ICS 91.120.25
CCS L 70

DB21

辽 宁 省 地 方 标 准

DB21/T 4170—2025

网络安全漏洞风险级别评估指南

Guidelines for cybersecurity vulnerability risk classified assessment

2025－08－30 发布　　2025－09－30 实施

辽宁省市场监督管理局　　发 布

目　　次

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、辽宁鲲鹏生态创新中心有限公司、辽宁省通信管理局、辽宁省福利彩票中心、东北大学。

本文件主要起草人：张健楠、袁洪朋、张建宇、刘文志、韩晓娜、隋大智、王海涛、段晓祥、李琳、王继宏、王明俊、石绍群、刘兴华、马超、牛晓雷、何永建、闫丽杰、孙辉航、蒋绪军、任铭、李成、姚羽。

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（辽宁省沈阳市浑南区智慧三街199号），联系电话：400-664-5588。

网络安全漏洞风险级别评估指南

1 范围

本文件提供了网络安全漏洞风险级别评估指南的术语和定义、网络安全漏洞分类、网络安全资产分类、网络安全漏洞风险定义和网络安全漏洞风险级别评估的建议。

本文件适用于网络产品和服务的提供者、网络运营者、网络安全评估机构在产品生产、技术研发、网络运营、检测评估、漏洞管理等相关活动中进行的漏洞风险级别评估。

2 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指南必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本指南；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本指南。

GB/T 20984—2022 信息安全技术 信息安全风险评估方法

GB/T 25069—2022 信息安全技术 术语

GB/T 28458—2020 信息安全技术 安全漏洞标识与描述规范

GB/T 30276—2020 信息安全技术 信息安全漏洞管理规范

GB/T 30279—2020 信息安全技术 网络安全漏洞分类分级指南

3 术语和定义

GB/T 25069—2022、GB/T 20984—2022、GB/T 28458—2020、GB/T 30276—2020、GB/T 30279—2020界定的术语和定义适用于本文件。

4 风险级别评估框架及流程

网络安全漏洞风险级别评估基本要素包括漏洞严重程度和资产重要性等级两方面，基于这两方面要素开展漏洞风险级别评估，基本要素的关系见图1。

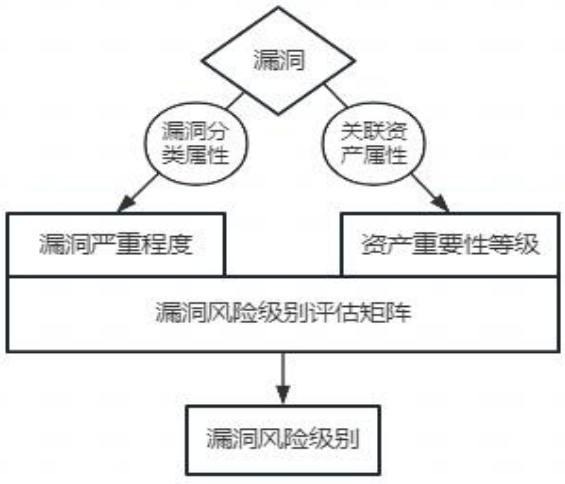

图1 漏洞风险级别评估要素及其关系

开展网络安全漏洞风险级别评估时，要素之间的关系和评估流程如下：

a) 网络安全的核心是资产，资产存在漏洞。漏洞包括漏洞风险类别和关联资产两个属性；
b) 确认漏洞对应的漏洞风险分类及关联资产分类；
c) 根据上述两个分类属性确认结果，建立漏洞风险分类与漏洞严重程度关系表、网络安全资产分类与资产重要性等级关系表；
d) 根据漏洞严重程度和关联资产重要性等级的结果，通过漏洞风险级别评估矩阵计算出漏洞风险分值；
e) 根据漏洞风险分值结果判定漏洞最终风险。

5 漏洞分类

本指南引用 GB/T 30279—2020 中 5.1 漏洞分类，通过技术特征提取、影响范围关联、结构化命名，进一步细化扩展第三级网络安全漏洞子类。

技术特征提取、影响范围关联、结构化命名三者联动形成“技术路径清晰、危害可评估、命名标准化”的网络安全漏洞三级分类方法，具体步骤如下：

a) 枚举技术特征列表：针对每个二级分类，梳理其涉及的具体技术缺陷或攻击手法（如“输入验证错误”下的“缓冲区溢出”“正则表达式注入”等）；
b) 匹配影响范围：为每个技术特征明确对应的直接安全影响（基于保密性、完整性、可用性维度），如“目录遍历”对应“敏感文件读取（保密性）”“恶意文件上传（完整性）”，同一技术特征可能涉及多个影响需全部标注；
c) 命名三级子类：采用“技术特征+影响结果/场景限定”模式命名，包括单一影响型（如“缓冲区溢出漏洞”）、多影响型（如“路径遍历-任意文件下载”）、场景限定型（如“API接口-未授权访问”），确保名称唯一且标准化。

依据网络安全漏洞三级分类方法，具体细化扩展出的网络安全漏洞风险三级分类示例见附录 A.1。

6 资产分类

本指南引用 GB/T 20984—2022 中 5.2.1.4 资产分类，通过功能维度解析、形式特征提取、组件结构划分，进一步细化扩展第三级网络安全资产子类。

功能维度解析、形式特征提取、组件结构划分三者联动形成“业务定位清晰、形态特征明确、架构层级标准化”的网络安全资产三级分类方法，具体步骤如下：

a) 功能维度解析：针对每个二级资产分类，分析其承载的业务用途或技术功能，梳理出具体功能属性（如“数据存储”“网络通信”“业务支撑”），并映射到具体资产类型。例如，在“存储设备”中，按功能维度可区分“主磁盘阵列”（生产环境数据存储）与“备份磁盘阵列”（数据备份专用）；
b) 形式特征提取：从资产的物理形态、技术架构或终端类型等形式维度，提取差异化特征（如“便携性”“传输介质”“架构分层”）。例如，“便携计算机”基于物理形态的便携性归类，“Web前端应用”基于技术架构的分层特性归类；
c) 组件结构划分：根据资产在系统架构中的角色或组成部分（如“核心层组件”“边界防护组件”“基础设施组件”）进行层级划分。例如，“核心路由器”属于网络架构核心层组件，“入侵防御系统”属于安全防护边界组件，“云计算平台”属于基础设施支撑组件。

依据网络安全资产三级分类方法，具体细化扩展出的网络安全资产三级分类示例见附录 A.2。

7 风险级别评估

7.1 漏洞风险严重程度识别

定义网络安全漏洞风险严重程度，将细化扩展出的网络安全漏洞与漏洞风险严重程度建立对应关系。

a) 参考GB/T 20984—2022，依据漏洞风险对业务信息和系统服务所造成的侵害程度，分5个级别对漏洞风险严重程度进行定义，见表1；

表 1 漏洞风险严重程度定义表

等级	标识	定义
1	很低	无法利用但影响使用的安全方面缺陷，对业务信息和系统服务基本不造成侵害
2	低	轻微信息泄露漏洞、配置错误和解析漏洞、资源管理错误，对业务信息和系统服务造成一般侵害
3	中等	一般数据泄露漏洞、逻辑设计缺陷或安全功能缺陷、完整性破坏或调试信息泄露漏洞，对业务信息和系统服务造成侵害
4	高	重要业务敏感数据泄露漏洞、重要业务逻辑漏洞、重要业务功能未授权漏洞，对业务信息和系统服务造成严重侵害
5	很高	直接获取权限的漏洞、直接导致严重的信息泄露漏洞、直接导致严重影响的逻辑漏洞，对业务信息和系统服务造成特别严重侵害

b) 对细化扩展出的网络安全漏洞风险，基于漏洞利用的难易程度、漏洞对数据及系统造成的影响等因素，通过维度等级划分、关联矩阵构建、判定规则定义、数据验证校准四个环节，形成漏洞风险与严重程度的系统化映射体系，建立网络安全漏洞风险与严重程度的对应关系表，具体步骤如下：

1) 划分维度等级：将“利用难易程度”划分为很低、低、中等、高、很高五级（如“很低”表示无需特殊条件即可利用，“很高”表示需复杂攻击链或特殊权限）；将“影响程度”划分为轻微、一般、中等、严重、很高五级（如“轻微”对应非敏感数据泄露，“很高”对应核心业务系统瘫痪或大规模敏感数据泄露），形成标准化五级评估体系；

2) 构建关联矩阵：以“利用难易程度”为横轴（5 级）、“影响程度”为纵轴（5 级），建立二维矩阵，通过交叉组合形成 25 个评估单元，每个单元对应唯一的风险等级（如“利用难度低+影响程度一般”对应“低风险”，“利用难度很高+影响程度很高”对应“很高风险”）；

3) 定义判定规则：参照表 1 漏洞风险严重程度定义表，为每个风险等级（1-5 级）制定具体映射规则。

依据漏洞风险严重程度识别方法，参照网络安全漏洞风险三级分类示例，形成网络安全漏洞风险所对应的严重程度关系示例表见附录 B.1。

7.2 资产重要性等级识别

定义网络安全资产重要性等级，将细化扩展出的网络安全资产与重要性等级建立对应关系。

a) 参考GB/T 20984—2022，分5个级别对资产重要性等级进行定义，见表2；

表 2 资产重要性等级定义表

等级	标识	定义
1	很低	资产遭到破坏后，对被测组织的业务对象造成很小的影响，甚至忽略不计
2	低	资产遭到破坏后，对被测组织的业务对象造成较低的影响

表 2 资产重要性等级定义表（续）

等级	标识	定义
3	中等	资产遭到破坏后，对被测组织的业务对象造成中等程度的影响
4	高	资产遭到破坏后，对被测组织的业务对象造成比较严重的影响
5	很高	资产遭到破坏后，对被测组织的业务对象造成非常严重的影响

b) 从资产保密性、完整性、可用性三方面，通过要素赋值与加权计算，对网络安全资产重要性等级进行识别和赋值。

依据资产重要性等级定义表，结合加权计算结果，形成网络安全资产重要性等级识别示例见表 B.2。

7.3 漏洞风险级别评估

7.3.1 漏洞风险级别评估矩阵

基于漏洞严重程度和资产重要性等级，建立漏洞风险级别评估矩阵，见表 3。

表 3 漏洞风险级别评估矩阵表

资产重要性等级		漏洞严重程度				
		很低（1）	低（2）	中等（3）	高（4）	很高（5）
很低	1	1	1.5	2	2.5	3
低	2	1.5	2	2.5	3	3.5
中等	3	2	2.5	3	3.5	4
高	4	2.5	3	3.5	4	4.5
很高	5	3	3.5	4	4.5	5

7.3.2 漏洞风险级别评估准则

依据漏洞风险级别评估矩阵所定义的风险值，制定如下漏洞风险级别评估准则，见表 4。

表 4 漏洞风险级别评估准则

风险等级	判定准则
超危	经漏洞严重程度和资产重要性等级两项综合评估，矩阵判定结果为 4.5 分及以上的漏洞风险
高危	经漏洞严重程度和资产重要性等级两项综合评估，矩阵判定结果为 3.5 或 4 分的漏洞风险
中危	经漏洞严重程度和资产重要性等级两项综合评估，矩阵判定结果为 2.5 或 3 分的漏洞风险
低危	经漏洞严重程度和资产重要性等级两项综合评估，矩阵判定结果为 1、1.5 或 2 分的漏洞风险

附 录 A
（资料性）
网络安全漏洞风险及网络安全资产三级分类示例表

A.1 网络安全漏洞风险三级分类示例表

网络安全漏洞风险三级分类示例表见表 A.1。

表 A.1 网络安全漏洞风险分类示例表

序号	漏洞大类	漏洞小类		漏洞子类
1	代码问题	资源管理错误	资源管理问题	不可控的内存分配
2				内存泄露
3				敏感信息存储于上锁不正确的内存空间
4				关键资源路径错误
5		输入验证错误	缓冲区错误	栈缓冲区溢出漏洞
6				堆缓冲区溢出漏洞
7				缓冲区越界读
8			注入	格式化字符串错误	使用外部控制的格式化字符串
9					FastJson 反序列化漏洞
10				跨站脚本	存储 xss 漏洞
11					反射 xss 漏洞
12					Dom 型 xss 漏洞
13				命令注入	shell 命令注入
14					远程命令执行漏洞
15					本地命令执行漏洞
16				代码注入	模板注入
17					木马文件上传
18					YAML 远程代码注入
19					LDAP 注入
20					表达式注入
21					XML 外部实体注入
22					Java 反序列化漏洞
23					XPath 注入
24					NoSQL 注入
25				SQL 注入	报错注入
26					联合查询 sql 注入
27					盲注
28					二次 SQL 注入
29					堆叠注入
30					排序注入
31			路径遍历		不可信的搜索路径
32					绝对路径遍历漏洞

表 A.1 网络安全漏洞风险分类示例表（续）

序号	漏洞大类	漏洞小类		漏洞子类
33			路径遍历	相对路径遍历漏洞
34				任意文件下载漏洞
35			后置链接	重定向
36				暗链或外链
37			跨站请求伪造	未验证的 CSRF 令牌
38				无 CSRF 令牌保护的敏感操作
39		数字错误	数字错误	整数溢出错误
40				除零错误
41				未经验证的输入数据
42		竞争条件问题	竞争条件问题	验证码不失效
43				验证码重放攻击
44		处理逻辑错误	处理逻辑错误	手机验证码返回前端
45				任意密码重置漏洞
46				任意用户登录漏洞
47				支付逻辑漏洞
48		加密问题	加密问题	使用过时的加密算法
49				硬编码密钥
50				不安全的加密模式
51				加密密钥泄露
52				缺乏加密
53		授权问题	信任管理问题	会话永不过期
54				Http 拆分
55			权限许可和访问控制问题	垂直越权漏洞
56				平行越权漏洞
57				未授权访问漏洞
58				弱口令问题
59		数据转换问题	数据转换问题	字符串转数字错误
60				数组转换错误
61				对象转换错误
62		未声明功能	未声明功能	内置或匿名用户
63				残留功能
64				预留后门
65	配置错误	配置错误	配置错误	关键参数篡改错误
66				空闲会话超时错误
67				配置错误引起的系统崩溃
68	环境问题	信息泄露	信息泄露	敏感信息泄露
69				日志信息泄露
70				配置或调试信息泄露

表 A.1 网络安全漏洞风险分类示例表（续）

序号	漏洞大类	漏洞小类		漏洞子类
71				侧信道信息泄露
72		故障注入	故障注入	拒绝服务攻击
73				错误处理不足
74	其他	其他	其他	其他

A.2 网络安全资产三级分类示例表

网络安全资产三级分类示例表见表 A.2。

表 A.2 网络安全资产三级分类示例表

序号	资产大类	资产小类	资产子类
1	计算机设备	大型机	大型机应用服务器
2			大型机数据库服务器
3			大型机消息服务器
4			大型机计算服务器
5			大型机虚拟化服务器
6			大型机备份或测试服务器
7		小型机	小型机应用服务器
8			小型机数据库服务器
9			小型机消息服务器
10			小型机计算服务器
11			小型机虚拟化服务器
12			小型机备份或测试服务器
13		服务器	应用服务器
14			数据库服务器
15			消息服务器
16			计算服务器
17			虚拟化服务器
18			运维管理服务器
19			备份或测试服务器
20		工作站	管理员站
21			工程师站
22			操作员站
23		台式计算机	运维管理台式计算机
24			用户台式计算机
25			开发台式计算机

表 A.2 网络安全资产三级分类示例表(续)

序号	资产大类	资产小类	资产子类
26	计算机设备	便携计算机	运维管理便携计算机
27			用户便携计算机
28			开发便携计算机
29	存储设备	磁带机	磁带机
30		磁盘阵列	主磁盘阵列
31			备份磁盘阵列
32		磁带	磁带
33		光盘	光盘
34		软盘	软盘
35		移动硬盘	移动硬盘
36	智能终端设备	感知节点设备（物联网感知终端）	物联网感知终端和摄像头
37			智能终端
38		移动终端	移动终端
39	网络设备	路由器	接入路由器
40			汇聚路由器
41			核心路由器
42			无线路由器
43		网关	认证网关
44			物联网网关
45			多媒体网关
46			应用网关
47		交换机	核心交换机
48			汇聚交换机
49			接入交换机
50			管理交换机
51	传输线路	光纤	裸光纤
52			数字专线
53			互联网专线
54			光纤宽带
55		双绞线	办公局域网络
56			数据中心网络
57	安全设备	防火墙	互联网出口防火墙
58			区域边界防火墙

表 A.2 网络安全资产三级分类示例表(续)

序号	资产大类	资产小类	资产子类
59	安全设备	入侵检测/防护系统	入侵检测
60			入侵防御
61			应用安全防护
62			终端管理
63			威胁感知
64			日志审计
65			上网行为管理
66		防病毒网关	网络防病毒
67			服务器防病毒
68			终端防病毒
69		VPN	IPSec VPN
70			SSL VPN
71	应用系统	应用系统	管理服务端应用
72			Web 前端应用
73			App 应用
74	应用系统	应用系统	小程序应用
75			公众号
76	应用软件	办公软件	办公软件
77		各类工具软件	各类工具软件
78		移动应用软件	移动应用软件
79	系统软件	操作系统	服务器操作系统
80			工作站操作系统
81			终端操作系统
82			其他操作系统
83		数据库管理系统	业务数据库
84			日志数据库
85			配置数据库
86		中间件	Web 中间件
87			消息中间件
88			服务总线
89			其他中间件
90		开发系统	开发系统
91		语句包	语句包
92	支撑平台	云计算平台	云计算平台
93		大数据平台	大数据平台
94	服务接口	服务接口	服务接口
95	数据资料	源代码	源代码
96		数据库数据	业务数据

表 A.2 网络安全资产三级分类示例表（续）

序号	资产大类	资产小类	资产子类
97	数据资料	数据库数据	日志和调试数据
98			配置数据
99		系统文档	系统文档
100		运行管理规范	运行管理规范
101		计划	计划
102		报告	报告
103		用户手册	用户手册
104	办公设备	打印机	打印机
105		复印机	复印机
106		扫描仪	扫描仪
107		传真机	传真机
108	保障设备	UPS	UPS
109		变电设备	变电设备
110		空调	空调
111		保险柜	保险柜
112	保障设备	文件柜	文件柜
113		门禁	门禁
114		消防设施	消防设施

附 录 B
（资料性）
网络安全漏洞风险与严重程度对应关系及资产重要性等级识别示例表

B.1 网络安全漏洞风险与严重程度对应关系示例表

网络安全漏洞风险与严重程度对应关系示例表见表 B.1。

表 B.1 网络安全漏洞风险与严重程度对应关系示例表

序号	漏洞分类	漏洞严重程度
1	不可控的内存分配	很低
2	内存泄露	低
3	敏感信息存储于上锁不正确的内存空间	很低
4	关键资源路径错误	低
5	栈缓冲区溢出漏洞	很高
6	堆缓冲区溢出漏洞	高
7	缓冲区越界读	中等
8	使用外部控制的格式化字符串	低
9	FastJson 反序列化漏洞	中等
10	存储 xss 漏洞	高
11	反射 xss 漏洞	低
12	Dom 型 xss 漏洞	低
13	shell 命令注入	很高
14	远程命令执行漏洞	很高
15	本地命令执行漏洞	高
16	模板注入	很高
17	木马文件上传	很高
18	YAML 远程代码注入	高
19	LDAP 注入	高
20	表达式注入	高
21	XML 外部实体注入	中等
22	Java 反序列化漏洞	很高
23	XPath 注入	中等
24	NoSQL 注入	中等
25	报错注入	高
26	联合查询 sql 注入	高
27	盲注	高
28	二次 SQL 注入	中等
29	堆叠注入	高
30	排序注入	中等
31	不可信的搜索路径	中等

表 B.1 网络安全漏洞风险与严重程度对应关系示例表（续）

序号	漏洞分类	漏洞严重程度
32	绝对路径遍历漏洞	高
33	相对路径遍历漏洞	低
34	任意文件下载漏洞	中等
35	重定向	很低
36	暗链或外链	很低
37	未验证的 CSRF 令牌	很低
38	无 CSRF 令牌保护的敏感操作	低
39	整数溢出错误	低
40	除零错误	低
41	未经验证的输入数据	低
42	验证码不失效	中等
43	验证码重放攻击	中等
44	手机验证码返回前端	高
45	任意密码重置漏洞	高
46	任意用户登录漏洞	高
47	支付逻辑漏洞	高
48	使用过时的加密算法	低
49	硬编码密钥	中等
50	不安全的加密模式	低
51	加密密钥泄露	低
52	缺乏加密	低
53	会话永不过期	低
54	Http 拆分	很低
55	垂直越权漏洞	高
56	平行越权漏洞	中等
57	未授权访问漏洞	中等
58	弱口令问题	高
59	字符串转数字错误	很低
60	数组转换错误	低
61	对象转换错误	很低
62	内置或匿名用户	中等
63	残留功能	低
64	预留后门	高
65	关键参数篡改错误	中等
66	空闲会话超时错误	低
67	配置错误引起的系统崩溃	中等
68	敏感信息泄露	高
69	日志信息泄露	中等

表 B.1 网络安全漏洞风险与严重程度对应关系示例表（续）

序号	漏洞分类	漏洞严重程度
70	配置或调试信息泄露	低
71	侧信道信息泄露	很低
72	拒绝服务攻击	低
73	错误处理不足	低
74	其他	很低

B.2 网络安全资产重要性等级识别示例表

网络安全资产重要性等级识别示例表见表 B.2。

表 B.2 网络安全资产重要性等级识别示例表

序号	资产分类	保密性赋值	完整性赋值	可用性赋值	综合计算	资产重要性等级
1	大型机应用服务器	3	5	5	5	很高
2	大型机数据库服务器	5	5	5	5	很高
3	大型机消息服务器	3	5	4	4	高
4	大型机计算服务器	3	5	4	4	高
5	大型机虚拟化服务器	5	5	4	5	很高
6	大型机备份或测试服务器	3	2	2	3	中等
7	小型机应用服务器	3	5	5	5	很高
8	小型机数据库服务器	5	5	5	5	很高
9	小型机消息服务器	3	5	4	4	高
10	小型机计算服务器	3	5	4	4	高
11	小型机虚拟化服务器	5	5	4	5	很高
12	小型机备份或测试服务器	3	2	2	3	中等
13	应用服务器	3	5	5	5	很高
14	数据库服务器	5	5	5	5	很高
15	消息服务器	3	5	4	4	高
16	计算服务器	3	5	4	4	高
17	虚拟化服务器	5	5	4	5	很高
18	运维管理服务器	4	4	3	4	高
19	备份或测试服务器	3	2	2	3	中等
20	管理员站	3	3	4	4	高
21	工程师站	3	3	4	4	高
22	操作员站	2	2	3	3	中等
23	运维管理台式计算机	2	2	3	3	中等
24	用户台式计算机	1	1	1	1	很低
25	开发台式计算机	2	1	2	2	低
26	运维管理便携计算机	2	2	3	3	中等

表 B.2 网络安全资产重要性等级识别示例表（续）

序号	资产分类	保密性赋值	完整性赋值	可用性赋值	综合计算	资产重要性等级
27	用户便携计算机	1	1	1	1	很低
28	开发便携计算机	2	1	2	2	低
29	磁带机	2	2	1	2	低
30	主磁盘阵列	5	4	5	5	很高
31	备份磁盘阵列	5	4	3	4	高
32	磁带	2	2	1	2	低
33	光盘	2	1	1	2	低
34	软盘	1	1	1	1	很低
35	移动硬盘	2	1	1	2	低
36	物联网感知终端和摄像头等	1	1	1	1	很低
37	智能终端	1	1	1	1	很低
38	移动终端	1	1	1	1	很低
39	接入路由器	1	1	1	1	很低
40	汇聚路由器	1	1	3	2	低
41	核心路由器	3	4	5	4	高
42	无线路由器	1	1	1	1	很低
43	认证网关	3	4	5	4	高
44	物联网网关	1	4	5	4	高
45	多媒体网关	1	4	5	4	高
46	应用网关	1	4	5	4	高
47	核心交换机	3	5	5	5	很高
48	汇聚交换机	1	3	3	3	中等
49	接入交换机	1	1	1	1	很低
50	管理交换机	1	1	1	1	很低
51	裸光纤	1	3	5	3	中等
52	数字专线	3	4	5	4	高
53	互联网专线	1	3	5	3	中等
54	光纤宽带	1	1	1	1	很低
55	办公局域网络	1	1	1	1	很低
56	数据中等心网络	3	4	5	4	高
57	互联网出口防火墙	4	4	5	5	很高
58	区域边界防火墙	1	3	3	3	中等
59	入侵检测	1	3	3	3	中等
60	入侵防御	1	3	3	3	中等
61	应用安全防护	1	3	3	3	中等
62	终端管理	3	4	4	4	高
63	威胁感知	1	3	3	3	中等

表 B.2 网络安全资产重要性等级识别示例表（续）

序号	资产分类	保密性赋值	完整性赋值	可用性赋值	综合计算	资产重要性等级
64	日志审计	4	4	5	5	很高
65	上网行为管理	1	3	3	3	中等
66	网络防病毒	1	3	3	3	中等
67	服务器防病毒	2	4	5	4	高
68	终端防病毒	1	3	3	3	中等
69	IPSec VPN	1	3	4	3	中等
70	SSL VPN	1	3	3	3	中等
71	管理服务端应用	3	4	5	4	高
72	Web 前端应用	1	2	4	3	中等
73	App 应用	1	2	4	3	中等
74	小程序应用	1	2	4	3	中等
75	公众号	1	2	3	2	低
76	办公软件	1	1	1	1	很低
77	各类工具软件	1	1	1	1	很低
78	移动应用软件	1	1	1	1	很低
79	服务器操作系统	3	4	5	4	高
80	工作站操作系统	1	3	3	3	中等
81	终端操作系统	1	2	2	2	低
82	其他操作系统	1	2	2	2	低
83	业务数据库	5	5	5	5	很高
84	日志数据库	3	4	5	4	高
85	配置数据库	4	3	4	4	高
86	Web 中等间件	1	1	4	2	低
87	消息中等间件	1	1	3	2	低
88	服务总线	3	3	3	3	中等
89	其他中等间件	1	1	3	2	低
90	开发系统	1	3	2	2	低
91	语句包	1	1	1	1	很低
92	云计算平台	5	5	5	5	很高
93	大数据平台	5	5	5	5	很高
94	服务接口	2	2	4	3	中等
95	源代码	3	4	1	3	中等
96	业务数据	5	5	5	5	很高
97	日志和调试数据	3	2	2	3	中等
98	配置数据	3	3	3	3	中等
99	系统文档	2	1	1	2	低
100	运行管理规范	1	1	1	1	很低

表 B.2 网络安全资产重要性等级识别示例表（续）

序号	资产分类	保密性赋值	完整性赋值	可用性赋值	综合计算	资产重要性等级
101	计划	1	1	1	1	很低
102	报告	1	1	1	1	很低
103	用户手册	1	1	1	1	很低
104	打印机	1	1	1	1	很低
105	复印机	1	1	1	1	很低
106	扫描仪	1	1	1	1	很低
107	传真机	1	1	1	1	很低
108	UPS	1	1	4	2	低
109	变电设备	1	1	5	3	中等
110	空调	1	1	5	3	中等
111	保险柜	1	1	3	2	低
112	文件柜	1	1	3	2	低
113	门禁	1	1	5	3	中等
114	消防设施	1	1	5	3	中等

附 录 C
（资料性）
网络安全漏洞风险级别评估示例

C.1 示例 1：XXX 系统 Shiro 反序列化漏洞风险级别评估示例

C.1.1 漏洞名称

XXX 系统 Shiro 反序列化漏洞。

C.1.2 漏洞危害描述

攻击者可以利用反序列化漏洞，在目标服务器上执行任意代码，可以完全控制受影响的系统应用服务器，进行任意操作。

C.1.3 漏洞风险级别评估

包括但不限于以下内容：

a）漏洞严重程度识别：

1）确定漏洞类型为：Java 反序列化；

2）查漏洞分类与严重程度对应关系表，漏洞严重程度为：很高（5）。

b）资产重要性等级识别：

1）确定漏洞关联的资产类型为：应用服务器；

2）查资产分类与资产重要性等级对应关系表，资产重要性等级为：很高（5）。

c）漏洞风险级别评估：通过漏洞风险级别评估矩阵，可以判定漏洞风险为：超危（5）。

C.2 示例 2：XXX 系统普通用户弱口令漏洞风险级别评估示例

C.2.1 漏洞名称

XXX 系统普通用户弱口令。

C.2.2 漏洞危害描述

攻击者可以利用普通用户弱口令漏洞，直接登录用户站点，查看用户相关信息。

C.2.3 漏洞风险级别评估

包括但不限于以下内容：

a）漏洞严重程度识别：

1）确定漏洞类型为：弱口令问题；

2）查漏洞分类与严重程度对应关系表，漏洞严重程度为：高（4）。

b）资产重要性等级识别：

1）确定漏洞关联的资产类型为：Web 前端应用。

2）查资产分类与资产重要性等级对应关系表，资产重要性等级为：中等（3）。

c）漏洞风险级别评估：通过漏洞风险级别评估矩阵，可以判定漏洞风险为：高危（3.5）。

C.3 示例 3：XXX 系统日志信息泄露漏洞风险级别评估示例

C.3.1 漏洞名称

XXX 系统日志信息泄露。

C.3.2 漏洞危害描述

攻击者可以通过日志信息进行分析利用，可以利用日志信息开展进一步攻击。

C.3.3 漏洞风险级别评估

包括但不限于以下内容：

a）漏洞严重程度识别：

1）确定漏洞类型为：日志信息泄露；

2）查漏洞分类与严重程度对应关系表，漏洞严重程度为：中等（3）。

b）资产重要性等级识别：

1）确定漏洞关联的资产类型为：配置和日志数据；

2）查资产分类与资产重要性等级对应关系表，资产重要性等级为：中等（3）。

c）漏洞风险级别评估：通过漏洞风险级别评估矩阵，可以判定漏洞风险为：中危（3）。

C.4 示例 4：XXX 系统返回中间件版本信息漏洞风险级别评估示例

C.4.1 漏洞名称

XXX 系统返回中间件版本信息。

C.4.2 漏洞危害描述

攻击者可以通过中间件版本信息开展进一步攻击。

C.4.3 漏洞风险级别评估

包括但不限于以下内容：

a）漏洞严重程度识别：

1）确定漏洞类型为：配置或调试信息泄露；

2）查漏洞分类与严重程度对应关系表，漏洞严重程度为：低（2）；

b）资产重要性等级识别：

1）确定漏洞关联的资产类型为：Web 中间件；

2）查资产分类与资产重要性等级对应关系表，资产重要性等级为：低（2）。

c）漏洞风险级别评估：

通过漏洞风险级别评估矩阵，可以判定漏洞风险为：低危（2）。