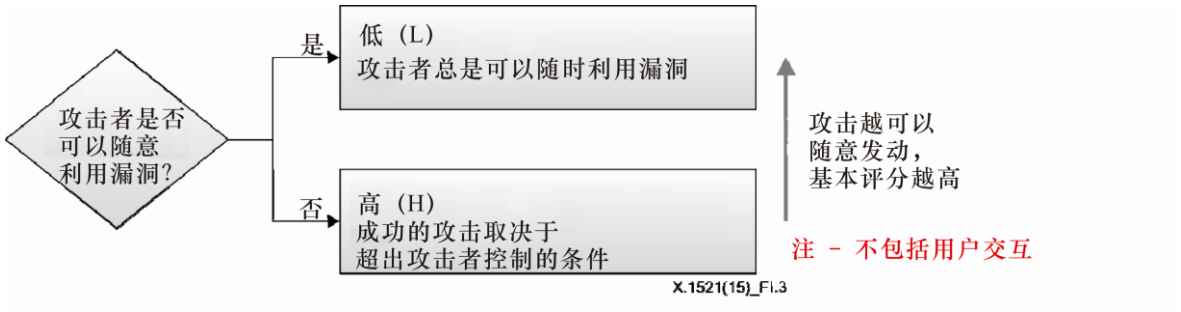
I.5 评分流程图

评分流程图为第 3.0 版本中的漏洞评分提供了一个快速参考，作为技术规范文件中现有评分内容的补充。

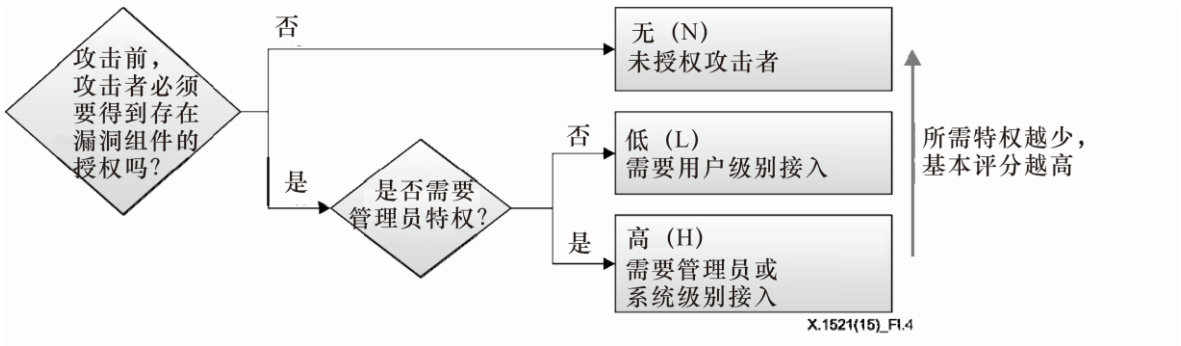
I.5.1 攻击矢量



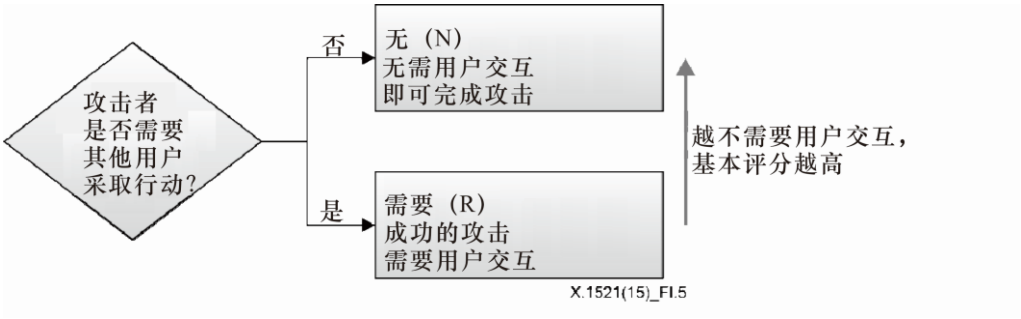
I.5.2 攻击复杂性



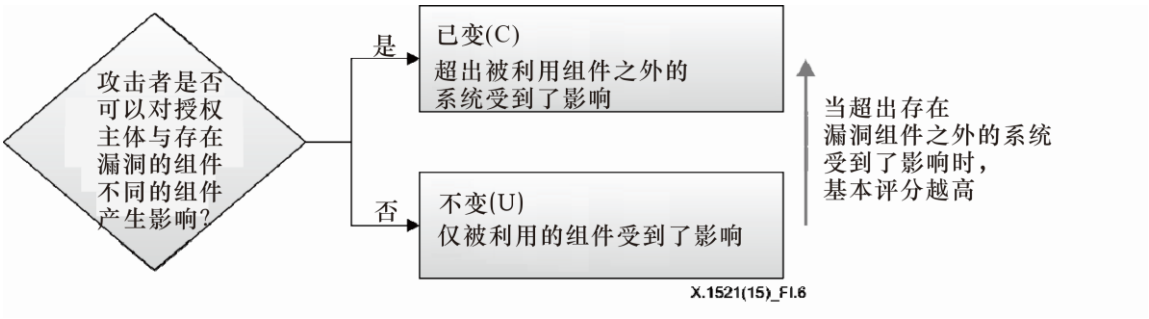
I.5.3 所需特权



I.5.4 用户交互

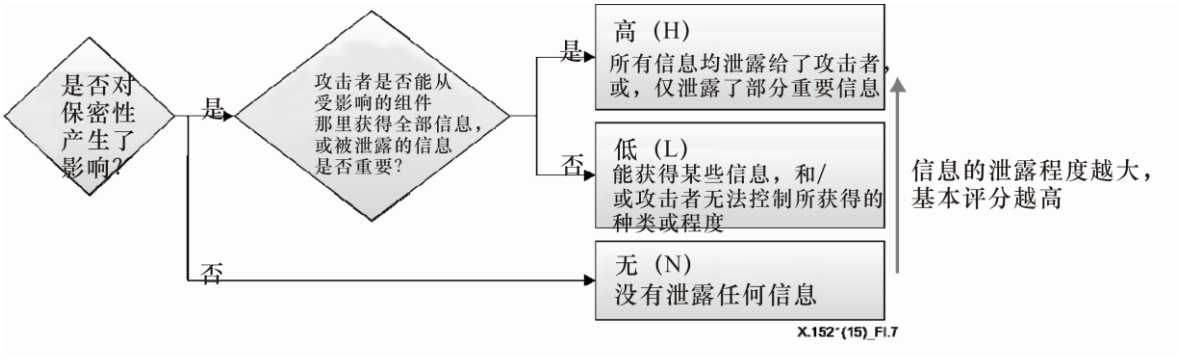


I.5.5 范围

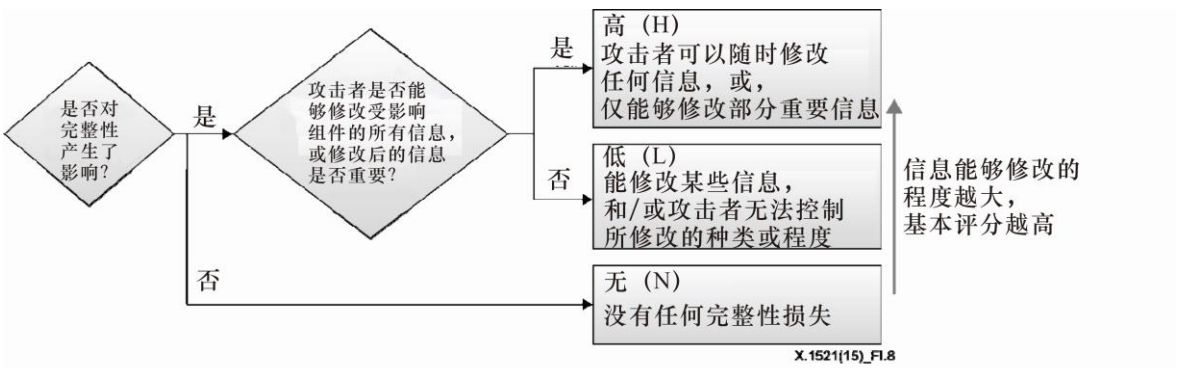


请注意，若范围没有发生变化，则保密性、完整性和可用性影响反映的是存在漏洞的组件的后果，否则反映的是遭受影响更大的组件的后果。

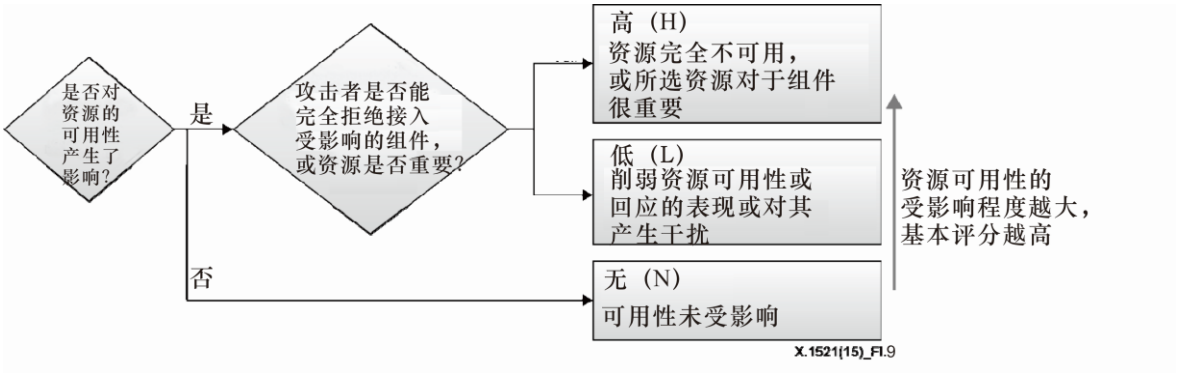
I.5.6 保密性影响



I.5.7 完整性影响



I.5.8 可用性影响


是否对资源的可用性产生了影响?
是
攻击者是否能完全拒绝接入受影响的组件，或资源是否重要?
否
高（H）
资源完全不可用，或所选资源对于组件很重要
低（L）
削弱资源可用性或回应的表现或对其产生干扰
无（N）
可用性未受影响
资源可用性的受影响程度越大，基本评分越高
X.1521(15)_FI.9

附录II

资源与链接

（本附件不是本建议书的组成部分。）

以下是更多CVSS第3.0版本文件的有用参考。

资源	位置
技术规范文件	包括度量指标描述、方程和矢量字符，请登录：http://www.first.org/cvss/specification-document
用户手册	包括有关CVSS第3.0版本的进一步讨论、评分流程图和术语表，请登录：http://www.first.org/cvss/user-guide
示例文件	包括实际的CVSS第3.0版本评分示例，请登录：https://www.first.org/cvss/examples
CVSS第3.0版本标识	低分辨率和高分辨率图片，请登录：http://www.first.org/cvss/identity
CVSS第3.0版本计算器	CVSS第3.0版本公式的参考运用，请登录：http://www.first.org/cvss/calculator/3.0
XML架构	架构定义，请登录：https://www.first.org/cvss/cvss-v3.0.xsd

参考资料

[b-ITU-T X.1500] ITU-T X.1500 建议书（2011），网络安全信息交换的概述

[b-ITU-T X.1524] ITU-T X.1524 建议书（2011），常见缺陷列表

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	环境与ICT、气候变化、电子废物、节能；线缆和外部设备的其它组件的建设、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、下一代网络、物联网和智慧城市
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2017年，日内瓦