|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | | |
| 漏洞扫描安全评估报告 | | | | |
| 统信软件logo-专色蓝 | | | | |
| **扫描器版本号** | 0.1 | **目标主机IP** |  |
| **目标主机用户** |  | **扫描耗时** |  |
| **扫描开始日期** | |  | |
| **扫描结束日期** | |  | |
| **扫描状态** | |  | |
| **目标主机系统版本** | |  | |

目录

[1 检测结果综述](#_Toc548015047)

[2 参考标准](#_Toc706014896)

[3 主机漏洞信息](#_Toc267957269)

[3.1 漏洞等级分布](#_Toc2035256949)

[3.2 漏洞信息](#_Toc592264422)

[3.2.1 严重漏洞](#_Toc1128017174)

[3.2.2 高危漏洞](#_Toc524355571)

[3.2.3 中危漏洞](#_Toc970559344)

[3.2.4 低危漏洞](#_Toc1842338505)

# 检测结果综述

|  |  |  |  |
| --- | --- | --- | --- |
| **0**  严重漏洞（个） | | **0**  高危漏洞（个） | |
| **0**  中危漏洞（个） | **0**  低危漏洞（个） | | **0**  已修复漏洞（个） |

# 参考标准

|  |  |
| --- | --- |
| **资产风险等级** | **资产风险值区域** |
| **wordml://01000003.gif严重漏洞** | 9 <= 漏洞评分 <= 10 |
| **wordml://0100000F.gif高危漏洞** | 7 <= 漏洞评分 < 9 |
| **wordml://01000010.gif中危漏洞** | 4 <= 漏洞评分 < 7 |
| **wordml://01000011.gif低危漏洞** | 0 <= 漏洞评分 < 4 |

漏洞等级说明：

1. 严重漏洞： 具有极高威胁，可能导致系统完全失控，需要立即修复或隔离以防潜在的灾难性后果。
2. 高危漏洞： 具有较高潜在威胁，需要尽快修复，可能导致系统被攻击者控制或敏感信息泄露。
3. 中危漏洞： 威胁相对较低，需要有计划地修复，可能需要特定条件才能成功利用，对系统整体威胁较小。
4. 低危漏洞： 威胁程度相对较小，修复在计划中进行，通常只影响系统的一小部分，需要综合考虑优先级。

# 主机漏洞信息

## 漏洞等级分布

本次任务中，漏洞按严重、高、中、低等级分布结构如下图所示。漏洞等级分布图如下所示：

数量统计图如下：

## 漏洞信息

### 严重漏洞

### 高危漏洞

### 中危漏洞

### 低危漏洞