



明鉴漏洞扫描系统

10.43日照市人民医院健康管理系统前置机

主机漏洞评估报告

**目 录**

1 任务信息 3

2 风险分布 3

2.1 主机风险分布 3

2.2 漏洞风险分布 4

2.3 操作系统分布 4

3 主机信息 5

3.1 主机信息列表 5

4 脆弱账号 5

4.1 脆弱账号列表 5

5 漏洞信息 5

5.1 漏洞分布 5

5.2 漏洞详情 5

5.2.1 高危 5

5.2.2 信息 7

附录A 评估标准 8

附录A.1 主机等级评估标准 8

附录A.2 漏洞等级评估标准 9

# 任务信息

本报告共扫描评估了1个IP，发现紧急漏洞数0个，高危漏洞数1个，中危漏洞数0个，低危漏洞数0个，信息漏洞数10个，为了您的资产安全，请及时修复。

|  |  |
| --- | --- |
| **任务名称** | 10.10.10.43人民医院dmz漏洞扫描202409024 |
| **执行方式** | 立即执行 |
| **存活主机** | 1 |
| **时间统计** | 开始时间：2024-09-24 14:50:12 结束时间：2024-09-24 14:53:21 扫描耗时：3分9秒 |
| **创建者** | admin |

# 风险分布

## 主机风险分布

风险等级列表：

|  |  |
| --- | --- |
| **风险等级** | 主机数量 |
| **紧急** | 0 |
| **高危** | 1 |
| **中危** | 0 |
| **低危** | 0 |
| **信息** | 0 |

风险等级占比分布：



## 漏洞风险分布

漏洞风险等级列表：

|  |  |  |
| --- | --- | --- |
| **风险等级** | **漏洞出现次数** | **百分比** |
| 紧急 | 0 | 0.00% |
| 高危 | 1 | 9.09% |
| 中危 | 0 | 0.00% |
| 低危 | 0 | 0.00% |
| 信息 | 10 | 90.91% |
| 漏洞数量总计 | 11 |  |

漏洞风险等级占比分布：



## 操作系统分布

操作系统情况列表：

|  |  |  |
| --- | --- | --- |
| **操作系统** | **主机数量** | **百分比** |
| Windows | 1 | 100.00% |

操作系统占比分布：

 

# 主机信息

## 主机信息列表

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **主机IP** | **主机名** | **操作系统** | **紧急** | **高危** | **中危** | **低危** | **信息** |
| 10.10.10.43 | DMZ-JKGLXT-SVR | Windows Server 2019 1809/Windows 10 1809 | 0 | 1 | 0 | 0 | 10 |

# 脆弱账号

## 脆弱账号列表

# 漏洞信息

## 漏洞分布

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **漏洞名称** | **影响主机个数** | **影响主机百分比** | **出现次数** |
| 1 | GeneratedSSL/TLS：报告易受攻击的密码套件(CVE-2016-2183)(原理扫描) | 1/1 | 100.00% | 1 |
| 2 | Generated服务器加密通信支持的SSL加密算法(原理扫描) | 1/1 | 100.00% | 1 |
| 3 | Generated服务器支持的SSL加密协议(原理扫描) | 1/1 | 100.00% | 1 |
| 4 | GeneratedASP.NET Server探测 | 1/1 | 100.00% | 2 |
| 5 | Generated允许Traceroute探测 | 1/1 | 100.00% | 1 |
| 6 | GeneratedHTTP Server类型和版本号 | 1/1 | 100.00% | 3 |
| 7 | Generated微软IIS Web服务器版本检测 | 1/1 | 100.00% | 2 |

## 漏洞详情

### 高危

|  |  |
| --- | --- |
| **漏洞名称** | SSL/TLS：报告易受攻击的密码套件(CVE-2016-2183)(原理扫描) |
| **影响主机** | 10.10.10.43:3389 |
| **漏洞类型** | 协议 |
| **CVSS评分** | 7.5 |
| **CVE编号** | CVE-2016-2183 |
| **CNNVD编号** | CNNVD-201608-448 |
| **CNCVE编号** | CNCVE-20162183 |
| **BUGTRAQ** | 95568 |
| **漏洞描述** | TLS是安全传输层协议，用于在两个通信应用程序之间提供保密性和数据完整性。TLS, SSH, IPSec协商及其他产品中使用的IDEA、DES及Triple DES密码或者3DES及Triple 3DES存在大约四十亿块的生日界，这可使远程攻击者通过Sweet32攻击，获取纯文本数据。来源链接：https://www.openssl.org/news/secadv/20160922.txt |
| **修复建议** | 避免使用IDEA、DES和3DES算法1、OpenSSL Security Advisory [22 Sep 2016]链接：https://www.openssl.org/news/secadv/20160922.txt请在下列网页下载最新版本： https://www.openssl.org/source/2、对于nginx、apache、lighttpd等服务器禁止使用DES加密算法 主要是修改conf文件3、Windows系统可以参考如下链接：https://social.technet.microsoft.com/Forums/en-US/31b3ba6f-d0e6-417a-b6f1-d0103f054f8d/ssl-medium-strength-cipher-suites-supported-sweet32cve20162183?forum=ws2016https://docs.microsoft.com/zh-cn/troubleshoot/windows-server/windows-security/restrict-cryptographic-algorithms-protocols-schannel |

### 信息

|  |  |
| --- | --- |
| **漏洞名称** | 服务器加密通信支持的SSL加密算法(原理扫描) |
| **影响主机** | 10.10.10.43:3389 |
| **漏洞类型** | 其他漏洞 |
| **CVSS评分** | 0.0 |
| **漏洞描述** | 远程连接SSL端口，探测目标服务器支持的SSL加密算法 |
| **修复建议** | 探测脚本，无需修改 |

|  |  |
| --- | --- |
| **漏洞名称** | 服务器支持的SSL加密协议(原理扫描) |
| **影响主机** | 10.10.10.43:3389 |
| **漏洞类型** | 其他漏洞 |
| **CVSS评分** | 0.0 |
| **漏洞描述** | 远程连接SSL端口，探测目标服务器支持的SSL加密协议 |
| **修复建议** | 探测脚本，无需修改 |

|  |  |
| --- | --- |
| **漏洞名称** | ASP.NET Server探测 |
| **影响主机** | 10.10.10.43:8001,10.10.10.43:8002 |
| **漏洞类型** | 编程语言 |
| **CVSS评分** | 0.0 |
| **漏洞描述** | 探测远程主机上安装的ASP.NET服务，并报告版本信息 |
| **修复建议** | 服务探测，无需修改 |

|  |  |
| --- | --- |
| **漏洞名称** | 允许Traceroute探测 |
| **影响主机** | 10.10.10.43:0 |
| **漏洞类型** | 其他漏洞 |
| **CVSS评分** | 0.0 |
| **漏洞描述** | 使用Traceroute探测来获取扫描器与远程主机之间的路由信息。攻击者可以利用这些信息来了解目标网络的网络拓扑。 |
| **修复建议** | 在防火墙出站规则中禁用echo-reply（type 0）、time-exceeded（type 11）、destination-unreachable（type 3）类型的ICMP包。 |

|  |  |
| --- | --- |
| **漏洞名称** | HTTP Server类型和版本号 |
| **影响主机** | 10.10.10.43:80,10.10.10.43:8001,10.10.10.43:8002 |
| **漏洞类型** | Web服务器类漏洞 |
| **CVSS评分** | 0.0 |
| **漏洞描述** | 此策略枚举检测HTTP服务器类型，并设置相应KB。 |
| **修复建议** | 配置您的服务器以使用像'Wintendo httpD w/Dotmatrix display'等替代名称，一定要删除像apache\_pb.gif等常见的标志。 如果目前使用的是Apache，您可以通过设置'ServerTokens Prod'来限制从服务器发出的响应头中的信息。 |

|  |  |
| --- | --- |
| **漏洞名称** | 微软IIS Web服务器版本检测 |
| **影响主机** | 10.10.10.43:8001,10.10.10.43:8002 |
| **漏洞类型** | Web服务器类漏洞 |
| **CVSS评分** | 0.0 |
| **漏洞描述** | 此脚本检测安装的MS IIS Web服务器并将结果设置为KB |
| **修复建议** | IIS服务探测, 无需修改 |

1. 评估标准
	1. 主机等级评估标准

目前定义有四类风险等级，具体定义依据扫描的漏洞结果根据算法得出风险等级：

|  |  |
| --- | --- |
| 风险等级 | 说明 |
| 非常危险 | 主机安全评分1-45分 |
| 比较危险 | 主机安全评分46-57分 |
| 比较安全 | 主机安全评分58-75分 |
| 非常安全 | 主机安全评分76-100分 |

* 1. 漏洞等级评估标准

目前定义有五类风险等级，具体定义依据评分系统CVSS V3.0结合实际可能造成的影响评估：

|  |  |
| --- | --- |
| 风险等级 | 说明 |
| 紧急 | 可以直接被利用的漏洞，且利用难度较低。被攻击之后可能对主机的正常运行造成严重影响，或对用户财产及个人信息造成重大损失。 |
| 高危 | 被利用之后，造成的影响较大，但直接利用难度较高的漏洞，或本身无法直接攻击，但能为进一步攻击造成极大便利的漏洞 |
| 中危 | 利用难度较高，或满足严格要求才能实现攻击的漏洞，或漏洞本身无法被直接攻击，但能为进一步攻击起较大帮助作用的漏洞 |
| 低危 | 无法直接实现攻击，但提供的信息可能让攻击者更容易找到其他安全漏洞。 |
| 信息 | 本身对主机安全没有直接影响，提供的信息可能为攻击者提供少量帮助，或可用于其他手段的攻击。 |