主机漏洞扫描

综合报告

|  |  |  |  |
| --- | --- | --- | --- |
| ■文档类型 | 主机漏洞扫描综合报告 | ■密级 | 限制分发 |
| ■版本编号 | V1.0 | ■导出时间 | 2024-08-14 |
| ■扫描时间 | 2024-08-14 10:01:32 | ■结束时间 | 2024-08-14 10:07:26 |

|  |
| --- |
|  |

|  |
| --- |
| 目录 |
| [一. 任务概述 - 1 -](#_Toc32300)  [1.1 任务信息 - 1 -](#_Toc10167)  [1.2 风险综述 - 1 -](#_Toc7793)  [1.3 主机风险等级分布 - 1 -](#_Toc21856)  [1.4 漏洞风险分布 - 2 -](#_Toc16299)  [1.5 漏洞应用分类 - 3 -](#_Toc29236)  [1.6 Top10漏洞 - 3 -](#_Toc27216)  [1.7 Top10服务 - 4 -](#_Toc26374)  [二. 主机风险等级列表 - 5 -](#_Toc17718)  [三. 漏洞风险列表 - 5 -](#_Toc25439)  [3.1 可入侵漏洞分析 - 5 -](#_Toc32163)  [3.2 版本漏洞分析 - 5 -](#_Toc13259)  [3.2.1 高风险 - 6 -](#_Toc6378)  [3.2.2 中风险 - 7 -](#_Toc20344)  [3.2.3 低风险 - 11 -](#_Toc17409)  [3.3 弱口令列表 - 13 -](#_Toc32766)  [附录A 附录 - 13 -](#_Toc6320)  [A.1 漏洞风险说明 - 13 -](#_Toc23629)  [A.2 主机漏洞加固策略 - 13 -](#_Toc19785) |

1. 任务概述
   1. 任务信息

|  |  |
| --- | --- |
| **任务名称** | 阜阳市环保局 (可入侵漏扫/版本漏扫/常规端口) |
| **扫描目标** | 10.34.232.237;10.34.232.239;10.34.232.240;10.34.232.241;10.34.232.242;10.34.232.243 |
| **存活主机数** | 5 |
| **开始时间** | 2024-08-14 10:01:32 |
| **结束时间** | 2024-08-14 10:07:26 |
| **系统版本信息** | 2.0.258 |

* 1. 风险综述

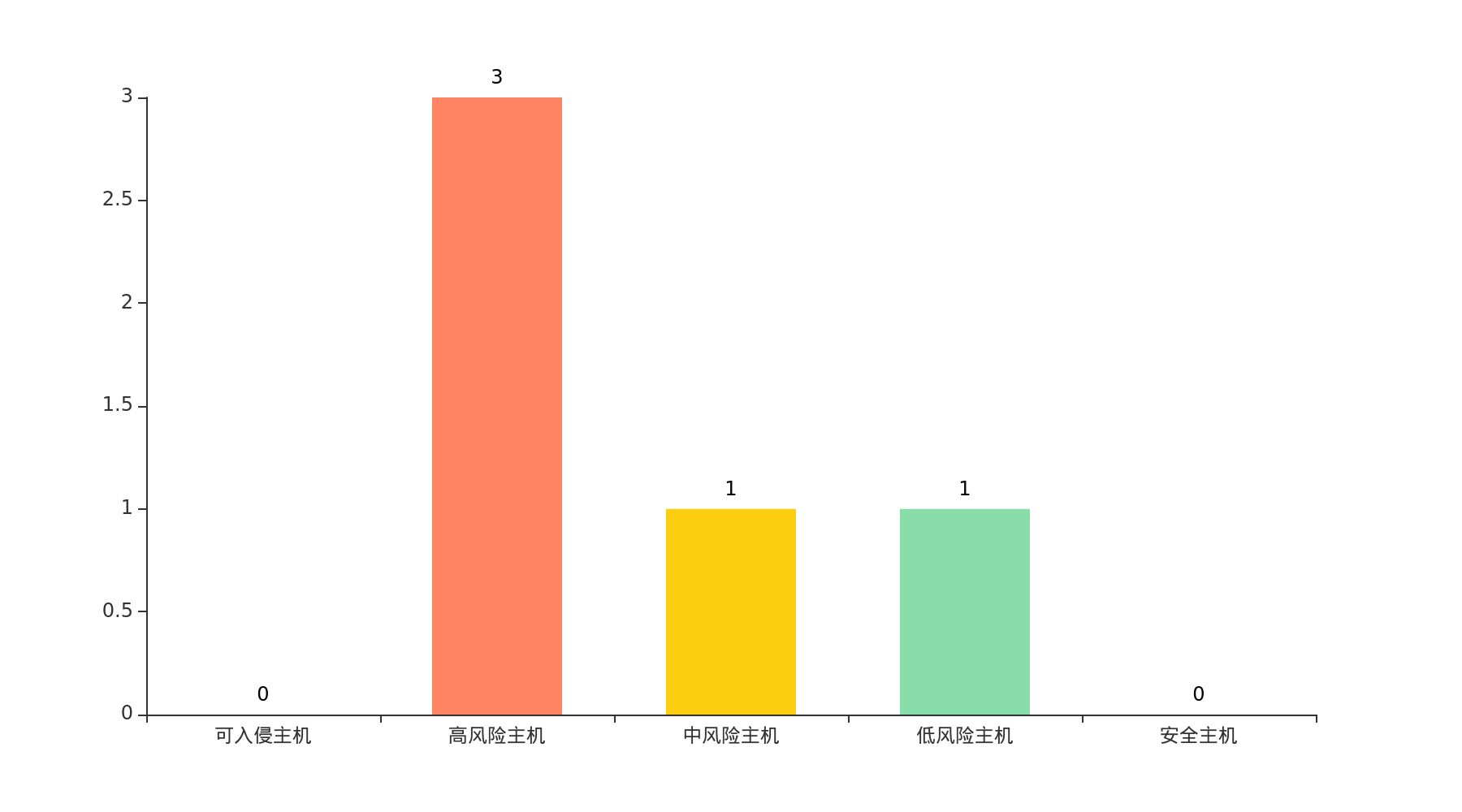
本次评估共发现存活主机5个，其中发现可入侵漏洞0个，高风险漏洞12个，弱口令0个，风险综述如下所示：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 存活主机数量 | 弱口令 | 可入侵漏洞 | 高风险 | 中风险 | 低风险 | 小计 |
| 5 | **0** | **0** | **12** | **34** | **26** | **72** |

* 1. 主机风险等级分布

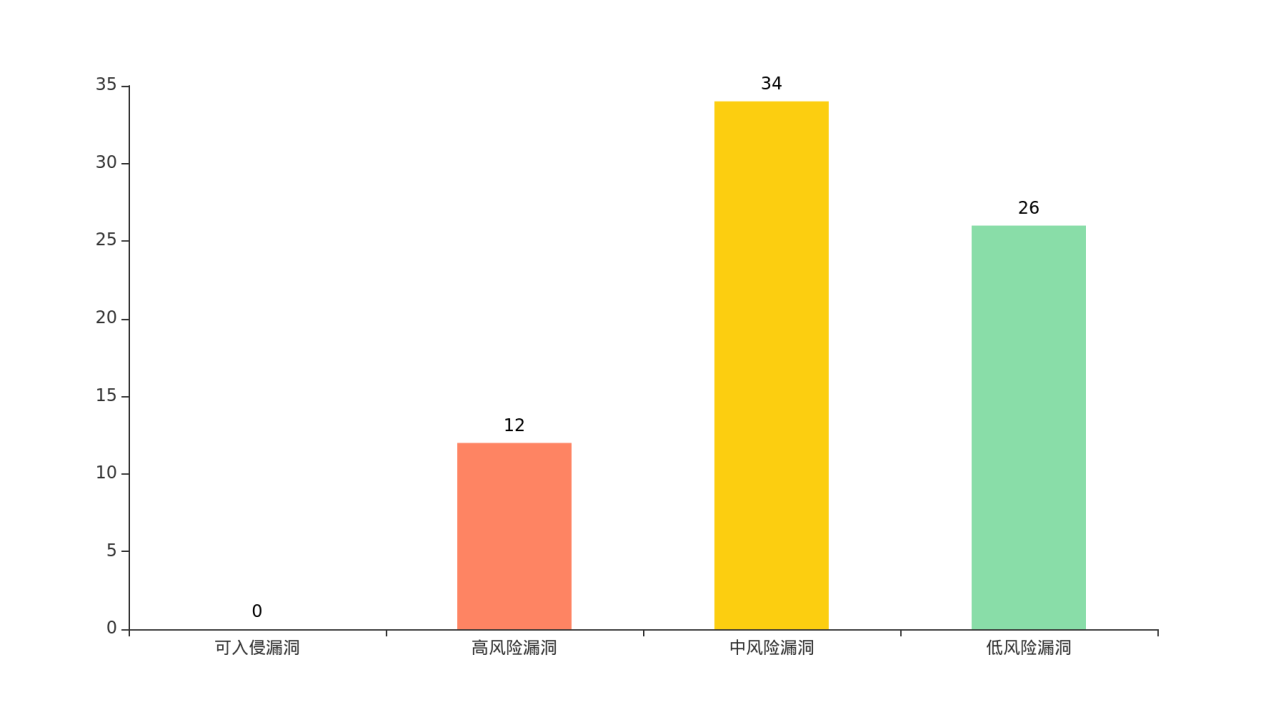
本次评估的5个主机中，存在可入侵漏洞主机0个，存在高风险漏洞主机3个，如下所示：

|  |  |
| --- | --- |
| **可入侵主机** | 0 |
| **高风险主机** | 3 |
| **中风险主机** | 1 |
| **低风险主机** | 1 |
| **安全主机** | 0 |

* 1. 漏洞风险分布

本次评估的5个主机中，存在可入侵风险漏洞0个，存在高风险漏洞12个，如下所示：

|  |  |
| --- | --- |
| **可入侵漏洞** | 0 |
| **高风险漏洞** | 12 |
| **中风险漏洞** | 34 |
| **低风险漏洞** | 26 |



* 1. 漏洞应用分类

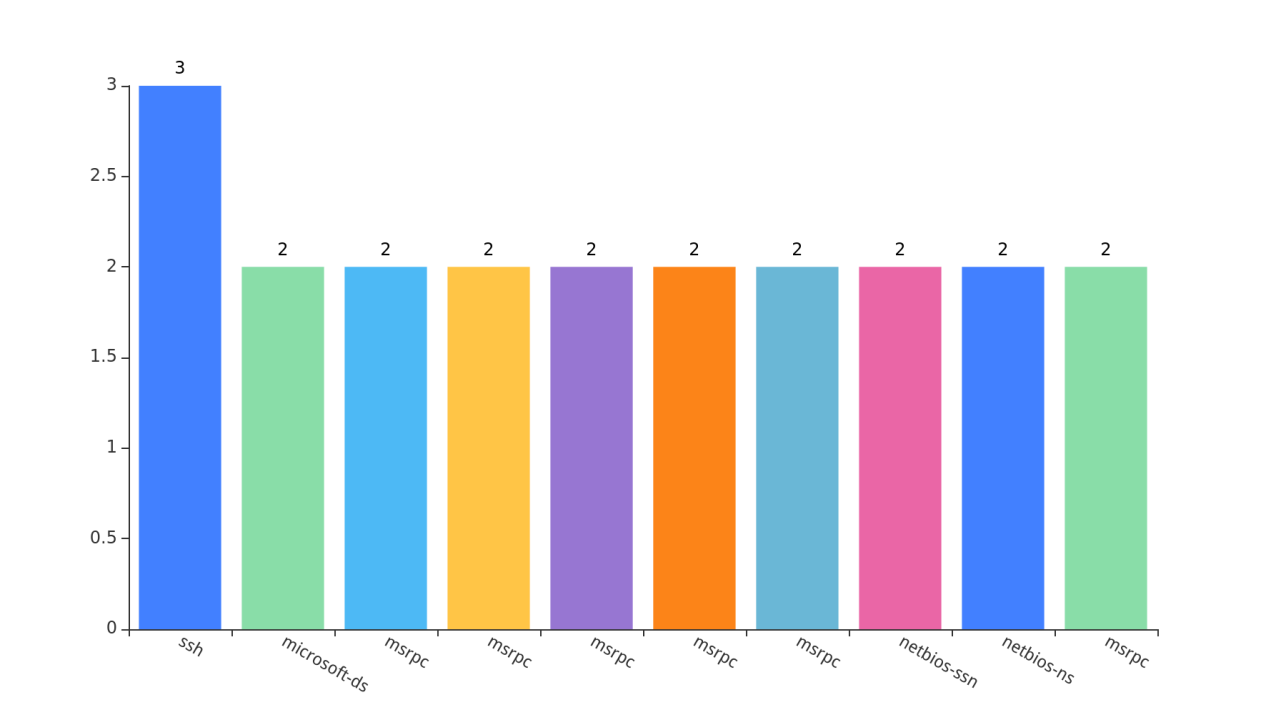
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 应用 | 高风险 | 中风险 | 低风险 | 合计 |
| OpenSSH | 12 | 33 | 3 | 48 |
| other | 0 | 1 | 21 | 22 |
| SSL/TLS | 0 | 0 | 2 | 2 |
| **合计** | **12** | **34** | **26** | **72** |

* 1. Top10漏洞

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 漏洞名称 | 风险等级 | 数量 | 影响资产 |
| 1 | OpenSSH 操作系统命令注入漏洞(CVE-2020-15778) | 高风险 | 3 | 10.34.232.243:22; 10.34.232.239:22 10.34.232.240:22 |
| 2 | OpenSSH 安全漏洞(CVE-2021-41617) | 高风险 | 3 | 10.34.232.243:22; 10.34.232.239:22 10.34.232.240:22 |
| 3 | OpenSSH 代码问题漏洞(CVE-2023-38408) | 高风险 | 3 | 10.34.232.243:22; 10.34.232.239:22 10.34.232.240:22 |
| 4 | OpenSSH 安全漏洞(CVE-2023-51385) | 高风险 | 3 | 10.34.232.243:22; 10.34.232.239:22 10.34.232.240:22 |
| 5 | OpenSSH 安全漏洞(CVE-2016-20012) | 中风险 | 3 | 10.34.232.243:22; 10.34.232.239:22 10.34.232.240:22 |
| 6 | OpenSSH 安全漏洞(CVE-2017-15906) | 中风险 | 3 | 10.34.232.243:22; 10.34.232.239:22 10.34.232.240:22 |
| 7 | OpenSSH 竞争条件问题漏洞(CVE-2018-15473) | 中风险 | 3 | 10.34.232.243:22; 10.34.232.239:22 10.34.232.240:22 |
| 8 | OpenSSH 信息泄露漏洞(CVE-2018-15919) | 中风险 | 3 | 10.34.232.243:22; 10.34.232.239:22 10.34.232.240:22 |
| 9 | OpenSSH 访问控制错误漏洞(CVE-2018-20685) | 中风险 | 3 | 10.34.232.243:22; 10.34.232.239:22 10.34.232.240:22 |
| 10 | OpenSSH 访问控制错误漏洞(CVE-2019-6109) | 中风险 | 3 | 10.34.232.243:22; 10.34.232.239:22 10.34.232.240:22 |

* 1. Top10服务

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 端口 | 服务 | 描述 | 数量 | 存在主机 |
| 1 | 22 | ssh | OpenSSH | 3 | 10.34.232.239 10.34.232.243 10.34.232.240 |
| 2 | 445 | microsoft-ds | Microsoft Windows Server 2008 R2 - 2012 microsoft-ds | 2 | 10.34.232.241 10.34.232.242 |
| 3 | 49154 | msrpc | Microsoft Windows RPC | 2 | 10.34.232.241 10.34.232.242 |
| 4 | 135 | msrpc | Microsoft Windows RPC | 2 | 10.34.232.241 10.34.232.242 |
| 5 | 49156 | msrpc | Microsoft Windows RPC | 2 | 10.34.232.241 10.34.232.242 |
| 6 | 49155 | msrpc | Microsoft Windows RPC | 2 | 10.34.232.241 10.34.232.242 |
| 7 | 49152 | msrpc | Microsoft Windows RPC | 2 | 10.34.232.241 10.34.232.242 |
| 8 | 139 | netbios-ssn | Microsoft Windows netbios-ssn | 2 | 10.34.232.241 10.34.232.242 |
| 9 | 137 | netbios-ns | Microsoft Windows netbios-ns | 2 | 10.34.232.241 10.34.232.242 |
| 10 | 49153 | msrpc | Microsoft Windows RPC | 2 | 10.34.232.241 10.34.232.242 |



1. 主机风险等级列表

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | IP地址 | 操作系统 | 端口数 | 可入侵漏洞 | 高风险 | 中风险 | 低风险 | 弱口令 | 小计 |
| 1 | 10.34.232.243 | linux | 2 | 0 | 4 | 11 | 6 | 0 | 21 |
| 2 | 10.34.232.239 | linux | 3 | 0 | 4 | 11 | 3 | 0 | 18 |
| 3 | 10.34.232.240 | linux | 2 | 0 | 4 | 11 | 3 | 0 | 18 |
| 4 | 10.34.232.241 | windows | 13 | 0 | 0 | 1 | 7 | 0 | 8 |
| 5 | 10.34.232.242 | windows | 20 | 0 | 0 | 0 | 7 | 0 | 7 |

1. 漏洞风险列表
   1. 可入侵漏洞分析

可入侵漏洞是指有公开利用方法，已验证可远程执行任意命令或者代码，或对系统进行远程拒绝服务攻击，或可获取重要敏感数据。此部分漏洞基于漏洞原理验证识别，在漏洞名称中，会标识【原理扫描】。

对主机资产脆弱性进行分析，共发现存在0个可入侵漏洞，漏洞种类涉及0种，详情请查阅Excel报表附件。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 漏洞名称 | 风险等级 | 加固建议 | 影响资产 |
| **暂未发现漏洞** | | | | |

* 1. 版本漏洞分析

此部分漏洞主要是通过服务版本识别，以及根据权威漏洞库数据，判断资产是否在漏洞影响范围内，从而检测出相关漏洞。

请根据漏洞分类，针对受影响的资产，升级到相关应用的最新版本即可修复此类漏洞。

具体的漏洞详情请参见对应Excel报表附件。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 漏洞类型 | 高风险 | 中风险 | 低风险 | 影响资产 |
| 1 | OpenSSH | 12 | 33 | 3 | 10.34.232.243; 10.34.232.239; 10.34.232.240 |
| 2 | other | 0 | 1 | 21 | 10.34.232.243; 10.34.232.240; 10.34.232.239 10.34.232.241; 10.34.232.242 |
| 3 | SSL/TLS | 0 | 0 | 2 | 10.34.232.243 |

* + 1. 高风险

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 漏洞名称 | 风险等级 | 加固建议 | 影响资产 |
| 1 | OpenSSH 操作系统命令注入漏洞(CVE-2020-15778) | 高风险 | 若您不需要使用该应用或服务，请关闭该应用或服务即可。 目前厂商已经发布了升级补丁以修复这个安全问题，截止2024年7月3日，建议升级到当前最新的版本9.8，或后续更高版本。 Linux系统请在以下页面进行下载： http://www.openssh.com/portable.html  其他版本系统请到厂商主页下载最新版本： http://www.openssh.com/ | 10.34.232.243:22; 10.34.232.239:22 10.34.232.240:22 |
| 2 | OpenSSH 安全漏洞(CVE-2021-41617) | 高风险 | 若您不需要使用该应用或服务，请关闭该应用或服务即可。 目前厂商已经发布了升级补丁以修复这个安全问题，截止2024年7月3日，建议升级到当前最新的版本9.8，或后续更高版本。 Linux系统请在以下页面进行下载： http://www.openssh.com/portable.html  其他版本系统请到厂商主页下载最新版本： http://www.openssh.com/ | 10.34.232.243:22; 10.34.232.239:22 10.34.232.240:22 |
| 3 | OpenSSH 代码问题漏洞(CVE-2023-38408) | 高风险 | 若您不需要使用该应用或服务，请关闭该应用或服务即可。 目前厂商已经发布了升级补丁以修复这个安全问题，截止2024年7月3日，建议升级到当前最新的版本9.8，或后续更高版本。 Linux系统请在以下页面进行下载： http://www.openssh.com/portable.html  其他版本系统请到厂商主页下载最新版本： http://www.openssh.com/ | 10.34.232.243:22; 10.34.232.239:22 10.34.232.240:22 |
| 4 | OpenSSH 安全漏洞(CVE-2023-51385) | 高风险 | 若您不需要使用该应用或服务，请关闭该应用或服务即可。 目前厂商已经发布了升级补丁以修复这个安全问题，截止2024年7月3日，建议升级到当前最新的版本9.8，或后续更高版本。 Linux系统请在以下页面进行下载： http://www.openssh.com/portable.html  其他版本系统请到厂商主页下载最新版本： http://www.openssh.com/ | 10.34.232.243:22; 10.34.232.239:22 10.34.232.240:22 |

* + 1. 中风险

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **漏洞名称** | **风险等级** | **加固建议** | **影响资产** |
| 1 | 检测到远程主机开放了向日葵sunlogin服务 | 中风险 | 如果不是绝对必要，建议您关闭该服务，或者加强该应用的口令 | 10.34.232.241:49158 |
| 2 | OpenSSH 安全漏洞(CVE-2016-20012) | 中风险 | 若您不需要使用该应用或服务，请关闭该应用或服务即可。 目前厂商已经发布了升级补丁以修复这个安全问题，截止2024年7月3日，建议升级到当前最新的版本9.8，或后续更高版本。 Linux系统请在以下页面进行下载： http://www.openssh.com/portable.html  其他版本系统请到厂商主页下载最新版本： http://www.openssh.com/ | 10.34.232.243:22; 10.34.232.239:22 10.34.232.240:22 |
| 3 | OpenSSH 安全漏洞(CVE-2017-15906) | 中风险 | 若您不需要使用该应用或服务，请关闭该应用或服务即可。 目前厂商已经发布了升级补丁以修复这个安全问题，截止2024年7月3日，建议升级到当前最新的版本9.8，或后续更高版本。 Linux系统请在以下页面进行下载： http://www.openssh.com/portable.html  其他版本系统请到厂商主页下载最新版本： http://www.openssh.com/ | 10.34.232.243:22; 10.34.232.239:22 10.34.232.240:22 |
| 4 | OpenSSH 竞争条件问题漏洞(CVE-2018-15473) | 中风险 | 若您不需要使用该应用或服务，请关闭该应用或服务即可。 目前厂商已经发布了升级补丁以修复这个安全问题，截止2024年7月3日，建议升级到当前最新的版本9.8，或后续更高版本。 Linux系统请在以下页面进行下载： http://www.openssh.com/portable.html  其他版本系统请到厂商主页下载最新版本： http://www.openssh.com/ | 10.34.232.243:22; 10.34.232.239:22 10.34.232.240:22 |
| 5 | OpenSSH 信息泄露漏洞(CVE-2018-15919) | 中风险 | 若您不需要使用该应用或服务，请关闭该应用或服务即可。 目前厂商已经发布了升级补丁以修复这个安全问题，截止2024年7月3日，建议升级到当前最新的版本9.8，或后续更高版本。 Linux系统请在以下页面进行下载： http://www.openssh.com/portable.html  其他版本系统请到厂商主页下载最新版本： http://www.openssh.com/ | 10.34.232.243:22; 10.34.232.239:22 10.34.232.240:22 |
| 6 | OpenSSH 访问控制错误漏洞(CVE-2018-20685) | 中风险 | 若您不需要使用该应用或服务，请关闭该应用或服务即可。 目前厂商已经发布了升级补丁以修复这个安全问题，截止2024年7月3日，建议升级到当前最新的版本9.8，或后续更高版本。 Linux系统请在以下页面进行下载： http://www.openssh.com/portable.html  其他版本系统请到厂商主页下载最新版本： http://www.openssh.com/ | 10.34.232.243:22; 10.34.232.239:22 10.34.232.240:22 |
| 7 | OpenSSH 访问控制错误漏洞(CVE-2019-6109) | 中风险 | 若您不需要使用该应用或服务，请关闭该应用或服务即可。 目前厂商已经发布了升级补丁以修复这个安全问题，截止2024年7月3日，建议升级到当前最新的版本9.8，或后续更高版本。 Linux系统请在以下页面进行下载： http://www.openssh.com/portable.html  其他版本系统请到厂商主页下载最新版本： http://www.openssh.com/ | 10.34.232.239:22; 10.34.232.243:22 10.34.232.240:22 |
| 8 | OpenSSH 访问控制错误漏洞(CVE-2019-6110) | 中风险 | 若您不需要使用该应用或服务，请关闭该应用或服务即可。 目前厂商已经发布了升级补丁以修复这个安全问题，截止2024年7月3日，建议升级到当前最新的版本9.8，或后续更高版本。 Linux系统请在以下页面进行下载： http://www.openssh.com/portable.html  其他版本系统请到厂商主页下载最新版本： http://www.openssh.com/ | 10.34.232.239:22; 10.34.232.243:22 10.34.232.240:22 |
| 9 | OpenSSH 路径遍历漏洞(CVE-2019-6111) | 中风险 | 若您不需要使用该应用或服务，请关闭该应用或服务即可。 目前厂商已经发布了升级补丁以修复这个安全问题，截止2024年7月3日，建议升级到当前最新的版本9.8，或后续更高版本。 Linux系统请在以下页面进行下载： http://www.openssh.com/portable.html  其他版本系统请到厂商主页下载最新版本： http://www.openssh.com/ | 10.34.232.239:22; 10.34.232.243:22 10.34.232.240:22 |
| 10 | OpenSSH 信息泄露漏洞(CVE-2020-14145) | 中风险 | 若您不需要使用该应用或服务，请关闭该应用或服务即可。 目前厂商已经发布了升级补丁以修复这个安全问题，截止2024年7月3日，建议升级到当前最新的版本9.8，或后续更高版本。 Linux系统请在以下页面进行下载： http://www.openssh.com/portable.html  其他版本系统请到厂商主页下载最新版本： http://www.openssh.com/ | 10.34.232.243:22; 10.34.232.239:22 10.34.232.240:22 |
| 11 | OpenSSH 安全漏洞(CVE-2023-48795) | 中风险 | 若您不需要使用该应用或服务，请关闭该应用或服务即可。 目前厂商已经发布了升级补丁以修复这个安全问题，截止2024年7月3日，建议升级到当前最新的版本9.8，或后续更高版本。 Linux系统请在以下页面进行下载： http://www.openssh.com/portable.html  其他版本系统请到厂商主页下载最新版本： http://www.openssh.com/ | 10.34.232.243:22; 10.34.232.239:22 10.34.232.240:22 |
| 12 | OpenSSH 安全漏洞(CVE-2023-51384) | 中风险 | 若您不需要使用该应用或服务，请关闭该应用或服务即可。 目前厂商已经发布了升级补丁以修复这个安全问题，截止2024年7月3日，建议升级到当前最新的版本9.8，或后续更高版本。 Linux系统请在以下页面进行下载： http://www.openssh.com/portable.html  其他版本系统请到厂商主页下载最新版本： http://www.openssh.com/ | 10.34.232.243:22; 10.34.232.239:22 10.34.232.240:22 |

* + 1. 低风险

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **漏洞名称** | **风险等级** | **加固建议** | **影响资产** |
| 1 | 检测到远程主机开放了ssh服务 | 低风险 | 若不需要使用此服务，建议关闭此服务；若需要使用此服务，建议在主机防火墙或者网络防火墙限制只有授权IP地址才可以访问此服务。 | 10.34.232.243:22; 10.34.232.240:22 10.34.232.239:22 |
| 2 | 可通过HTTP获取远端WWW服务信息 | 低风险 | 建议您采取以下措施以降低威胁： \* 改变您的HTTP服务器的缺省banner。 | 10.34.232.243:9090; 10.34.232.241:49158 10.34.232.241:80; 10.34.232.242:8011 |
| 3 | 检测到远程主机开放了ftp服务 | 低风险 | 若不需要使用此服务，建议关闭此服务；若需要使用此服务，建议在主机防火墙或者网络防火墙限制只有授权IP地址才可以访问此服务。 | 10.34.232.242:8021 |
| 4 | 可获取到ssh服务版本信息 | 低风险 | 修改源代码或者配置文件，改变该服务的缺省banner信息 | 10.34.232.243:22; 10.34.232.240:22 10.34.232.239:22 |
| 5 | 可通过NetBIOS名字服务端口远程获取系统信息 | 低风险 | 建议您采取以下措施以降低威胁： \* 如果您并不需要提供网络共享服务，可以完全关闭共享。  \* 在网关设备或边界防火墙上过滤对内网主机下列端口的访问： 137/UDP 注意这不能防止内部恶意用户的攻击。如需防止内部恶意用户的攻击，需要安装主机防火墙软件或者启用Windows自带的TCP/IP筛选机制来过滤上述端口。 | 10.34.232.241:137; 10.34.232.242:137 |
| 6 | 检测到远程主机开放了microsoft-ds服务 | 低风险 | 若不需要使用此服务，建议关闭此服务；若需要使用此服务，建议在主机防火墙或者网络防火墙限制只有授权IP地址才可以访问此服务。 | 10.34.232.242:445; 10.34.232.241:445 |
| 7 | 检测到远程主机开放了SQL-Server服务 | 低风险 | 若不需要使用此服务，建议关闭此服务；若需要使用此服务，建议在主机防火墙或者网络防火墙限制只有授权IP地址才可以访问此服务。 | 10.34.232.241:1433 |
| 8 | 检测到SpringBoot指纹信息 | 低风险 | SpringBoot开源框架容易遭受攻击威胁，建议日常保持升级维护此应用。若指纹信息中包含版本号，建议隐藏banner信息。 | 10.34.232.242:8011 |
| 9 | 可获取到SQL-Server服务版本信息 | 低风险 | 修改源代码或者配置文件，改变该服务的缺省banner信息 | 10.34.232.241:1433 |
| 10 | 检测到Spring框架指纹信息 | 低风险 | Spring框架容易遭受攻击威胁，建议日常保持升级维护此应用。若指纹信息中包含版本号，建议隐藏banner信息。 | 10.34.232.242:8011 |
| 11 | OpenSSH 授权问题漏洞(CVE-2021-36368) | 低风险 | 若您不需要使用该应用或服务，请关闭该应用或服务即可。 目前厂商已经发布了升级补丁以修复这个安全问题，截止2024年7月3日，建议升级到当前最新的版本9.8，或后续更高版本。 Linux系统请在以下页面进行下载： http://www.openssh.com/portable.html  其他版本系统请到厂商主页下载最新版本： http://www.openssh.com/ | 10.34.232.243:22; 10.34.232.239:22 10.34.232.240:22 |
| 12 | windows server服务正在运行【原理扫描】 | 低风险 | 如果不需要使用 Server 服务，建议在系统服务列表（services.msc）禁止启动 Server 服务。注意： Server 服务支持此计算机通过网络的文件、打印、和命名管道共享。如果服务停止，这些功能不可用。如果服务被禁用，任何直接依赖于此服务的服务将无法启动。 | 10.34.232.242:445; 10.34.232.241:445 |
| 13 | SSL 证书无法受到信任【原理扫描】 | 低风险 | 若是正式的业务系统，建议购买SSL证书。 | 10.34.232.243:9090 |
| 14 | 可获取目标SSL证书过期时间【原理扫描】 | 低风险 | 仅用作信息收集，无需修复。 | 10.34.232.243:9090 |

* 1. 弱口令列表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | IP地址 | 端口 | 类型 | 用户名 | 口令 |
| **暂未发现弱口令** | | | | | |

1. 附录
   1. 漏洞风险说明

漏洞是与信息资产有关的弱点或安全隐患。漏洞本身并不对资产构成危害，但是在一定条件得到满足时，漏洞会被威胁加以利用来对信息资产造成危险！本报告的漏洞共分了以下4种漏洞风险等级。

|  |  |
| --- | --- |
| 危险程度 | 危险程度说明 |
| **可入侵漏洞**  **（严重）** | 有公开利用方法，已验证可远程执行任意命令或者代码，或对系统进行远程拒绝服务攻击，或可获取重要敏感数据。此部分漏洞基于漏洞原理验证识别，在漏洞名称中，会标识【原理扫描】。 |
| **高** | 攻击者可以远程执行任意命令或者代码，或对系统进行远程拒绝服务攻击，或可获取重要敏感数据。此部分漏洞主要通过服务版本识别，可能会有一定的误报。 |
| **中** | 攻击者可以远程创建、修改、删除部分文件或数据，或对普通服务进行拒绝服务攻击。此部分漏洞主要通过服务版本识别，可能会有一定的误报。 |
| **低** | 攻击者可以获取某些系统、服务的信息，或读取某些系统文件和数据。此部分漏洞主要通过服务版本识别，可能会有一定的误报。 |

* 1. 主机漏洞加固策略

基于多年的安全整改经验，提供了以下5种安全加固整改策略，并对不同整改建议的有效防护度、整改困难度作了评级参考，有效防护度越高则表示加固效果越好，整改困难度越高则表示整改方案实施越难。您可以根据实际的业务情况，参考以下表，选择加固整改策略。

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 加固整改策略 | 有效  防护度 | 整改  困难度 |
| 1 | 根据漏洞整改建议打补丁或者修改配置进行安全加固，加固前建议作好相关备份以便回退；建议所有 Windows 系统使用"Windows Update"进行更新。 | 高 | 高 |
| 2 | 若存在漏洞的应用服务平时不需要使用，建议关闭这些不必要的服务或应用。 | 高 | 低 |
| 3 | 若存在漏洞的应用服务不需要对外开放或者只对部分用户开放，建议在主机防火墙上进行访问控制，限定只有合法IP才能访问此应用。 | 中 | 低 |
| 4 | 若不便在主机防火墙上配置，建议在网络/出口防火墙上做白名单访问控制。 | 低 | 低 |
| 5 | 建议修改应用的banner信息，隐藏应用名称、版本号等信息，让攻击者无法识别目标系统，使之难以进行针对性的攻击入侵。 | 低 | 中 |