|  |  |
| --- | --- |
| ICS  | 91.120.25 |
| CCS  | L70 |

|  |
| --- |
|  21 |

辽宁省地方标准

DB21/T XXXX—XXXX

网络安全漏洞级别判定方法

Method for Determining the Level of Network Security Vulnerability

（征求意见稿）

XXXX - XX - XX发布

XXXX - XX - XX实施

辽宁省市场监督管理局  发布

目次

[前言 II](#_Toc3150)

[1 范围 4](#_Toc1600)

[2 规范性引用文件 4](#_Toc24293)

[3 术语和定义 4](#_Toc6968)

[4 网络安全漏洞分类 4](#_Toc1646)

[4.1 概述 4](#_Toc19308)

[4.2 配置问题 4](#_Toc29443)

[4.2.1 描述 4](#_Toc14652)

[4.3 代码问题 5](#_Toc3461)

[4.3.1 描述 5](#_Toc16893)

[4.3.2 输入验证 5](#_Toc24073)

[4.3.3 数字错误 7](#_Toc13631)

[4.3.4 信息泄露 7](#_Toc26239)

[4.3.5 安全特征问题 7](#_Toc17220)

[4.3.6 竞争条件 8](#_Toc23510)

[4.3.7 资源管理错误 8](#_Toc17455)

[4.4 资料不足 8](#_Toc30948)

[4.4.1 描述 8](#_Toc17848)

[5 网络安全漏洞分级 8](#_Toc16852)

[5.1 漏洞等级-严重 9](#_Toc31588)

[5.2 漏洞等级-高危 9](#_Toc1020)

[5.3 漏洞等级-中危 9](#_Toc19855)

[5.4 漏洞等级-低危 9](#_Toc32054)

[5.5 忽略 9](#_Toc26067)

[6 网络安全漏洞判定 9](#_Toc12086)

[6.1 概述 9](#_Toc19339)

[6.2 网络安全漏洞判定指标 10](#_Toc18045)

[6.2.1 被利用性 10](#_Toc31108)

[6.2.2 影响程度 11](#_Toc31178)

[6.2.3 环境因素 12](#_Toc24087)

[6.3 网络安全漏洞判定方法 13](#_Toc11841)

[6.3.1 概述 13](#_Toc326)

[6.3.2 网络安全漏洞指标分级 13](#_Toc19870)

[6.3.3 网络安全漏洞技术分级 14](#_Toc10386)

[6.3.4 网络安全漏洞综合分级 14](#_Toc26414)

[附录A（规范性） 被利用性分级表 15](#_Toc20129)

[附录B（规范性） 影响程度分级表 17](#_Toc14695)

[附录C（规范性） 影响程度分级表 18](#_Toc13547)

[附录D（规范性） 漏洞技术分级表 19](#_Toc29005)

[附录E（规范性） 漏洞综合分级表 20](#_Toc18444)

[附录F（规范性） 漏洞分级示例 21](#_Toc5648)

1. 前言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由辽宁省工业和信息化厅提出并归口。

本文件起草单位：北方实验室（沈阳）股份有限公司、辽宁省标准化研究院。

本文件主要起草人：张健楠、李海涛、袁洪朋、刘文志、鲁宁、段晓祥、王海涛、刘兴华、李琳、张建宇、石绍群、王明俊、牛晓雷、何永建、李开、曹明、李强、张东志、邱学思、叶松、韩燕妮。

本文件发布实施后，任何单位和个人如有问题和意见建议，均可以通过来电和来函等方式进行反馈，我们将及时答复并认真处理，根据实际情况依法进行评估及复审。

归口管理部门通讯地址：辽宁省工业和信息化厅（沈阳市皇姑区北陵大街45-2号），联系电话：024-86893258。

标准起草单位通讯地址：北方实验室（沈阳）股份有限公司（沈阳市浑南新区三义街6-1号21层），联系电话：024-83785841/83785849。

网络安全漏洞级别判定方法

* 1. 范围

本文件提供了网络安全漏洞(以下简称“漏洞”)的分类、分级指标,给出了漏洞级别判定方法的建议。

本文件适用于网络产品和服务的提供者、网络运营者、漏洞收录组织、漏洞应急组织在漏洞管理、品生产、技术研发、网络运营等相关活动中进行的漏洞分类和危害等级评估等。

* 1. 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20984 信息安全技术 信息安全风险评估方法

GB/T 25069 信息安全技术 术语

GB/T 28458 信息安全技术 安全漏洞标识与描述规范

GB/T 30276 信息安全技术 信息安全漏洞管理规范

GB/T 30279 信息安全技术 网络安全漏洞分类分级指南

* 1. 术语和定义

GB/T 20984、GB/T 25069、GB/T 28458、GB/T 30276、GB/T 30279界定的以及下列术语和定义适用于本文件。

* 1. 网络安全漏洞分类
		1. 基本分类

网络安全漏洞分类是基于漏洞产生或触发的技术原因对漏洞进行划分，包括采集的公开漏洞以及收录的未公开漏洞，通用型漏洞及事件型漏洞。本次将网络安全漏洞分为26型，分别是：配置错误、代码问题、资源管理错误、数字错误、信息泄露、竞争条件、输入验证、缓冲区错误、格式化字符串、跨站脚本、路径遍历、后置链接、SQL注入、注入、代码注入、命令注入、操作系统命令注入、安全特征问题、授权问题、信任管理、加密问题、未充分验证数据可靠性、跨站请求伪造、权限许可和访问控制、访问控制错误、资料不足。

* + 1. 配置问题
			1. 描述

此类漏洞指软件配置过程中产生的漏洞。该类漏洞并非软件开发过程中造成的，不存在于软件的代码之中，是由于软件使用过程中的不合理配置造成的。

* + 1. 代码问题
			1. 描述

此类漏洞指代码开发过程中产生的漏洞，包括软件的规范说明、设计和实现。该漏洞是一个高级别漏洞，如果有足够的信息可进一步分为更低级别的漏洞。

* + - 1. 输入验证
				1. 描述

产品没有验证或者错误地验证可以影响程序的控制流或数据流的输入。如果有足够的信息，此类漏洞可进一步分为更低级别的类型。

当软件不能正确地验证输入时，攻击者能够伪造非应用程序所期望的输入。这将导致系统接收部分非正常输入，攻击者可能利用该漏洞修改控制流、控制任意资源和执行任意代码。

* + - * 1. 路径遍历

描述

为了识别位于受限的父目录下的文件或目录，软件使用外部输入来构建路径。由于软件不能正确地过滤路径中的特殊元素，能够导致访问受限目录之外的位置。

许多文件操作都发生在受限目录下。攻击者通过使用特殊元素（例如，“…”、“/”）可到达受限目录之外的位置，从而获取系统中其他位置的文件或目录。相对路径遍历是指使用最常用的特殊元素“…/”来代表当前目录的父目录。绝对路径遍历（例如"/usr/local/bin"）可用于访问非预期的文件。

* + - * 1. 后置链接

描述

软件尝试使用文件名访问文件，但该软件没有正确阻止表示非预期资源的链接或者快捷方式的文件名。

* + - * 1. 注入

描述

软件使用来自上游组件的受外部影响的输入，构造全部或部分命令、数据结构或记录，但是没有过滤或没有正确过滤掉其中的特殊元素，当发送给下游组件时，这些元素可以修改其解析或解释方式。

软件对于构成其数据和控制的内容有其特定的假设，然而，由于缺乏对用户输入的验证而导致注入问题。

命令注入

描述

软件使用来自上游组件的受外部影响的输入构造全部或部分命令，但是没有过滤或没有正确过滤掉其中的特殊元素，这些元素可以修改发送给下游组件的预期命令。

操作系统命令注入

4.3.2.4.2.2.1描述

软件使用来自上游组件的受外部影响的输入构造全部或部分操作系统命令，但是没有过滤或没有正确过滤掉其中的特殊元素，这些元素可以修改发送给下游组件的预期操作系统命令。

此类漏洞允许攻击者在操作系统上直接执行意外的危险命令。

跨站脚本

描述

在用户控制的输入放置到输出位置之前软件没有对其中止或没有正确中止，这些输出用作向其他用户提供服务的网页。

跨站脚本漏洞通常发生在：

1）不可信数据进入网络应用程序，通常通过网页请求；

2）网络应用程序动态地生成一个带有不可信数据的网页；

3）在网页生成期间，应用程序不能阻止Web浏览器可执行的内容数据，例如JavaScript，HTML标签，HTML属性、鼠标事件、Flash、ActiveX等；

4）受害者通过浏览器访问的网页包含带有不可信数据的恶意脚本；

5）由于脚本来自于通过web服务器发送的网页，因此受害者的web浏览器会在web服务器域的上下文中执行恶意脚本；

6）违反web浏览器的同源策略，同源策略是一个域中的脚本不能访问或运行其他域中的资源或代码。

SQL注入

描述

软件使用来自上游组件的受外部影响的输入构造全部或部分SQL命令，但是没有过滤或没有正确过滤掉其中的特殊元素，这些元素可以修改发送给下游组件的预期SQL命令。

如果在用户可控输入中没有充分删除或引用SQL语法，生成的SQL查询可能会导致这些输入被解释为SQL命令而不是普通用户数据。利用SQL注入可以修改查询逻辑以绕过安全检查，或者插入修改后端数据库的其他语句，如执行系统命令。

代码注入

描述

软件使用来自上游组件的受外部影响的输入构造全部或部分代码段，但是没有过滤或没有正确过滤掉其中的特殊元素，这些元素可以修改发送给下游组件的预期代码段。

当软件允许用户的输入包含代码语法时，攻击者可能会通过伪造代码修改软件的内部控制流。此类修改可能导致任意代码执行。

格式化字符串

描述

软件使用的函数接收来自外部源代码提供的格式化字符串作为函数的参数。

当攻击者能修改外部控制的格式化字符串时，这可能导致缓冲区溢出、拒绝服务攻击或者数据表示问题。

* + - * 1. 缓冲区错误

描述

软件在内存缓冲区上执行操作，但是它可以读取或写入缓冲区的预定边界以外的内存位置。

某些语言允许直接访问内存地址，但是不能自动确认这些内存地址是有效的内存缓冲区。这可能导致在与其他变量、数据结构或内部程序数据相关联的内存位置上执行读/写操作。作为结果，攻击者可能执行任意代码、修改预定的控制流、读取敏感信息或导致系统崩溃。

* + - 1. 数字错误
				1. 描述

此类漏洞与不正确的数字计算或转换有关。该类漏洞主要由数字的不正确处理造成的，如整数溢出、符号错误、被零除等。

* + - 1. 信息泄露
				1. 描述

信息泄露是指有意或无意地向没有访问该信息权限者泄露信息。此类漏洞是由于软件中的一些不正确的设置造成的信息泄漏。信息指：

1）产品自身功能的敏感信息，如私有消息；

2）或者有关产品或其环境的信息，这些信息可能在攻击中很有用，但是攻击者通常不能获取这些信息。信息泄露涉及多种不同类型的问题，并且严重程度依赖于泄露信息的类型。

* + - 1. 安全特征问题
				1. 描述

此类漏洞是指与身份验证、访问控制、机密性、密码学、权限管理等有关的漏洞，是一些与软件安全有关的漏洞。如果有足够的信息，此类漏洞可进一步分为更低级别的类型。

* + - * 1. 信任管理

描述

此类漏洞是与证书管理相关的漏洞。包含此类漏洞的组件通常存在默认密码或者硬编码密码、硬编码证书。

* + - * 1. 特权许可和访问控制

描述

此类漏洞是与许可、权限和其他用于执行访问控制的安全特征的管理有关的漏洞。

访问控制错误

描述

软件没有或者没有正确限制来自未授权角色的资源访问。

访问控制涉及若干保护机制，例如认证（提供身份证明）、授权（确保特定的角色可以访问资源）与记录（跟踪执行的活动）。

当未使用保护机制或保护机制失效时，攻击者可以通过获得权限、读取敏感信息、执行命令、规避检测等来危及软件的安全性。

* + - * 1. 授权问题

描述

程序没有进行身份验证或身份验证不足，此类漏洞是与身份验证有关的漏洞。

* + - * 1. 加密问题

描述

此类漏洞是与加密使用有关的漏洞，涉及内容加密、密码算法、弱加密（弱口令）、明文存储敏感信息等。

* + - * 1. 未充分验证数据可靠性

描述

程序没有充分验证数据的来源或真实性，导致接受无效的数据。

* + - * 1. 跨站请求伪造

描述

Web应用程序没有或不能充分验证有效的请求是否来自可信用户。

如果web服务器不能验证接收的请求是否是客户端特意提交的，则攻击者可以欺骗客户端向服务器发送非预期的请求，web服务器会将其视为真实请求。这类攻击可以通过URL、图像加载、XMLHttpRequest等实现，可能导致数据暴露或意外的代码执行。

* + - 1. 竞争条件
				1. 描述

程序中包含可以与其他代码并发运行的代码序列，且该代码序列需要临时地、互斥地访问共享资源。但是存在一个时间窗口，在这个时间窗口内另一段代码序列可以并发修改共享资源。

如果预期的同步活动位于安全关键代码，则可能带来安全隐患。安全关键代码包括记录用户是否被认证，修改重要状态信息等。竞争条件发生在并发环境中，根据上下文，代码序列可以以函数调用，少量指令，一系列程序调用等形式出现。

* + - 1. 资源管理错误
				1. 描述

此类漏洞与系统资源的管理不当有关。该类漏洞是由于软件执行过程中对系统资源（如内存、磁盘空间、文件等）的错误管理造成的。

* + 1. 资料不足
			1. 描述

根据目前信息暂时无法将该漏洞归入上述任何类型，或者没有足够充分的信息对其进行分类，漏洞细节未指明。

* 1. 网络安全漏洞分级
		1. 漏洞等级-严重

a）直接获取核心服务器权限的漏洞，包括但不限于上传Webshell、任意代码执行、远程命令执行等。

b）直接导致严重的信息泄露漏洞，包括但不限于重要数据库的SQL注入、系统权限控制不严格等导致的敏感数据泄露漏洞等。

c）直接导致严重影响的逻辑漏洞，包括但不限于核心账户体系的账密校验逻辑等。

* + 1. 漏洞等级-高危

a）重要业务敏感数据信息泄露漏洞，包括但不限于重要用户信息、订单信息、数据文件信息等。

b）重要业务的逻辑漏洞，包括但不限于权限绕过等。

c）不需交互的重点业务漏洞，包括但不限于文件遍历、任意文件包含、任意文件读取等。

d）包含重要业务敏感信息的非授权访问，包括但不仅限于绕过认证直接访问管理后台、后台弱密码、可直接获取大量内网敏感信息的SSRF等。

* + 1. 漏洞等级-中危

a）不需交互对用户产生危害的安全漏洞，包括但不限于一般页面存储型XSS等。

b）普通信息泄露漏洞，包括但不限于用户信息泄露和业务敏感信息泄露等。

c）普通的逻辑设计缺陷和流程缺陷，包括但不限于越权查看非核心系统的订单信息等。

d）其他造成中度影响的漏洞，例如：没有敏感信息的SQL注入、无回显SSRF漏洞等。

* + 1. 漏洞等级-低危

a）在特殊条件下才能获取用户信息的安全漏洞，包括但不限于反射XSS等。

b）轻微信息泄露，包括但不限于服务器物理路径、边缘系统文件、本地日志等。

c）其他造成低危害的漏洞，例如：管理后台开放、解析漏洞、存在可被暴力破解接口等。

* + 1. 忽略

a）无关安全的 bug。包括但不限于网页乱码、网页无法打开、某功能无法用。

b）无法利用的“漏洞”。包括但不限于没有实际危害的“扫描”报告、Self-XSS、无敏感信息的 JSONHijacking、无敏感操作的 CSRF、无意义的源码泄漏、内网 IP 地址/域名泄漏、401 基础认证钓鱼、程序路径信任问题、无敏感信息的信息泄漏（如无敏感信息的/metrics，/.htaccess，/DS\_store，/ swagger-ui等）。

* 1. 网络安全漏洞判定
		1. 基本分类

网络安全漏洞分级根据漏洞分级的场景不同，分为技术分级和综合分级两种分级方式，每种分级方式均包括严重、高危、中危和低危四个等级。其中，技术分级反映特定产品或系统的漏洞危害程度，用于从技术角度对漏洞危害等级进行划分，主要针对漏洞分析人员、产品开发人员等特定产品或系统漏洞的评估工作。综合分级反映在特定时期特定环境下漏洞危害程度，用于在特定场景下对漏洞危害等级进行划分，主要针对用户对产品或系统在特定网络环境中的漏洞评估工作。漏洞技术分级和综合分级均可对单漏洞进行分级，也可对多个漏洞构成的组合漏洞进行分级。

网络安全漏洞分级过程包括分级指标和分级方法两方面内容。分级指标主要阐述反映漏洞特征的属性和赋值，包括被利用性指标类、影响程度指标类和环境因案指标类等三类指标。分级方法主要阐述漏洞技术分级和综合分级的具体实现步骤和实现方法，包括漏洞指标类的分级方法、漏洞技术分级方法和漏洞综合分级方法。

* + 1. 网络安全漏洞判定指标
			1. 被利用性
				1. 访问路径

“访问路径”是指触发漏洞的路径前提，反映漏洞触发时与受影响组件最低接触程度。

访问路径的赋值包括：网络、邻接、本地和物理。通常因网络、邻接、本地和物理触发的漏洞，其被利用性程度由高到低依次降序，见表1。

表1 访问路径赋值说明

|  |  |
| --- | --- |
| 赋值 | 描述 |
| 网络 | 网络安全漏洞可以通过网络远程触发 |
| 邻接 | 网络安全漏洞需通过共享的物理网络或逻辑网络触发 |
| 本地 | 网络安全漏洞需要在本地环境中触发 |
| 物理 | 网络安全漏洞需通过物理接触/操作才能触发 |

* + - * 1. 触发要求

“触发要求”是指漏洞成功触发的要求,反映受影响组件在系统环境的版本、配置等因素影响下，成功触发漏洞的要求。

触发要求的赋值包括:低、高。通常触发要求低的漏洞危害程度高,见表2。

表2 触发要求赋值说明

|  |  |
| --- | --- |
| 赋值 | 描述 |
| 低 | 漏洞触发对受影响组件的配置参数、运行环境、版本等无特别要求，包括：默认的配置参数、普遍的运行环境 |
| 高 | 漏洞触发对受影响组件的配置参数、运行环境、版本等有特别要求，包括：不常用的配置参数，特殊的运行环境条件 |

* + - * 1. 权限需求

“权限需求”是指触发漏洞所需的权限,反映漏洞成功触发需要的最低的权限，权限需求的赋值包括:无、低和高。通常所需要的权限越少漏洞危害程度越高,见表 3。

表3 权限需求赋值说明

|  |  |
| --- | --- |
| 赋值 | 描述 |
| 无 | 网络安全漏洞触发无需特殊的权限，只需要公开权限和匿名访问权限 |
| 低 | 网络安全漏洞触发需要较低的权限，需要普通用户权限 |
| 高 | 网络安全漏洞触发需要较高的权限，需要管理员权限 |

* + - * 1. 交互条件

“交互条件”是指漏洞触发是否需要其他主体(如:系统用户、外部用户、其他系统等)的参与、配合，反映漏洞触发时，是否需要除触发漏洞的主体之外的其他主体参与。

交写条件的赋值包括,不需要、需要。通常不需交互条件即能触发的漏洞，其危害程度较高，见表4。

表4 交互条件赋值说明

|  |  |
| --- | --- |
| 赋值 | 描述 |
| 不需要 | 网络安全漏洞无需用户或系统的参与或配合 |
| 需要 | 网络安全漏洞触发需要较低的权限，需要普通用户权限 |

* + - 1. 影响程度

“影响程度”指触发漏洞对受影响组件造成的损害程度。影响程度根据受漏洞影响的各个对象所承载信息的保密性、完整性、可用性等三个指标决定,每个指标的影响赋值为:严重、一般和无，见表5、表6、表7。

“保密性影响”指标反映漏洞对受影响实体(如:系统、模块、软硬件等)承载(如:处理、存储、传输等)信息的保密性的影响程度。

“完整性影响”指标反映漏洞对受影响实体(如;系统、模块、软硬件等)承载(如:处理、存储、传输等)信息的完整性的影响程度。

“可用性影响”指标反映漏洞对受影响实体(如:系统、模块、软硬件等)承载(如:处理、存储、传输等)信息的可用性的影响程度。

表5 保密性影响赋值说明

|  |  |
| --- | --- |
| 赋值 | 描述 |
| 严重 | 信息保密性影响严重，例如:保密性完全丢失，导致受影响组件的所有信息资源暴露给攻击者；或者攻击者只能得到一些受限信息，但被暴露的信息可以直接导致严重的信息丢失 |
| 一般 | 信息保密性影响一般，例如:保密性部分丢失,攻击者可以获取一些受限信息，但是攻击者不能控制获得信息的数量和种类。被暴露的信息不会引起受影响组件直接的、严重的信息丢失 |
| 无 | 信息保密性无影响，漏洞对保密性不产生影响 |

表6 完整性影响赋值说明

|  |  |
| --- | --- |
| 赋值 | 描述 |
| 严重 | 信息完整性破坏严重，例如：完整性完全丢失，攻击者能够修改受影响组件中的任何信息：或者，攻击者只能修改一些信息，但是，能够对受影响组件带来严重的后果 |
| 一般 | 信息完整性破坏程度一般，例如：完整性部分天失，攻击者可以修改信息，信息修改不会给受影响组件带来严重的影响 |
| 无 | 信息完整性无影响，漏洞对完整性不产生影响 |

表7 可用性影响赋值说明

|  |  |
| --- | --- |
| 赋值 | 描述 |
| 严重 | 信息可用性破坏严重。可用性完全丧失，攻击者能够完全破坏对受影响组件中信息资源的使用访问；或者，攻击者可破坏部分信息的可用性，但是能够给受影响组件带来直接严重的后果 |
| 一般 | 信息可用性破坏程度一般。可用性部分丧失，攻击者能够降低信息资源的性能或者导致其可用性降低。受影响组件的资源是部分可用的，或在某些情况是完企可用的，但总体上不会给受影响组件带来直接严重的后果 |
| 无 | 信息可用性无影响，漏洞对可用性不产生影响 |

* + - 1. 环境因素
				1. 被利用成本

被利用成本包括：低、中、高。通常成本越低，漏洞的危害越严重，如表8所示。

“被利用成本”指标反映，在参考环境下（例如：当前全球互联网环境，或者某企业内网环境等）,漏洞触发所需的成本，例如：是否有公开的漏洞触发工具、漏洞触发需要的设备是否容易获取等。

表8 被利用成本赋值说明

|  |  |
| --- | --- |
| 赋值 | 描述 |
| 低 | 漏洞触发所需资源很容易获取，成本低，通常付出很少的成本即可成功触发漏洞，例如：漏洞触发工具已被公开下载、漏洞脆弱性组件暴露在公开网络环境下等 |
| 中 | 漏洞触发所需的部分资源比较容易获取，成本不高，在现有条件基础上通过一定的技术、资源投入可以触发漏洞，例如：漏洞触发原理已公开但是无相应工具、漏洞触发需要某种硬件设备、漏洞触发需要一定的网络资源等 |
| 高 | 漏洞触发需要的资源多，成本高，难于获取，例如：漏洞脆弱性组件未暴露在公开网络、漏洞触发工具难以获取等 |

* + - * 1. 修复难度

修复难度包括：高、中、低。通常漏洞修复的难度越高，危害越严重，如表9所示。

“修复难度”指标反映，在参考环境下(例如：当前全球互联网环境，或者某企业内网环境等)，修复漏洞所需的成本。

表9 修复难度赋值说明

|  |  |
| --- | --- |
| 赋值 | 描述 |
| 高 | 缺少有效、可行的修复方案，或者修复方案难以执行，例如：无法获取相应的漏洞补丁、由于某种原因无法安装补丁等 |
| 中 | 虽然有修复方案，但是需要付出一定的成本，或者修复方案可能影响系统的使用，或者修复方案非常复杂，适用性差，例如：虽然有临时漏洞修复措施，但是需要关闭某些网络服务等 |
| 低 | 已有完善的修复方案，例如：已有相应漏洞的补丁等 |

* + - * 1. 影响范围

影响范围包括：高、中、低、无。通常漏洞对环境的影响越高，危害越严重，如表10所示。

影响范围指标描述反映漏洞触发对环境的影响，漏洞受影响组件在环境中的重要性。

表10 影响范围赋值说明

|  |  |
| --- | --- |
| 赋值 | 描述 |
| 高 | 触发漏洞会对系统、资产等造成严重影响，例如：对环境中大部分资产造成影响，通常高于50%；或者受影响实体处于参考环境的重要位置，或者其有重要作用 |
| 中 | 漏洞触发会对系统、资产等造成中等程度的影响，例如：对环境中相当部分资产造成影响，通常介于10%-50%；或者受影响实体处于参考环境的比较重要位置，或者具有比较重要的作用 |
| 低 | 触发漏洞只会对系统、资产等造成轻微的影响，例如：只对环境中小部分资产造成影响，通常低于10%：或者受影响实体处于参考环境的不重要位置，或者具有不重要作用 |
| 无 | 触发漏洞不会对系统、资产等造成任何资产损失 |

* + 1. 网络安全漏洞判定方法
			1. 概述

网络安全漏洞分级是指采用分级的方式对网络安全漏洞潜在危害的程度进行描述，包括技术分级和综合分级两种分级方式，每种方式均分为严重、高危、中危和低危四个等级,其体内容如下：

——严重：漏洞可以非常容易地对目标对象造成特别严重后果；

——高危：漏洞可以容易地对目标对象造成严重后果；

——中危：漏洞可以对目标对象造成一般后果，或者比较困难地对目标造成严重后果；

——低危：漏洞可以对目标对象造成轻微后果，或者比较困难地对目标对象造成一般严重后果，或者非常困难地对目标对象造成严重后果。

漏洞分级过程主要包括最初的指标赋值、中间的指标分级和最后的分级计算三个步骤，其中，指标赋值是对根据具体漏洞对每个漏洞分级指标进行人工赋值：指标分级是根据指标赋值结果分别对被利用性、影响程度和环境因案等三个指标类进行分级；分级计算是根据指标分级计算产生技术分级或综合分级的结果，技术分级结果由被利用性和影响程度两个指标类计算产生，综合分级由被利用性、影响程度和环境因素三个指标类计算产生。

* + - 1. 网络安全漏洞指标分级
				1. 被利用性分级

被利用性分级反映网络安全漏洞触发的技术可能性。被利用性指标组中各指标的不同取值的组合对应不同的被利用性级别。被利用性级别分为9级，用1-9的数字表示，数值越大被利用的可能性越高，见附录A。

* + - * 1. 影响程度分级

影响程度分级反映网络安全漏洞触发造成的危害程度。影响程度指标组中各指标的不同取值的组合对应不同的影响程度级别。不同的影响程度级分为9级，用1-9的数字表示，数值越大导致的危害程度越高，见附录B。

* + - * 1. 环境因素分级

环境因素是对漏洞进行分级是需要考虑的漏洞所处的网络环境、当前漏洞被利用的技术程度等外部环境。环境因素分级反映在参考环境下，漏洞的危害程度。环境因素指标组中各指标的不同取值的组合对应不同的环境因素级别。不同的环境因素级别分为9级，用1-9的数字表示，数值越大环境因素导致的漏洞危害程度越高，见附录C。

* + - 1. 网络安全漏洞技术分级

网络安全漏洞技术分级分为：严重、高危、中危、低危四个级别。网络安全漏洞技术分级由被利用性和影响程度两个指标类决定，漏洞被利用可能性越高（被利用性分级越高）、影响程度越严重（影响程度分级越高），漏洞技术分级的级别越高（漏洞危害程度越大）。漏洞技术分级方法如下：

——首先，对被利用性指标进行赋值，根据赋值结果，按照附录A计算得到漏洞被利用性分级；

——然后，对影响程度指标进行赋值，根据赋值结果，按照附录B计算得到影响程度分级；

——最后，根据被利用性和影响程度分级的结果，按照附录D，计算得到网络安全漏洞技术分级。

* + - 1. 网络安全漏洞综合分级

网络安全漏洞综合分级分为：严重、高危、中危、低危四个级别。网络安全漏洞综合分级由被利用性、影响程度和环境因素三个指标类决定，漏洞被利用可能性越高（被利用性分级越高）、影响程度越严重（影响程度分级越高），环境对漏洞影响越敏感（环境因素分级越高），漏洞综合分级的级别越高（漏洞危害程度越大）。漏洞综合分级方法如下：

——首先，对漏洞进行技术分级，根据前述漏洞技术分级步骤，对被利用性指标进行赋值，根据赋值结果，按照附录A计算得到漏洞被利用性分级；对影响程度指标进行赋值，根据赋值结果，按照附录B计算得到影响程度分级；根据被利用性和影响程度分级的结果，按照附录，计算得到网络安全漏洞技术分级。

——然后，对环境因素指标进行赋值，根据赋值结果，按照附录C计算得到漏洞环境因素分级；

——最后，根据技术分级和环境因素分级的结果，按照附录E，计算得到网络安全漏洞综合分级，漏洞分级示例参见附录F。

1. （规范性）
被利用性分级表

被利用性分级见表A.1。

表A.1 被利用性分级

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 访问路径 | 触发要求 | 权限需求 | 交互条件 | 被利用性分级 |
| 1 | 网络 | 低 | 无 | 不需要 | 9 |
| 2 | 网络 | 低 | 低 | 不需要 | 8 |
| 3 | 网络 | 低 | 无 | 需要 |
| 4 | 邻接 | 低 | 无 | 不需要 |
| 5 | 本地 | 低 | 无 | 不需要 |
| 6 | 网络 | 高 | 无 | 不需要 |
| 7 | 网络 | 低 | 低 | 需要 | 7 |
| 8 | 邻接 | 低 | 高 | 不需要 |
| 9 | 网络 | 低 | 高 | 不需要 |
| 10 | 邻接 | 低 | 无 | 需要 | 6 |
| 11 | 本地 | 低 | 无 | 需要 |
| 12 | 本地 | 低 | 低 | 不需要 |
| 13 | 网络 | 高 | 低 | 不需要 | 5 |
| 14 | 网络 | 高 | 无 | 需要 |
| 15 | 邻接 | 高 | 无 | 不需要 |
| 16 | 邻接 | 低 | 低 | 需要 |
| 17 | 邻接 | 高 | 无 | 需要 | 4 |
| 18 | 邻接 | 高 | 低 | 不需要 |
| 19 | 本地 | 高 | 无 | 不需要 |
| 20 | 本地 | 低 | 低 | 需要 |
| 21 | 网络 | 高 | 低 | 需要 |

表A.1（续）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 访问路径 | 触发要求 | 权限需求 | 交互条件 | 被利用性分级 |
| 22 | 本地 | 高 | 低 | 不需要 | 3 |
| 23 | 网络 | 高 | 高 | 不需要 |
| 24 | 网络 | 低 | 高 | 需要 |
| 25 | 邻接 | 低 | 高 | 需要 |
| 26 | 邻接 | 低 | 高 | 不需要 |
| 27 | 本地 | 低 | 高 | 不需要 | 2 |
| 28 | 本地 | 高 | 无 | 需要 |
| 29 | 物理 | 低 | 无 | 不需要 |
| 30 | 网络 | 高 | 高 | 需要 |
| 31 | 邻接 | 高 | 高 | 不需要 |
| 32 | 邻接 | 高 | 低 | 需要 |
| 33 | 本地 | 低 | 高 | 需要 |
| 34 | 物理 | 低 | 无 | 需要 |
| 35 | 物理 | 低 | 低 | 不需要 |
| 36 | 本地 | 高 | 高 | 不需要 |
| 37 | 本地 | 高 | 低 | 需要 | 1 |
| 38 | 邻接 | 高 | 高 | 需要 |
| 39 | 物理 | 高 | 无 | 不需要 |
| 40 | 物理 | 低 | 高 | 不需要 |
| 41 | 物理 | 低 | 低 | 需要 |
| 42 | 物理 | 高 | 低 | 不需要 |
| 43 | 本地 | 高 | 高 | 需要 |
| 44 | 物理 | 高 | 无 | 需要 |
| 45 | 物理 | 高 | 高 | 需要 |
| 46 | 物理 | 高 | 高 | 不需要 |
| 47 | 物理 | 高 | 低 | 需要 |
| 48 | 物理 | 低 | 高 | 需要 |
| 注：按照“访向路径”“触发要求”“权限需求”“交互程度”的不同，可分为48种组合情况，按照每种组合的被利用程度的差异，从高到低可分为9个级别。 |

1. （规范性）
影响程度分级表

影响程度分级见表B.1

表B.1影响程度分级

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 严重（次数） | 一般（次数） | 无（次数） | 影响程度分级 |
| 1 | 3 | 0 | 0 | 9 |
| 2 | 2 | 1 | 0 | 8 |
| 3 | 2 | 0 | 1 | 7 |
| 4 | 1 | 2 | 0 | 6 |
| 5 | 1 | 1 | 1 | 5 |
| 6 | 1 | 0 | 2 | 4 |
| 7 | 0 | 3 | 0 | 3 |
| 8 | 0 | 2 | 1 | 2 |
| 9 | 0 | 1 | 2 | 1 |
| 注：按照保密性、完整性、可用性权重相同，按照影响程度指标“严示”“一般”“无”的数量进行影响程度的分级，如：严重出现2次，一般出现1次，无出现0次，则响程度的组合可能性包括：保密性（严重）、完整性（严重）、可用性(一般)，保密性(严重)、完整性(一般)、可用性(严重)，保密性(一般)、完整性(严重)、可用性(严重)三种情况。同时，这三种情况的影响程度分级均为8级。 |

1. （规范性）
环境因素分级表

环境因素分级见表C.1

表C.1环境因素分级

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 影响范围 | 被利用成本 | 修复难度 | 环境因素分级 |
| 1 | 高 | 低 | 高 | 9 |
| 2 | 高 | 低 | 中 | 8 |
| 3 | 高 | 中 | 高 |
| 4 | 中 | 低 | 高 |
| 5 | 高 | 低 | 低 | 7 |
| 6 | 高 | 中 | 中 |
| 7 | 高 | 高 | 高 |
| 8 | 中 | 低 | 中 |
| 9 | 中 | 中 | 高 |
| 10 | 高 | 中 | 低 | 6 |
| 11 | 高 | 高 | 中 |
| 12 | 中 | 低 | 低 |
| 13 | 中 | 中 | 中 |
| 14 | 中 | 高 | 高 |
| 15 | 高 | 高 | 低 | 5 |
| 16 | 中 | 中 | 低 |
| 17 | 中 | 高 | 中 |
| 18 | 低 | 低 | 高 |
| 19 | 中 | 高 | 低 | 4 |
| 20 | 低 | 低 | 中 |
| 21 | 低 | 中 | 高 |
| 22 | 低 | 低 | 低 | 3 |
| 23 | 低 | 中 | 中 |
| 24 | 低 | 高 | 高 |
| 25 | 低 | 中 | 低 | 2 |
| 26 | 低 | 高 | 中 |
| 27 | 低 | 高 | 低 | 1 |
| 注：按照“影响范围”“被利用成本”“修复难度”的不同，可分为27种组合情况，按照每种组合环境因素分级的差异，从高到低可分为9个级别。 |

1. （规范性）
漏洞技术分级表

漏洞技术分级见表D.1

表D.1漏洞技术分级

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 被利用性分级 | 影响程度分级 | 安全漏洞技术分级 |
| 1 | 9 | 7-9 | 严重 |
| 2 | 2-8 | 9 | 高危 |
| 3 | 5-8 | 8 | 高危 |
| 4 | 6-8 | 7 | 高危 |
| 5 | 8-9 | 6 | 高危 |
| 6 | 8-9 | 5 | 高危 |
| 7 | 9 | 4 | 高危 |
| 8 | 9 | 3 | 高危 |
| 9 | 1 | 9 | 中危 |
| 10 | 1-4 | 8 | 中危 |
| 11 | 1-5 | 7 | 中危 |
| 12 | 1-7 | 6 | 中危 |
| 13 | 1-7 | 5 | 中危 |
| 14 | 2-8 | 4 | 中危 |
| 15 | 3-8 | 3 | 中危 |
| 16 | 3-9 | 2 | 中危 |
| 17 | 9 | 1 | 中危 |
| 18 | 1 | 4 | 低危 |
| 19 | 1-2 | 3 | 低危 |
| 20 | 1-2 | 2 | 低危 |
| 21 | 1-8 | 1 | 低危 |

1. （规范性）
漏洞综合分级表

漏洞综合分级见表E.1

表E.1漏洞技术分级

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 技术分级 | 环境因素分级 | 网络安全漏洞综合分级 |
| 1 | 严重 | 7-9 | 严重 |
| 2 | 严重 | 4-6 | 高危 |
| 3 | 严重 | 1-3 | 中危 |
| 4 | 高危 | 8-9 | 严重 |
| 5 | 高危 | 7 | 高危 |
| 6 | 高危 | 5-6 | 中危 |
| 7 | 高危 | 1-4 | 低危 |
| 8 | 中危 | 9 | 严重 |
| 9 | 中危 | 8 | 高危 |
| 10 | 中危 | 6-7 | 中危 |
| 11 | 中危 | 1-5 | 低危 |
| 12 | 低危 | 9 | 高危 |
| 13 | 低危 | 7-8 | 中危 |
| 14 | 低危 | 1-6 | 低危 |

1. （规范性）
漏洞分级示例
	1. 示例一 OpenSSL 缓冲区溢出(CVE-2014-0160)漏洞分级示例
		1. 漏洞名称

OpenSSL 缓冲区溢出(CVE-2014-0160)

* + 1. 漏洞简介

OpenSSL的TLS和DTLS实现过程中的d1\_both.c 和tl\_lib.c文件中存在安全漏洞，该漏洞源于处理Heartbeat Extension数据包时，缺少边界检查。远程攻击者可借助特制的数据包利用该漏洞读取服务器内存中的敏感信息（如用户名、密码、Cookie、私销等）。

* + 1. 漏洞分级示例

见表F.1

表F.1 CVE-2014-0160漏洞分级

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 指标类 | 指标子类 | 描述 | 赋值说明 | 分级说明 |
| 被利用性 | 访问路径 | 通过网络远程访问 | 网络 | 9 |
| 触发要求 | 无需特定环境，普通环境即可触发 | 低 |
| 权限需求 | 无需任何特权信息或身份验证 | 无 |
| 交互条件 | 漏洞触发无需用户或系统的参与或配合 | 不需要 |
| 影响程度 | 保密性 | 攻击者从内存中可读取多达64KB的数据，通过该漏洞读取每次攻击泄露出来的信息，可轻松获取到服务器的私钥、用户cookic和密码等 | 严重 | 4 |
| 完整性 | 漏洞对完整性不产生影响 | 无 |
| 可用性 | 漏洞对可用性不产生影响 | 无 |
| 环境因素 | 被利用成本 | 协议本身漏洞，直接暴露于公网之下，容易被利用 | 低 | 7 |
| 修复难度 | 已有较为完善的修复方案，修复难度不大 | 低 |
| 影响范围 | 影响范围广泛 | 高 |

* + 1. 漏洞分级

通过表F.1，CVE-2014-0160漏洞的被利用性为9级、影响程度为4级，因此技术分级为高危；同时该漏洞的环境因素为7级，结合技术分级为高危，可知该漏洞的综合分级为高危

* 1. 示例二 开源软件Plait plaiter 文件覆盖（CVE-2008-4085）漏洞分级示例
		1. 漏洞名称

开源软件Plait plaiter 文件覆盖（CVE-2008-4085）

* + 1. 漏洞介绍

Plait是一款命令行方式的音乐播放软件。

Plait 1.6之前版本的 plaiter 存在文件覆盖漏洞。本地用户可通过在 cut，$ $，head.$ $,awk.$ $，Ps.$ $的临时文件中使用symlink，覆盖任意文件。

* + 1. 漏洞分级示例

见表F.2

表F.2 CVE-2008-4085漏洞分级

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 指标类 | 指标子类 | 描述 | 赋值说明 | 分级说明 |
| 被利用性 | 访问路径 | 需要在本地环境中触发 | 本地 | 6 |
| 触发要求 | 无需特定环境，普通环境即可触发 | 低 |
| 权限需求 | 无需特殊的权限，普通用户即可 | 低 |
| 交互条件 | 无需用户或系统的参与或配合 | 不需要 |
| 影响程度 | 保密性 | 保密性部分天失，攻击者可以获取一些受限信息 | 一般 | 3 |
| 完整性 | 完整性部分丢失，攻击者可以修改信息 | 一般 |
| 可用性 | 信息可用性破坏程度一般 | 一般 |
| 环境因素 | 被利用成本 | 编辑使用symlink即可覆盖任意文件，所付出成本较低 | 低 | 3 |
| 修复难度 | 目前厂商已经发布了升级补丁以修复这个安全问题 | 低 |
| 影响范围 | 该漏洞为一款开源音乐播放软件，只对环境中小部分资产造成影响，影响范围不大 | 高 |

* + 1. 漏洞分级

通过表F.2，CVE-2008-4085 漏洞的被利用性为6级、响程度为3级，因此技术分级为中危；同时，该漏洞的环境因素为3级，结合技术分级为中危，可知该漏洞的综合分级为低危。