

# T/JXEA

## 江西省工程师联合会团体标准

T/JXEA 247—2026

### 信息安全技术网络安全漏洞分级分类与 修复优先级判定指南

Guideline for Grading, Classification, and Repair Priority Determination of  
Cybersecurity Vulnerabilities

（征求意见稿）

2026 - XX - XX 发布

2026 - XX - XX 实施

江西省工程师联合会 发布

# 目 录

前 言 .....	3
引 言 .....	4
1. 范 围 .....	5
2. 规范性引用文件 .....	5
3. 术语和定语 .....	5
4. 漏洞分级原则 .....	6
5. 漏洞分级指标体系 .....	6
6. 通用漏洞分级标准 .....	7
7. 漏洞分类原则 .....	8
8. 按成因的漏洞分类 .....	9
9. 按利用方式的漏洞分类 .....	10
10. 修复优先级判定原则 .....	10
11. 修复优先级判定指标 .....	11
12. 优先级等级划分 .....	12
13. 特殊场景优先级调整 .....	12
14. 漏洞分级实施流程 .....	13
15. 漏洞分类实施流程 .....	14
16. 修复优先级判定流程 .....	15
17. 修复优先级动态调整 .....	16
18. 漏洞信息管理要求 .....	16
19. 漏洞信息报送要求 .....	17
20. 标准实施监督 .....	18
21. 附 则 .....	19

# 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。

本文件由江西省工程师联合会提出并归口。

本文件起草单位：

本文件主要起草人：

# 引言

在数字化时代，信息技术飞速发展，网络已深入到社会生活的各个角落。然而，网络安全漏洞也随之成为网络空间面临的重大威胁。当前，网络安全漏洞数量呈快速增长态势，类型愈发复杂多样。从常见的 Web 应用漏洞，如 SQL 注入、跨站脚本攻击，到系统层面的漏洞，如缓冲区溢出、权限提升漏洞等，这些漏洞一旦被恶意利用，可能导致个人隐私泄露、企业数据被盗取、关键信息基础设施瘫痪等严重后果。

网络安全漏洞治理现状不容乐观。一方面，不同组织和企业对漏洞的认知和处理方式存在差异，缺乏统一的分级分类标准，导致在漏洞评估和管理上难以形成有效的协同。另一方面，对于漏洞修复优先级的判定缺乏科学合理的方法，往往依赖主观经验，使得一些高风险漏洞未能及时得到修复，增加了网络安全事件发生的概率。

制定《信息安全技术 网络安全漏洞分级分类与修复优先级判定指南》这一团体标准具有重要意义。它能够各组织和企业提供统一的漏洞分级分类框架，使各方对漏洞的严重程度和类型有清晰的认识。同时，该标准提供科学的修复优先级判定方法，有助于合理分配资源，优先处理高风险漏洞，提高网络安全防护能力。通过本标准的实施，将提升整个行业的网络安全管理水平，保障网络空间的稳定与安全。

# 信息安全技术网络安全漏洞分级分类与修复优先级判定指南

## 1. 范围

本文件规定了信息安全技术网络安全漏洞分级分类与修复优先级判定的相关要求。具体涵盖漏洞的分级原则、分类方法以及修复优先级的判定依据和流程等内容。本文件适用于各类信息系统，包括但不限于政府部门、企事业单位的办公信息系统、工业控制系统、云计算平台、物联网系统等。同时也适用于各类信息产品，如操作系统、数据库管理系统、中间件、网络设备、安全设备等。相关主体包括信息系统和产品的开发方、运营方、使用方以及安全评估机构等。本标准的覆盖边界明确为针对网络安全漏洞的分级分类及修复优先级判定，不涉及漏洞的发现、修复技术实现等其他方面。通过本标准的实施，有助于规范信息系统和产品的网络安全漏洞管理，提高网络安全防护水平，保障信息系统和产品的稳定运行，为相关主体在网络安全漏洞管理方面提供科学、统一的指导。

## 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—2022 信息安全技术 信息安全风险评估规范  
GB/T 25069—2022 信息安全技术 术语  
GB/T 30276—2022 信息安全技术 安全漏洞标识与描述规范  
GB/T 36627—2018 信息安全技术 网络安全漏洞管理规范  
GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求  
GA/T 1763—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

下列术语和定义适用于本文件。

### 1 网络安全漏洞

可被攻击者利用的信息系统安全缺陷。

### 2 漏洞分级

按危害程度划分的漏洞等级体系。

### 3 漏洞分类

按成因或利用方式划分的漏洞类别。

### 4 修复优先级

判定漏洞修复顺序的依据。

5 漏洞利用难度

攻击者利用漏洞的技术门槛。

6 受影响资产范围

漏洞波及的信息系统规模。

4. 漏洞分级原则

遵循科学性、客观性、可操作性基本原则开展漏洞分级工作

4.1 科学性

采用量化与定性结合的判定方法，依据漏洞技术特征制定分级规则

4.2 客观性

以漏洞实际危害为核心依据，避免主观臆断影响分级结果

4.3 可操作性

分级指标清晰易懂，便于安全运维人员快速完成漏洞判定

4.4 统一化

建立全组织统一的漏洞分级体系，保障分级结果一致性

4.5 规范化

遵循国家网络安全相关标准要求，规范分级流程与判定维度

4.6 动态化

结合网络威胁态势变化，定期更新漏洞分级判定规则

4.7 场景适配

针对不同业务场景调整分级权重，适配业务安全防护需求

4.8 数据支撑

基于漏洞利用案例、危害影响数据完成分级判定

4.9 可追溯

保留分级判定过程记录，确保分级结果可回溯验证

4.10 风险匹配

分级结果与组织风险管控策略相匹配，支撑安全资源分配

5. 漏洞分级指标体系

构建多维度漏洞分级判定指标体系

5.1 危害程度指标

包含数据泄露风险、系统控制权影响、业务中断影响

5.2 利用难度指标

包含攻击门槛要求、利用工具成熟度、前置条件复杂度

5.3 影响范围指标

包含资产覆盖范围、业务影响层级、数据敏感程度

5.4 权重分配规则

危害程度占比 40%、利用难度占比 30%、影响范围占比 30%

5.5 量化阈值

设置各指标量化判定阈值，实现半自动化分级判定

5.6 定性补充

针对无法量化的漏洞特征，采用专家评审定性判定

5.7 指标联动

建立指标间联动关系，避免单一指标偏差影响分级结果

5.8 动态调整

根据威胁情报更新调整指标阈值与权重

5.9 场景适配

针对工业控制、云计算等不同场景优化指标体系

5.10 数据采集

通过漏洞扫描工具、威胁情报平台采集指标数据

6. 通用漏洞分级标准

明确危急、高危、中危、低危四级漏洞判定规则

6.1 危急漏洞

可被未授权远程利用，直接获取系统最高权限且无前置条件

6.2 危急漏洞

导致大规模敏感数据泄露，影响范围覆盖核心业务系统

6.3 危急漏洞

引发业务系统完全中断且无法通过冗余恢复服务

6.4 高危漏洞

需低权限用户方可利用，获取系统核心权限或敏感数据

6.5 高危漏洞

利用工具公开且攻击成功率高于 70%，影响范围覆盖部门级业务

6.6 中危漏洞

需特定配置或用户交互方可利用，仅获取非核心敏感信息

6.7 中危漏洞

攻击成功率介于 30%-70%，影响范围覆盖单个业务模块

6.8 低危漏洞

仅需本地访问或高权限用户利用，无实质性业务影响

6.9 低危漏洞

攻击成功率低于 30%，仅影响单个终端或非核心资产

6.10 分级校验

建立分级结果交叉校验机制，避免误判与漏判

表 1 漏洞分级判定实验数据模拟记录表

漏洞编号	漏洞名称/类型	实验触发条件 (利用条件)	实验观测结果 (业务影响)	成功率/范围数据	交叉校验 定级
VUL-2026-001	远程命令执行 (RCE)	未授权远程发送 Payload，无需登录	获取服务器 Root 权限，核心数据库宕机	成功率 95% 影响核心业务	危急
VUL-2026-002	越权访问漏洞	需普通用户登录后构造恶意请求	获取同部门其他用户的订单敏感数据	成功率 80% 影响部门业务	高危
VUL-2026-003	存储型 XSS 漏洞	需管理员点击特定恶意链接触发	获取管理员非核心 Cookie 信息	成功率 50% 影响单个模块	中危
VUL-2026-004	本地信息泄露	需物理接触服务器并在本地操作	仅暴露非敏感的系统版本号信息	成功率 10% 影响单台终端	低危

7. 漏洞分类原则

遵循统一、兼容、可扩展的漏洞分类基本原则

7.1 统一化

采用国家网络安全漏洞分类标准作为基础分类框架

7.2 兼容性

兼容现有漏洞库分类体系，保障历史数据可映射关联

7.3 可扩展性

预留分类扩展接口，支持新型漏洞类型的快速接入

7.4 场景适配

针对不同业务场景优化分类维度，适配安全防护需求

7.5 标准化

遵循 GB/T 30276 等国家相关标准规范分类流程

7.6 层级化

建立一级、二级分类层级体系，实现分类的精细化管理

7.7 一致性

保障分类规则在全组织范围内统一执行



### 7.8 可复用

分类体系可直接用于漏洞管理平台的标签化管理

### 7.9 动态更新

根据新型威胁类型更新分类体系

### 7.10 数据对齐

与行业通用漏洞分类标准保持数据对齐

## 8. 按成因的漏洞分类

按漏洞成因划分为代码漏洞、配置漏洞、协议漏洞等类别

### 8.1 代码漏洞

包含缓冲区溢出、SQL 注入、跨站脚本等编码实现缺陷

### 8.2 代码漏洞

由内存管理不当、输入验证缺失等代码逻辑问题引发

### 8.3 配置漏洞

包含权限配置错误、安全策略缺失、默认口令未修改等

### 8.4 配置漏洞

由安全配置未按最佳实践部署引发的安全风险

### 8.5 协议漏洞

包含协议实现缺陷、协议解析异常、协议认证缺失等

### 8.6 协议漏洞

由网络通信协议设计或实现缺陷引发的安全风险

### 8.7 硬件漏洞

包含固件缺陷、硬件逻辑错误、侧信道攻击相关风险

### 8.8 硬件漏洞

由硬件电路设计或固件实现问题引发的安全风险

### 8.9 第三方组件漏洞

包含开源组件、商用软件、第三方服务的安全缺陷

### 8.10 第三方组件漏洞

由第三方软件供应链引入的安全风险

### 8.11 分类映射

建立成因分类与 CVSS 评分体系的映射关系

## 9. 按利用方式的漏洞分类

按漏洞利用方式划分为远程执行、权限提升等类别

### 9.1 远程执行漏洞

包含远程代码执行、远程命令执行等无接触攻击类型

### 9.2 远程执行漏洞

攻击者无需本地访问即可触发漏洞获取系统权限

### 9.3 权限提升漏洞

包含本地权限提升、远程权限提升等权限越权类型

### 9.4 权限提升漏洞

攻击者通过漏洞获取超出授权范围的系统权限

### 9.5 信息泄露漏洞

包含数据泄露、凭证泄露、敏感信息暴露等类型

### 9.6 信息泄露漏洞

攻击者通过漏洞获取未授权访问的敏感数据

### 9.7 拒绝服务漏洞

包含带宽消耗、资源耗尽、服务中断等攻击类型

### 9.8 拒绝服务漏洞

攻击者通过漏洞导致系统或服务无法正常提供服务

### 9.9 绕过防护漏洞

包含身份认证绕过、访问控制绕过、防火墙绕过等

### 9.10 绕过防护漏洞

攻击者通过漏洞绕过现有安全防护机制

### 9.11 利用场景适配

针对不同利用方式制定针对性防护策略

## 10. 修复优先级判定原则

综合危害程度、利用难度、影响范围判定修复优先级

### 10.1 危害优先

将漏洞实际危害程度作为优先级判定核心依据

### 10.2 时效性

结合漏洞公开时间与利用情况调整优先级权重

### 10.3 紧迫性

针对已出现公开利用工具的漏洞提升优先级等级

#### 10.4 影响范围

覆盖核心业务系统的漏洞优先级高于普通资产

#### 10.5 资源适配

结合组织安全资源配置调整优先级判定规则

#### 10.6 动态调整

根据威胁情报更新实时调整修复优先级

#### 10.7 分级对应

修复优先级等级与漏洞分级结果保持对应关联

#### 10.8 责任明确

明确各业务部门与运维团队的优先级判定职责

#### 10.9 可追溯

保留优先级判定过程记录，便于后续审计与复盘

#### 10.10 风险匹配

优先级判定结果与组织风险管控目标保持一致

## 11. 修复优先级判定指标

确定影响修复优先级判定的核心量化与定性指标

#### 11.1 量化指标

包含漏洞 CVSS 评分值、漏洞公开天数、攻击成功率数据

#### 11.2 量化指标

包含受影响资产数量、业务中断损失预估数据

#### 11.3 定性指标

包含漏洞利用复杂度、敏感数据影响程度、业务依赖度

#### 11.4 权重分配

量化指标占比 60%、定性指标占比 40%构建判定体系

#### 11.5 阈值设置

设置各指标的优先级判定阈值，实现自动化判定

#### 11.6 数据采集

通过漏洞管理平台、威胁情报平台采集指标数据

#### 11.7 动态更新

根据威胁态势变化调整指标阈值与权重

#### 11.8 场景适配

针对不同业务场景优化指标权重分配

11.9 专家评审

针对无法量化的指标采用专家评审定性判定

11.10 联动机制

建立优先级指标与漏洞分级指标的联动关系

12. 优先级等级划分

将修复优先级划分为紧急、高、中、低四个等级的规则

12.1 紧急优先级

CVSS 评分 $\geq 9.0$  且存在公开利用工具，影响核心业务系统

12.2 紧急优先级

需在 24 小时内完成修复，避免重大安全事件发生

12.3 高优先级

CVSS 评分介于 7.0-8.9，影响部门级核心业务系统

12.4 高优先级

需在 72 小时内完成修复，避免较大范围安全风险

12.5 中优先级

CVSS 评分介于 4.0-6.9，影响单个业务模块或非核心资产

12.6 中优先级

需在 30 天内完成修复，保障业务正常运行

12.7 低优先级

CVSS 评分 $< 4.0$ ，仅影响单个终端或无实质性业务影响

12.8 低优先级

可在 90 天内完成修复，纳入日常安全运维计划

12.9 优先级调整

根据实际威胁情况调整优先级等级，保障修复时效性

12.10 验证机制

建立优先级判定结果验证机制，避免误判与漏判

13. 特殊场景优先级调整

针对政务、工业控制等特殊场景调整优先级判定规则

13.1 政务场景漏洞优先级调整

漏洞 CVSS 评分权重提升 15%；存在政务数据泄露风险的漏洞直接上调至一级优先级；涉及政务系统可用性中断的漏洞修复时限缩短至 24 小时内

### 13.2 工业控制场景漏洞优先级调整

漏洞影响生产连续性的权重提升 20%；涉及工业控制系统核心控制器的漏洞修复时限不得超过 48 小时；存在工业设备安全风险的漏洞需同步纳入工控安全专项整改清单

### 13.3 跨场景联动调整规则

政务与工业控制场景重叠的漏洞，优先级判定取两者最高阈值；跨场景漏洞修复需建立跨部门协同机制，明确责任主体与协同流程

### 13.4 特殊场景漏洞判定阈值

政务场景 CVSS 评分 $\geq 7.0$  即列为高优先级漏洞；工业控制场景 CVSS 评分 $\geq 6.0$  即列为高优先级漏洞；特殊场景漏洞需单独建立台账进行跟踪管理

### 13.5 特殊场景修复资源倾斜

政务场景漏洞修复所需的安全资源优先调配；工业控制场景漏洞修复需配备工控安全专项技术人员；特殊场景漏洞修复完成后需开展专项安全验证

### 13.6 特殊场景应急响应机制

政务场景漏洞触发红色预警响应；工业控制场景漏洞触发黄色预警响应；特殊场景漏洞应急响应需同步上报行业主管部门

### 13.7 特殊场景合规性要求

政务场景漏洞修复需符合等保 2.0 三级及以上要求；工业控制场景漏洞修复需符合 GB/T 22239-2019 相关要求；特殊场景漏洞整改记录需留存至少 3 年备查

### 13.8 特殊场景验证标准

政务场景漏洞修复后需通过第三方安全检测机构验证；工业控制场景漏洞修复后需开展生产环境模拟测试；特殊场景漏洞验证报告需纳入安全管理档案

## 14. 漏洞分级实施流程

说明漏洞发现后开展分级判定的具体步骤与要求

### 14.1 漏洞信息采集

收集漏洞基础信息包括 CVSS 评分、影响范围、利用复杂度等核心参数；采集漏洞验证结果包括可利用性、攻击路径、影响程度等验证数据；采集漏洞所属业务系统、资产类型等关联信息；采集漏洞发现时间、上报人等流程相关信息

### 14.2 漏洞基础核验

核验采集信息的完整性与准确性；核验漏洞验证结果的有效性与可重复性；核验漏洞影响范围与实际资产的匹配度；核验漏洞相关文档的规范性与可追溯性

### 14.3 分级指标判定

按照 CVSSv3.1 评分标准开展基础分级；结合业务场景调整分级权重；按照漏洞影响范围、利用难度、修

复成本开展多维度判定；按照漏洞分级阈值划分一级、二级、三级、四级优先级

#### 14.4 分级结果确认

组织安全技术人员开展分级结果复核；组织业务部门负责人开展分级结果确认；分级结果需形成书面记录并加盖责任部门公章；分级结果发生争议时需组织专家评审会开展论证

#### 14.5 分级结果存档

将分级判定记录、复核材料、评审意见等纳入漏洞管理档案；按照 GB/T 22239-2019 要求留存分级记录至少 3 年；分级档案需实现电子化存储与权限化管理

#### 14.6 分级结果通报

将分级结果通报至业务部门、运维团队、安全管理部门；将分级结果纳入资产安全管理台账；将分级结果作为安全考核的重要依据

#### 14.7 分级流程优化

每季度开展分级流程有效性评估；每年更新漏洞分级判定指标体系；根据漏洞案例数据优化分级权重分配；建立分级流程持续改进机制

## 15. 漏洞分类实施流程

说明漏洞发现后开展分类标识的具体步骤与要求

#### 15.1 漏洞分类标准制定

依据 GB/T 30279-2020 制定漏洞分类体系；划分网络设备漏洞、主机系统漏洞、应用程序漏洞、数据安全漏洞四大核心类别；细化每类漏洞的子分类标准与判定依据；明确漏洞分类的编码规则与标识方法

#### 15.2 漏洞信息分类

按照漏洞所属资产类型开展一级分类；按照漏洞影响业务范围开展二级分类；按照漏洞技术类型开展三级分类；按照漏洞危害等级开展四级分类

#### 15.3 分类标识制作

按照分类编码规则生成漏洞唯一标识；将分类标识标注至漏洞管理台账与安全告警系统；将分类标识纳入漏洞修复工单与跟踪记录；将分类标识同步至资产安全管理平台

#### 15.4 分类结果核验

组织安全技术人员开展分类结果复核；核验分类结果与漏洞实际技术特征的匹配度；核验分类结果与业务场景的适配性；核验分类标识的规范性与唯一性

#### 15.5 分类结果存档

将分类记录、复核材料、标识样本纳入漏洞管理档案；按照分类编码规则建立漏洞分类索引；实现分类信息与资产信息的关联存储；分类档案需支持多维度查询与统计分析

#### 15.6 分类流程优化

每半年开展分类体系有效性评估；根据新兴漏洞类型更新分类子项；优化分类编码规则提升标识效率；建

立分类流程与分级流程的联动机制

15.7 分类数据统计

按照漏洞类别开展月度统计分析；按照漏洞分类开展年度安全风险评估；按照漏洞分类生成安全态势报告；按照漏洞分类制定针对性防护措施

15.8 分类标识应用

将分类标识作为漏洞修复资源分配的依据；将分类标识作为安全告警过滤的参考标准；将分类标识作为安全培训的核心内容；将分类标识作为安全合规检查的重要指标

16. 修复优先级判定流程

明确从漏洞评估到优先级确定的完整实施步骤

16.1 漏洞评估数据采集

收集漏洞 CVSS 评分、利用复杂度、影响范围等基础数据；收集漏洞所属资产的重要性等级数据；收集漏洞影响业务系统的可用性要求数据；收集漏洞修复所需的技术资源与时间成本数据

16.2 漏洞风险评估

开展漏洞基础风险评分；开展漏洞业务影响评估；开展漏洞利用可能性评估；开展漏洞修复成本效益分析

16.3 优先级权重分配

按照漏洞类别分配基础权重；按照业务场景调整权重系数；按照漏洞影响等级分配优先级权重；按照修复资源可用性调整权重分配

16.4 优先级阈值判定

按照权重分配结果计算优先级综合得分；按照综合得分划分一级、二级、三级、四级优先级；按照优先级阈值确定漏洞修复时限要求；按照优先级阈值确定漏洞修复资源配置

16.5 优先级结果确认

组织安全管理部门开展优先级结果复核；组织业务部门开展优先级结果确认；优先级结果需形成书面记录并同步至相关部门；优先级结果发生争议时需开展专家论证

16.6 优先级结果通报

将优先级结果通报至运维团队、修复团队、业务部门；将优先级结果纳入漏洞修复工单；将优先级结果作为安全运维的核心任务；将优先级结果纳入安全考核指标体系

16.7 优先级动态调整

根据漏洞利用情况调整优先级；根据业务场景变化调整优先级；根据修复进度调整优先级；根据安全态势变化调整优先级

16.8 优先级流程优化

每季度开展优先级判定流程评估；每年更新优先级判定指标体系；优化优先级权重分配模型；建立优先级判定流程与漏洞管理流程的联动机制

## 17. 修复优先级动态调整

规定漏洞利用情况、影响范围变化时的调整规则

### 17.1 漏洞利用情况调整

漏洞被公开披露后优先级上调一级；漏洞出现野外利用案例后优先级上调至最高级；漏洞利用工具公开传播后需开展专项应急响应；漏洞利用范围扩大时需同步调整修复资源配置

### 17.2 影响范围变化调整

漏洞影响范围扩大至核心业务系统时优先级上调一级；漏洞影响范围扩大至跨部门业务系统时需开展专项评估；漏洞影响范围扩大至外部网络时需同步上报行业主管部门；漏洞影响范围缩小后可适当下调优先级

### 17.3 业务场景变化调整

政务场景漏洞涉及核心业务时优先级上调一级；工业控制场景漏洞影响生产连续性时优先级上调至最高级；金融场景漏洞涉及资金安全时需开展专项整改；医疗场景漏洞涉及患者数据安全时优先级上调至一级

### 17.4 修复进度变化调整

修复进度滞后于计划时限 30%时优先级上调一级；修复资源不足时需优先调配核心资源；修复完成后需开展验证并更新优先级状态；修复失败时需重新开展优先级判定

### 17.5 安全态势变化调整

高危漏洞数量激增时需调整整体优先级阈值；重大安全事件发生时需上调同类漏洞优先级；新的攻击技术出现时需优化优先级判定模型；合规性检查发现漏洞时需同步调整优先级

### 17.6 调整记录存档

将调整依据、调整过程、调整结果纳入漏洞管理档案；按照调整时间顺序建立调整记录索引；调整记录需留存至少 3 年备查；调整记录需实现电子化存储与权限化管理

### 17.7 调整结果通报

将调整结果通报至相关部门与人员；将调整结果纳入漏洞修复工单；将调整结果作为安全运维的动态任务；将调整结果纳入安全考核指标体系

### 17.8 调整流程规范

调整优先级需履行书面申请与审批流程；调整优先级需提供充分的依据与数据支撑；调整优先级需同步更新漏洞管理台账；调整优先级需开展后续跟踪与验证

## 18. 漏洞信息管理要求

明确漏洞信息采集、验证、记录与存储的基本规范

### 18.1 漏洞信息采集规范

采集漏洞基础信息包括漏洞编号、发现时间、发现人等；采集漏洞技术信息包括 CVSS 评分、漏洞类型、影响范围等；采集漏洞业务信息包括所属系统、资产重要性、业务影响等；采集漏洞修复信息包括修复方案、



修复时限、修复责任人等

#### 18.2 漏洞信息验证规范

开展漏洞可利用性验证；开展漏洞影响范围验证；开展漏洞修复可行性验证；开展漏洞危害等级验证；验证结果需形成书面报告并由验证人签字确认

#### 18.3 漏洞信息记录规范

按照统一格式记录漏洞全生命周期信息；记录漏洞发现、分级、分类、修复、关闭等全流程信息；记录漏洞调整、验证、复核等变更信息；记录漏洞相关的所有沟通与审批记录

#### 18.4 漏洞信息存储规范

按照 GB/T 22239-2019 要求存储漏洞信息；采用加密方式存储敏感漏洞信息；实现漏洞信息与资产信息的关联存储；实现漏洞信息的多副本备份与异地存储

#### 18.5 漏洞信息访问规范

建立漏洞信息访问权限控制机制；按照角色分配漏洞信息访问权限；审计漏洞信息访问操作记录；定期开展漏洞信息安全检查

#### 18.6 漏洞信息更新规范

实时更新漏洞利用情况与影响范围数据；定期更新漏洞分级与分类信息；定期更新漏洞修复进度与结果数据；定期更新漏洞管理台账与档案

#### 18.7 漏洞信息销毁规范

漏洞修复完成并验证通过后需归档留存；留存期限满足合规性要求后可按照规范流程销毁；销毁过程需履行审批与记录流程；销毁记录需纳入安全管理档案

## 19. 漏洞信息报送要求

规定漏洞信息上报主管部门或相关机构的流程要求

#### 19.1 报送主体规范

明确漏洞信息报送的责任主体为安全管理部门；明确报送责任人与联系方式；明确报送流程的审批节点与权限；明确报送信息的审核标准与要求

#### 19.2 报送内容规范

报送漏洞基础信息包括漏洞编号、发现时间、漏洞类型等；报送漏洞风险信息包括 CVSS 评分、影响范围、危害等级等；报送漏洞修复信息包括修复方案、修复时限、修复进度等；报送漏洞调整信息包括调整依据、调整过程、调整结果等

#### 19.3 报送时限规范

一级优先级漏洞需在发现后 2 小时内报送；二级优先级漏洞需在发现后 12 小时内报送；三级优先级漏洞需在发现后 24 小时内报送；四级优先级漏洞需在发现后 72 小时内报送；重大漏洞需立即报送

#### 19.4 报送方式规范

采用线上报送与线下报送相结合的方式；线上报送需通过指定的安全管理平台完成；线下报送需采用加密邮件或纸质文件方式；报送过程需确保信息的完整性与保密性

#### 19.5 报送审核规范

建立报送信息审核机制；审核报送信息的准确性与完整性；审核报送信息的合规性与安全性；审核报送流程的规范性与审批节点

#### 19.6 报送跟踪规范

建立报送信息跟踪机制；跟踪报送信息的接收与处理情况；跟踪报送信息的反馈与整改情况；跟踪报送信息的统计与分析

#### 19.7 报送归档规范

将报送记录、审核材料、反馈意见纳入漏洞管理档案；按照报送时间顺序建立报送记录索引；报送记录需留存至少 3 年备查；报送记录需实现电子化存储与权限化管理

## 20. 标准实施监督

明确本标准执行情况的监督检查与评估要求

#### 20.1 监督检查主体

明确监督检查的责任主体为安全管理部门；明确监督检查的执行主体为第三方安全检测机构；明确监督检查的参与主体为业务部门与运维团队；明确监督检查的审计主体为内部审计部门

#### 20.2 监督检查内容

检查漏洞分级分类流程的执行情况；检查修复优先级判定流程的执行情况；检查特殊场景优先级调整规则的执行情况；检查修复优先级动态调整规则的执行情况；检查漏洞信息管理要求的执行情况；检查漏洞信息报送要求的执行情况

#### 20.3 监督检查频次

一级优先级漏洞每月开展一次专项检查；二级优先级漏洞每季度开展一次全面检查；三级优先级漏洞每半年开展一次全面检查；四级优先级漏洞每年开展一次全面检查；重大漏洞随时开展专项检查

#### 20.4 监督检查方法

采用现场检查与文档审查相结合的方法；采用自动化工具扫描与人工核查相结合的方法；采用抽样检查与全面检查相结合的方法；采用内部检查与第三方检查相结合的方法

#### 20.5 监督检查结果处理

对不符合标准要求的情况下达整改通知书；对严重不符合标准要求的情况开展问责；对整改情况开展跟踪验证；将监督检查结果纳入安全考核指标体系

#### 20.6 监督评估机制

建立标准实施效果评估机制；每年开展一次标准实施效果评估；评估内容包括标准的适用性、有效性、可操作性；评估结果用于标准的修订与完善

### 20.7 监督整改闭环

建立监督整改闭环管理机制；明确整改责任主体与整改时限；跟踪整改过程与整改结果；验证整改效果并纳入安全管理档案

### 20.8 监督队伍建设

建立专职监督检查队伍；开展监督检查人员的专业培训；提升监督检查人员的技术能力与合规意识；建立监督检查人员的考核与激励机制

## 21. 附则

说明本标准的解释权、实施日期等相关附则内容

### 21.1 标准解释权

明确本标准的解释权归江西省工程师联合会所有；明确标准解释的申请流程与审批要求；明确标准解释的发布形式与范围；明确标准解释的时效性与适用范围

### 21.2 标准实施日期

明确本标准的实施日期为 XXXX 年 XX 月 XX 日；明确标准实施前的过渡期安排；明确标准实施前已存在漏洞的处理规则；明确标准实施后的新旧标准衔接要求

### 21.3 标准修订规则

明确本标准的修订周期与修订流程；明确标准修订的申请主体与审批要求；明确标准修订的内容与发布形式；明确标准修订后的实施日期与过渡期安排

### 21.4 标准废止规则

明确本标准的废止条件与废止流程；明确废止标准的替代方案与实施要求；明确废止标准的留存期限与管理要求；明确废止标准的通知与告知要求

### 21.5 术语与定义

明确本标准涉及的核心术语与定义；明确术语的适用范围与解释依据；明确术语的统一表述与使用要求；明确术语的更新与修订规则

### 21.6 参考文献

列出本标准引用的相关国家标准与行业标准；明确参考文献的编号与名称；明确参考文献的适用范围与引用要求；明确参考文献的更新与修订规则

### 21.7 附则说明

明确本标准的编写与发布单位；明确本标准的备案要求与备案流程；明确本标准的宣传与培训要求；明确本标准的实施与监督责任主体