

明鉴网络安全等级保护检查工具箱

**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 7

5.2.1 紧急 7

5.2.2 高危 9

5.2.3 中危 17

5.2.4 低危 24

5.2.5 信息 26

附录A 评估标准 30

附录A.1 主机等级评估标准 30

附录A.2 漏洞等级评估标准 30

# 任务信息

本报告共扫描评估了1个IP，发现紧急漏洞数2个，高危漏洞数17个，中危漏洞数12个，低危漏洞数3个，信息漏洞数16个，为了您的资产安全，请及时修复。

|  |  |
| --- | --- |
| **任务名称** | 涿鹿文景工作室 |
| **执行方式** | 立即执行 |
| **扫描目标** | 111.231.21.41 |
| **存活主机** | 1 |
| **时间统计** | 开始时间：2024-11-05 23:58:00 结束时间：2024-11-06 00:17:07 扫描耗时：19分7秒 |
| **创建者** | admin |

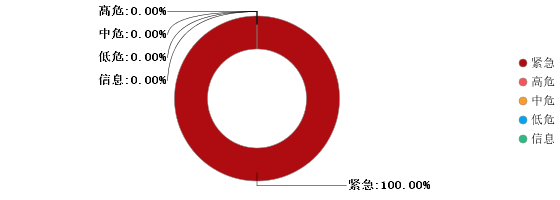
# 风险分布

## 主机风险分布

风险等级列表：

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

风险等级占比分布：

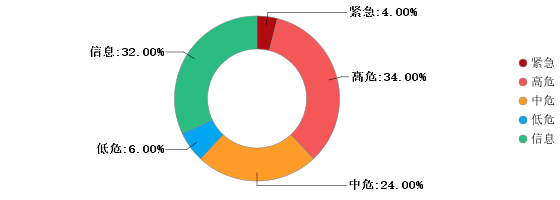


## 漏洞风险分布

漏洞风险等级列表：

|  |  |  |
| --- | --- | --- |
| **风险等级** | **漏洞出现次数** | **百分比** |
| 紧急 | 2 | 4.00% |
| 高危 | 17 | 34.00% |
| 中危 | 12 | 24.00% |
| 低危 | 3 | 6.00% |
| 信息 | 16 | 32.00% |
| 漏洞数量总计 | 50 |  |

漏洞风险等级占比分布：

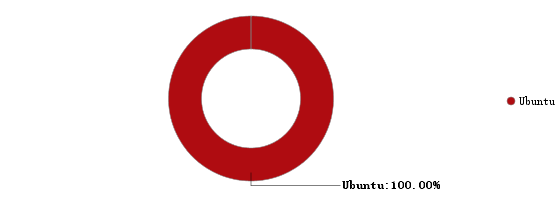


## 操作系统分布

操作系统情况列表：

|  |  |  |
| --- | --- | --- |
| **操作系统** | **主机数量** | **百分比** |
| Ubuntu | 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** |
| 111.231.21.41 | 0b842aa5.phpmyadmin | Ubuntu 20.04 | 2 | 17 | 12 | 3 | 16 |

# 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 | GeneratedISC BIND 缓冲区错误漏洞(CVE-2021-25216) | 1/1 | 100.00% | 1 |
| 2 | GeneratedOpenSSH 安全漏洞(CVE-2023-38408) | 1/1 | 100.00% | 1 |
| 3 | GeneratedOpenSSH 资源管理错误漏洞(CVE-2021-28041) | 1/1 | 100.00% | 1 |
| 4 | GeneratedOpenSSH权限提升漏洞(CVE-2021-41617) | 1/1 | 100.00% | 1 |
| 5 | GeneratedISC BIND 安全漏洞(CVE-2023-2828) | 1/1 | 100.00% | 1 |
| 6 | GeneratedISC BIND 资源管理错误漏洞(CVE-2020-8616) | 1/1 | 100.00% | 1 |
| 7 | GeneratedInternet Systems Consortium BIND server 安全漏洞(CVE-2020-8620) | 1/1 | 100.00% | 1 |
| 8 | GeneratedISC BIND拒绝服务漏洞(CVE-2020-8621) | 1/1 | 100.00% | 1 |
| 9 | GeneratedISC BIND拒绝服务漏洞(CVE-2020-8623) | 1/1 | 100.00% | 1 |
| 10 | GeneratedBind Server 安全漏洞(CVE-2020-8625) | 1/1 | 100.00% | 1 |
| 11 | GeneratedISC BIND 数据伪造问题漏洞(CVE-2022-38177) | 1/1 | 100.00% | 1 |
| 12 | GeneratedISC BIND 数据伪造问题漏洞(CVE-2022-38178) | 1/1 | 100.00% | 1 |
| 13 | GeneratedISC BIND 安全漏洞(CVE-2023-3341) | 1/1 | 100.00% | 1 |
| 14 | GeneratedISC BIND 多个 DoS 漏洞(CVE-2023-50868) | 1/1 | 100.00% | 1 |
| 15 | GeneratedISC BIND DoS漏洞(CVE-2023-4408) | 1/1 | 100.00% | 1 |
| 16 | GeneratedISC BIND DoS漏洞(CVE-2023-5517) | 1/1 | 100.00% | 1 |
| 17 | GeneratedISC BIND 多个 DoS 漏洞(CVE-2023-50387) | 1/1 | 100.00% | 1 |
| 18 | GeneratedISC BIND DoS漏洞(CVE-2023-6516) | 1/1 | 100.00% | 1 |
| 19 | GeneratedOpenSSH 安全漏洞(CVE-2023-51767) | 1/1 | 100.00% | 1 |
| 20 | GeneratedOpenSSH 信息泄露漏洞(CVE-2020-14145) | 1/1 | 100.00% | 1 |
| 21 | GeneratedOpenSSH 质询漏洞(CVE-2016-20012) | 1/1 | 100.00% | 1 |
| 22 | GeneratedISC BIND 安全漏洞(CVE-2020-8617) | 1/1 | 100.00% | 1 |
| 23 | Generatedisc bind 安全漏洞（CVE-2020-8622） | 1/1 | 100.00% | 1 |
| 24 | GeneratedISC BIND update-policy漏洞(CVE-2020-8624) | 1/1 | 100.00% | 1 |
| 25 | GeneratedISC BIND 安全漏洞(CVE-2021-25214) | 1/1 | 100.00% | 1 |
| 26 | GeneratedISC BIND 资源管理错误漏洞(CVE-2021-25219) | 1/1 | 100.00% | 1 |
| 27 | GeneratedISC BIND 代码问题漏洞(CVE-2021-25220) | 1/1 | 100.00% | 1 |
| 28 | GeneratedISC BIND 资源管理错误漏洞(CVE-2022-2795) | 1/1 | 100.00% | 1 |
| 29 | GeneratedOpenSSH 安全漏洞(CVE-2023-51385) | 1/1 | 100.00% | 1 |
| 30 | GeneratedOpenSSH 安全漏洞(CVE-2023-48795) | 1/1 | 100.00% | 1 |
| 31 | GeneratedOpenSSH 安全漏洞(CVE-2023-51384) | 1/1 | 100.00% | 1 |
| 32 | GeneratedOpenSSH 操作系统命令注入漏洞(CVE-2020-15778) | 1/1 | 100.00% | 1 |
| 33 | GeneratedOpenSSH 授权问题漏洞(CVE-2021-36368) | 1/1 | 100.00% | 1 |
| 34 | GeneratedICMP时间戳检测(原理扫描) | 1/1 | 100.00% | 1 |
| 35 | 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 |
| 36 | Generated服务器支持的SSL加密协议(原理扫描) | 1/1 | 100.00% | 1 |
| 37 | Generated允许Traceroute探测 | 1/1 | 100.00% | 1 |
| 38 | GeneratedHTTP Server类型和版本号 | 1/1 | 100.00% | 4 |
| 39 | GeneratedApache Web服务器版本检测 | 1/1 | 100.00% | 3 |
| 40 | Generated通过RPC获取所有端口映射器注册程序的列表(原理扫描) | 1/1 | 100.00% | 1 |
| 41 | Generated检测到RPCBIND/PORTMAP 端口映射表 (TCP)正在运行(CVE-1999-0632)(原理扫描) | 1/1 | 100.00% | 1 |
| 42 | GeneratedSSH版本信息可被获取(原理扫描) | 1/1 | 100.00% | 1 |
| 43 | GeneratedMySQL/MariaDB检测 | 1/1 | 100.00% | 1 |
| 44 | Generated检测到DNS服务正在运行 | 1/1 | 100.00% | 1 |
| 45 | GeneratedSSH协议支持的算法(原理扫描) | 1/1 | 100.00% | 1 |

## 漏洞详情

### 紧急

|  |  |
| --- | --- |
| **漏洞名称** | ISC BIND 缓冲区错误漏洞(CVE-2021-25216) |
| **影响主机** | 111.231.21.41:53 |
| **漏洞类型** | DNS |
| **CVSS评分** | 9.8 |
| **CVE编号** | CVE-2021-25216 |
| **CNNVD编号** | CNNVD-202104-2110 |
| **CNCVE编号** | CNCVE-202125216 |
| **漏洞描述** | ISC BIND是美国ISC公司的一套实现了DNS协议的开源软件。  BIND 存在缓冲区错误漏洞，该漏洞源于BIND的GSSAPI安全策略。 |
| **修复建议** | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：  https://kb.isc.org/v1/docs/cve-2021-25216 |

|  |  |
| --- | --- |
| **漏洞名称** | OpenSSH 安全漏洞(CVE-2023-38408) |
| **影响主机** | 111.231.21.41:22 |
| **漏洞类型** | SSH |
| **CVSS评分** | 9.8 |
| **CVE编号** | CVE-2023-38408 |
| **CNNVD编号** | CNNVD-202307-1721 |
| **CNCVE编号** | CNCVE-202338408 |
| **漏洞描述** | OpenSSH（OpenBSD Secure Shell）是加拿大OpenBSD计划组的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。  OpenSSH 9.3p2之前版本存在安全漏洞，该漏洞源于ssh-agent的PKCS11功能存在安全问题。攻击者可利用该漏洞执行远程代码。 |
| **修复建议** | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：  https://github.com/openbsd/src/commit/7bc29a9d5cd697290aa056e94ecee6253d3425f8 |

### 高危

|  |  |
| --- | --- |
| **漏洞名称** | OpenSSH 资源管理错误漏洞(CVE-2021-28041) |
| **影响主机** | 111.231.21.41:22 |
| **漏洞类型** | SSH |
| **CVSS评分** | 7.1 |
| **CVE编号** | CVE-2021-28041 |
| **CNNVD编号** | CNNVD-202103-527 |
| **CNCVE编号** | CNCVE-202128041 |
| **漏洞描述** | OpenSSH（OpenBSD Secure Shell）是Openbsd计划组的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。  OpenSSH before 8.5 存在安全漏洞，攻击者可利用该漏洞在遗留操作系统上不受约束的代理套接字访问。 |
| **修复建议** | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://github.com/openssh/openssh-portable/commit/e04fd6dde16de1cdc5a4d9946397ff60d96568db |

|  |  |
| --- | --- |
| **漏洞名称** | OpenSSH权限提升漏洞(CVE-2021-41617) |
| **影响主机** | 111.231.21.41:22 |
| **漏洞类型** | SSH |
| **CVSS评分** | 7.0 |
| **CVE编号** | CVE-2021-41617 |
| **CNNVD编号** | CNNVD-202109-1695 |
| **CNCVE编号** | CNCVE-202141617 |
| **漏洞描述** | OpenSSH（OpenBSD Secure Shell）是Openbsd计划组的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。  OpenSSH存在安全漏洞。该漏洞源于允许权限提升，因为补充组未按预期初始化。 |
| **修复建议** | 升级到 OpenSSH 版本 8.8 或更高版本，链接：https://www.openssh.com/txt/release-8.8 |

|  |  |
| --- | --- |
| **漏洞名称** | ISC BIND 安全漏洞(CVE-2023-2828) |
| **影响主机** | 111.231.21.41:53 |
| **漏洞类型** | DNS |
| **CVSS评分** | 7.5 |
| **CVE编号** | CVE-2023-2828 |
| **CNNVD编号** | CNNVD-202306-1536 |
| **CNCVE编号** | CNCVE-20232828 |
| **漏洞描述** | ISC BIND是美国ISC公司的一套实现了DNS协议的开源软件。  ISC BIND 9存在安全漏洞，该漏洞源于缓存配置限制不当，攻击者利用该漏洞可以导致拒绝服务条件。 |
| **修复建议** | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：  https://kb.isc.org/docs/cve-2023-2828 |

|  |  |
| --- | --- |
| **漏洞名称** | ISC BIND 资源管理错误漏洞(CVE-2020-8616) |
| **影响主机** | 111.231.21.41:53 |
| **漏洞类型** | DNS |
| **CVSS评分** | 8.6 |
| **CVE编号** | CVE-2020-8616 |
| **CNNVD编号** | CNNVD-202005-917 |
| **CNVD编号** | CNVD-2020-34454 |
| **CNCVE编号** | CNCVE-20208616 |
| **漏洞描述** | ISC BIND是美国ISC公司的一套实现了DNS协议的开源软件。  ISC BIND中存在安全漏洞。远程攻击者可利用该漏洞造成拒绝服务。以下产品及版本受到影响：BIND 9.0.0版本至 9.11.18版本，9.12.0版本至 9.12.4-P2版本，9.14.0版本至 9.14.11版本，9.16.0版本至 9.16.2版本，9.17.0版本至9.17.1版本，9.13版本，9.15版本，BIND Supported Preview Edition 9.9.3-S1版本至9.11.18-S1版本。 |
| **修复建议** | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：  https://kb.isc.org/docs/cve-2020-8616 |

|  |  |
| --- | --- |
| **漏洞名称** | Internet Systems Consortium BIND server 安全漏洞(CVE-2020-8620) |
| **影响主机** | 111.231.21.41:53 |
| **漏洞类型** | DNS |
| **CVSS评分** | 7.5 |
| **CVE编号** | CVE-2020-8620 |
| **CNNVD编号** | CNNVD-202008-1022 |
| **CNCVE编号** | CNCVE-20208620 |
| **漏洞描述** | TCP（Transmission Control Protocol,传输控制协议）是一种面向连接的、可靠的、基于字节流的传输层通信协议，由IETF的RFC 793定义。  Internet Systems Consortium BIND server 9.15.6版本至9.16.5版本，9.17.0版本至 9.17.3版本中存在安全漏洞，该漏洞源于在通过libuv流量处理TCP流量时，如果对该服务器的TCP端口（用于处理较大的DNS请求（AXFR））发送大量数据包，程序会将长度值传入到服务器，造成断言失败。攻击者可通过向该端口发送大量未认证的数据包利用该漏洞造成拒绝服务。 |
| **修复建议** | 目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：  https://www.isc.org/bind/ |

|  |  |
| --- | --- |
| **漏洞名称** | ISC BIND拒绝服务漏洞(CVE-2020-8621) |
| **影响主机** | 111.231.21.41:53 |
| **漏洞类型** | DNS |
| **CVSS评分** | 7.5 |
| **CVE编号** | CVE-2020-8621 |
| **CNNVD编号** | CNNVD-202008-1078 |
| **CNCVE编号** | CNCVE-20208621 |
| **漏洞描述** | BIND 9.14.0至9.16.5, 9.17.0至9.17.3存在安全漏洞，攻击者可以构造一个特殊请求造成目标服务异常结束。 |
| **修复建议** | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：  https://kb.isc.org/docs/cve-2020-8621 |

|  |  |
| --- | --- |
| **漏洞名称** | ISC BIND拒绝服务漏洞(CVE-2020-8623) |
| **影响主机** | 111.231.21.41:53 |
| **漏洞类型** | DNS |
| **CVSS评分** | 7.5 |
| **CVE编号** | CVE-2020-8623 |
| **CNNVD编号** | CNNVD-202008-1070 |
| **CNCVE编号** | CNCVE-20208623 |
| **漏洞描述** | BIND 9.10.0至9.11.21, 9.12.0至9.16.5, 9.17.0至9.17.3，9.10.5-S1至9.11.21-S1存在安全漏洞，攻击者可以构造一个特殊的查询数据包触发异常。 |
| **修复建议** | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：  https://kb.isc.org/docs/cve-2020-8623 |

|  |  |
| --- | --- |
| **漏洞名称** | Bind Server 安全漏洞(CVE-2020-8625) |
| **影响主机** | 111.231.21.41:53 |
| **漏洞类型** | DNS |
| **CVSS评分** | 8.1 |
| **CVE编号** | CVE-2020-8625 |
| **CNNVD编号** | CNNVD-202102-1310 |
| **CNCVE编号** | CNCVE-20208625 |
| **漏洞描述** | Bind Server是一款DNS（域名系统）协议的完整实现。  BIND 存在安全漏洞，该漏洞源于通过显式地为tkey-gssapi-keytab或tkey-gssapi-credentialconfiguration选项设置有效值，服务器可能会变得脆弱。 |
| **修复建议** | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：  https://kb.isc.org/v1/docs/cve-2020-8625 |

|  |  |
| --- | --- |
| **漏洞名称** | ISC BIND 数据伪造问题漏洞(CVE-2022-38177) |
| **影响主机** | 111.231.21.41:53 |
| **漏洞类型** | Other |
| **CVSS评分** | 7.5 |
| **CVE编号** | CVE-2022-38177 |
| **CNNVD编号** | CNNVD-202209-1662 |
| **CNCVE编号** | CNCVE-202238177 |
| **漏洞描述** | ISC BIND是美国ISC公司的一套实现了DNS协议的开源软件。  ISC BIND 9.8.4版本至9.16.32版本存在安全漏洞，该漏洞源于使用格式错误的ECDSA签名，欺骗目标解析程序，导致内存因资源不足而崩溃。 |
| **修复建议** | 目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：  https://www.isc.org/bind/ |

|  |  |
| --- | --- |
| **漏洞名称** | ISC BIND 数据伪造问题漏洞(CVE-2022-38178) |
| **影响主机** | 111.231.21.41:53 |
| **漏洞类型** | DNS |
| **CVSS评分** | 7.5 |
| **CVE编号** | CVE-2022-38178 |
| **CNNVD编号** | CNNVD-202209-1661 |
| **CNCVE编号** | CNCVE-202238178 |
| **漏洞描述** | ISC BIND是美国ISC公司的一套实现了DNS协议的开源软件。  BIND存在安全漏洞，该漏洞源于使用格式错误的EdDSA签名，欺骗目标解析程序，导致内存因资源不足而崩溃。以下产品及版本受到影响：9.9.12版本至9.9.13版本、9.10.7版本至9.10.8版本、9.11.3版本至9.16.32版本、9.18.0版本至 9.18.6版本、9.19.0版本至9.19.4版本。 |
| **修复建议** | 目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：  https://www.isc.org/bind/ |

|  |  |
| --- | --- |
| **漏洞名称** | ISC BIND 安全漏洞(CVE-2023-3341) |
| **影响主机** | 111.231.21.41:53 |
| **漏洞类型** | DNS |
| **CVSS评分** | 7.5 |
| **CVE编号** | CVE-2023-3341 |
| **CNNVD编号** | CNNVD-202309-1944 |
| **CNCVE编号** | CNCVE-20233341 |
| **漏洞描述** | ISC BIND是美国ISC公司的一套实现了DNS协议的开源软件。 ISC BIND 9 9.2.0 到 9.16.43、9.18.0 到 9.18.18、9.19.0 到 9.19.16、9.9.3-S1 到 9.16.43-S1 以及 9.18.0-S1 到 9.18 .18-S1版本存在安全漏洞，该漏洞源于处理发送到named的控制通道消息的代码在数据包解析期间递归地调用某些函数，但递归深度仅受最大接受数据包大小的限制，这可能导致数据包解析代码耗尽可用的堆栈内存，导致named意外终止。 |
| **修复建议** | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://kb.isc.org/docs/cve-2023-3341 |

|  |  |
| --- | --- |
| **漏洞名称** | ISC BIND 多个 DoS 漏洞(CVE-2023-50868) |
| **影响主机** | 111.231.21.41:53 |
| **漏洞类型** | Other |
| **CVSS评分** | 7.8 |
| **CVE编号** | CVE-2023-50868 |
| **CNNVD编号** | CNNVD-202402-1126 |
| **CNCVE编号** | CNCVE-202350868 |
| **漏洞描述** | ISC BIND 容易出现多个拒绝服务 (DoS) 漏洞。 |
| **修复建议** | 更新到版本 9.16.48、9.18.24、9.19.21、9.16.48-S1、9.18.24-S1 或更高版本。 |

|  |  |
| --- | --- |
| **漏洞名称** | ISC BIND DoS漏洞(CVE-2023-4408) |
| **影响主机** | 111.231.21.41:53 |
| **漏洞类型** | Other |
| **CVSS评分** | 7.5 |
| **CVE编号** | CVE-2023-4408 |
| **CNCVE编号** | CNCVE-20234408 |
| **漏洞描述** | ISC BIND容易产生拒绝服务(DoS)漏洞。 |
| **修复建议** | 更新到版本9.16.48、9.18.24、9.19.21、9.16.48- s1、9.18.24- s1或更高版本。 |

|  |  |
| --- | --- |
| **漏洞名称** | ISC BIND DoS漏洞(CVE-2023-5517) |
| **影响主机** | 111.231.21.41:53 |
| **漏洞类型** | Other |
| **CVSS评分** | 7.5 |
| **CVE编号** | CVE-2023-5517 |
| **CNCVE编号** | CNCVE-20235517 |
| **漏洞描述** | ISC BIND容易产生拒绝服务(DoS)漏洞。 |
| **修复建议** | 更新到版本9.16.48、9.18.24、9.19.21、9.16.48- s1、9.18.24- s1或更高版本。 |

|  |  |
| --- | --- |
| **漏洞名称** | ISC BIND 多个 DoS 漏洞(CVE-2023-50387) |
| **影响主机** | 111.231.21.41:53 |
| **漏洞类型** | Other |
| **CVSS评分** | 7.5 |
| **CVE编号** | CVE-2023-50387 |
| **CNNVD编号** | CNNVD-202402-1127 |
| **CNCVE编号** | CNCVE-202350387 |
| **漏洞描述** | ISC BIND 容易出现多个拒绝服务 (DoS) 漏洞。 |
| **修复建议** | 更新到版本 9.16.48、9.18.24、9.19.21、9.16.48-S1、9.18.24-S1 或更高版本。 |

|  |  |
| --- | --- |
| **漏洞名称** | ISC BIND DoS漏洞(CVE-2023-6516) |
| **影响主机** | 111.231.21.41:53 |
| **漏洞类型** | Other |
| **CVSS评分** | 7.5 |
| **CVE编号** | CVE-2023-6516 |
| **CNCVE编号** | CNCVE-20236516 |
| **漏洞描述** | ISC BIND容易产生拒绝服务(DoS)漏洞。 |
| **修复建议** | 更新到版本9.16.48, 9.16.48-S1或更高版本。 |

|  |  |
| --- | --- |
| **漏洞名称** | OpenSSH 安全漏洞(CVE-2023-51767) |
| **影响主机** | 111.231.21.41:22 |
| **漏洞类型** | Other |
| **CVSS评分** | 7.0 |
| **CVE编号** | CVE-2023-51767 |
| **CNNVD编号** | CNNVD-202312-2216 |
| **CNCVE编号** | CNCVE-202351767 |
| **漏洞描述** | OpenSSH（OpenBSD Secure Shell）是加拿大OpenBSD计划组的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。 OpenSSH 9.6及之前版本存在安全漏洞，该漏洞源于当使用常见类型的DRAM时，mm\_answer\_authpassword中已验证的整数值不能抵抗单个比特的翻转，导致攻击者可以绕过身份验证。 |
| **修复建议** | 目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法 |

### 中危

|  |  |
| --- | --- |
| **漏洞名称** | OpenSSH 信息泄露漏洞(CVE-2020-14145) |
| **影响主机** | 111.231.21.41:22 |
| **漏洞类型** | SSH |
| **CVSS评分** | 5.9 |
| **CVE编号** | CVE-2020-14145 |
| **CNNVD编号** | CNNVD-202006-1822 |
| **CNVD编号** | CNVD-2021-25272 |
| **CNCVE编号** | CNCVE-202014145 |
| **漏洞描述** | OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。  OpenSSH 5.7版本至8.3版本的客户端中存在安全漏洞。攻击者可利用该漏洞获取信息。 |
| **修复建议** | 目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法：  https://www.openssh.com/ |

|  |  |
| --- | --- |
| **漏洞名称** | OpenSSH 质询漏洞(CVE-2016-20012) |
| **影响主机** | 111.231.21.41:22 |
| **漏洞类型** | SSH |
| **CVSS评分** | 5.3 |
| **CVE编号** | CVE-2016-20012 |
| **CNNVD编号** | CNNVD-202109-1073 |
| **CNCVE编号** | CNCVE-201620012 |
| **漏洞描述** | OpenSSH（OpenBSD Secure Shell）是Openbsd计划组的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。  OpenSSH 之前版本存在安全漏洞，允许远程攻击者怀疑 SSH 服务器知道用户名和公钥的特定组合，以测试这种怀疑是否正确。 发生这种情况是因为仅当该组合对登录会话有效时才会发送质询,目前openssh开发人员认为这是一个重要的安全功能，不打算进行修复此漏洞。 |
| **修复建议** | 目前openssh开发人员认为这是一个重要的安全功能，不打算进行修复此漏洞，回复链接：https://github.com/openssh/openssh-portable/pull/270 |

|  |  |
| --- | --- |
| **漏洞名称** | ISC BIND 安全漏洞(CVE-2020-8617) |
| **影响主机** | 111.231.21.41:53 |
| **漏洞类型** | DNS |
| **CVSS评分** | 5.9 |
| **CVE编号** | CVE-2020-8617 |
| **CNNVD编号** | CNNVD-202005-916 |
| **CNVD编号** | CNVD-2020-29429 |
| **CNCVE编号** | CNCVE-20208617 |
| **漏洞描述** | ISC BIND是美国ISC公司的一套实现了DNS协议的开源软件。  ISC BIND中存在安全漏洞。远程攻击者可利用该漏洞导致拒绝服务。以下产品及版本受到影响：BIND 9.0.0版本至9.11.18版本，9.12.0版本至9.12.4-P2版本，9.14.0版本至9.14.11版本，9.16.0版本至9.16.2版本，9.17.0版本至9.17.1版本，9.13版本，9.15版本，BIND Supported Preview Edition from 9.9.3-S1版本至9.11.18-S1版本。 |
| **修复建议** | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：  https://kb.isc.org/docs/cve-2020-8617 |

|  |  |
| --- | --- |
| **漏洞名称** | isc bind 安全漏洞（CVE-2020-8622） |
| **影响主机** | 111.231.21.41:53 |
| **漏洞类型** | DNS |
| **CVSS评分** | 6.5 |
| **CVE编号** | CVE-2020-8622 |
| **CNNVD编号** | CNNVD-202008-1071 |
| **CNCVE编号** | CNCVE-20208622 |
| **漏洞描述** | 因isc bind导入、使用或以其他方式与该CVE主体存在关联，因此受到影响，runc是一款用于根据OCI规范生成和运行容器的CLI（命令行界面）工具。  BIND 9.0.0至9.11.21, 9.12.0至9.16.5, 9.17.0至9.17.3,9.9.3-S1至9.11.21-S1存在安全漏洞，攻击者可以构造一个特殊请求引发断言失败造成目标服务异常结束。 |
| **修复建议** | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：  https://kb.isc.org/docs/cve-2020-8622 |

|  |  |
| --- | --- |
| **漏洞名称** | ISC BIND update-policy漏洞(CVE-2020-8624) |
| **影响主机** | 111.231.21.41:53 |
| **漏洞类型** | DNS |
| **CVSS评分** | 4.3 |
| **CVE编号** | CVE-2020-8624 |
| **CNNVD编号** | CNNVD-202008-1069 |
| **CNCVE编号** | CNCVE-20208624 |
| **漏洞描述** | BIND 9.9.12 至9.9.13, 9.10.7至9.10.8, 9.11.3至9.11.21, 9.12.1至9.16.5, 9.17.0 至9.17.3， 9.9.12-S1至9.9.13-S1, 9.11.3-S1至9.11.21-S1存在安全漏洞，攻击者可以恶意使用新增权限更新其他区域内容。 |
| **修复建议** | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：  https://kb.isc.org/docs/cve-2020-8624 |

|  |  |
| --- | --- |
| **漏洞名称** | ISC BIND 安全漏洞(CVE-2021-25214) |
| **影响主机** | 111.231.21.41:53 |
| **漏洞类型** | DNS |
| **CVSS评分** | 6.5 |
| **CVE编号** | CVE-2021-25214 |
| **CNNVD编号** | CNNVD-202104-2108 |
| **CNCVE编号** | CNCVE-202125214 |
| **漏洞描述** | ISC BIND是美国ISC公司的一套实现了DNS协议的开源软件。  ISC BIND 存在安全漏洞，该漏洞导致接收已命名服务器无意中从区域数据库中删除有问题的区域的SOA记录。 |
| **修复建议** | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：  https://kb.isc.org/v1/docs/cve-2021-25214 |

|  |  |
| --- | --- |
| **漏洞名称** | ISC BIND 资源管理错误漏洞(CVE-2021-25219) |
| **影响主机** | 111.231.21.41:53 |
| **漏洞类型** | DNS |
| **CVSS评分** | 5.3 |
| **CVE编号** | CVE-2021-25219 |
| **CNNVD编号** | CNNVD-202110-2018 |
| **CNCVE编号** | CNCVE-202125219 |
| **漏洞描述** | ISC BIND是美国ISC公司的一套实现了DNS协议的开源软件。  BIND 中存在资源管理错误漏洞，该漏洞源于产品的授权服务器的相应处理存在错误。攻击者可通过该漏洞导致BIND解析器性能下降进而导致查询处理延迟。 |
| **修复建议** | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：  https://www.isc.org/bind/ |

|  |  |
| --- | --- |
| **漏洞名称** | ISC BIND 代码问题漏洞(CVE-2021-25220) |
| **影响主机** | 111.231.21.41:53 |
| **漏洞类型** | DNS |
| **CVSS评分** | 6.8 |
| **CVE编号** | CVE-2021-25220 |
| **CNNVD编号** | CNNVD-202203-1514 |
| **CNVD编号** | CNVD-2022-62999 |
| **CNCVE编号** | CNCVE-202125220 |
| **漏洞描述** | ISC BIND是美国ISC公司的一套实现了DNS协议的开源软件。  ISC BIND 存在安全漏洞，该漏洞源于已经收紧了接受记录到缓存中的规则，以防止如果转发器在配置的范围之外发送记录可能会中毒。 |
| **修复建议** | 目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法：  https://vigilance.fr/vulnerability/ISC-BIND-spoofing-via-DNS-Forwarders-Cache-Poisoning-37754 |

|  |  |
| --- | --- |
| **漏洞名称** | ISC BIND 资源管理错误漏洞(CVE-2022-2795) |
| **影响主机** | 111.231.21.41:53 |
| **漏洞类型** | DNS |
| **CVSS评分** | 5.3 |
| **CVE编号** | CVE-2022-2795 |
| **CNNVD编号** | CNNVD-202209-1695 |
| **CNVD编号** | CNVD-2022-55071 |
| **CNCVE编号** | CNCVE-20222795 |
| **漏洞描述** | ISC BIND是美国ISC公司的一套实现了DNS协议的开源软件。  ISC BIND 9.16.33之前版本、9.18.7之前的9.18.x版本、9.19.5之前的9.19.x版本存在安全漏洞，该漏洞源于解析器代码中的缺陷可能会导致命名在处理大型委托上花费过多的时间,攻击者通过利用此漏洞向目标解析器充斥查询，可以显着削弱解析器的性能，从而有效地拒绝合法客户端访问DNS解析服务。 |
| **修复建议** | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：  https://kb.isc.org/docs/cve-2022-2795 |

|  |  |
| --- | --- |
| **漏洞名称** | OpenSSH 安全漏洞(CVE-2023-51385) |
| **影响主机** | 111.231.21.41:22 |
| **漏洞类型** | SSH |
| **CVSS评分** | 6.5 |
| **CVE编号** | CVE-2023-51385 |
| **CNNVD编号** | CNNVD-202312-1665 |
| **CNCVE编号** | CNCVE-202351385 |
| **漏洞描述** | OpenSSH（OpenBSD Secure Shell）是加拿大OpenBSD计划组的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。 OpenSSH 9.6之前版本存在安全漏洞，该漏洞源于存在操作系统命令注入漏洞。 |
| **修复建议** | 目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：https://www.openssh.com/txt/release-9.6 |

|  |  |
| --- | --- |
| **漏洞名称** | OpenSSH 安全漏洞(CVE-2023-48795) |
| **影响主机** | 111.231.21.41:22 |
| **漏洞类型** | SSH |
| **CVSS评分** | 5.9 |
| **CVE编号** | CVE-2023-48795 |
| **CNNVD编号** | CNNVD-202312-1668 |
| **CNCVE编号** | CNCVE-202348795 |
| **漏洞描述** | OpenSSH（OpenBSD Secure Shell）是加拿大OpenBSD计划组的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。 OpenSSH 9.6之前版本存在安全漏洞，该漏洞源于允许远程攻击者绕过完整性检查，从而省略某些数据包。 |
| **修复建议** | 目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：https://www.openssh.com/openbsd.html |

|  |  |
| --- | --- |
| **漏洞名称** | OpenSSH 安全漏洞(CVE-2023-51384) |
| **影响主机** | 111.231.21.41:22 |
| **漏洞类型** | SSH |
| **CVSS评分** | 5.5 |
| **CVE编号** | CVE-2023-51384 |
| **CNNVD编号** | CNNVD-202312-1662 |
| **CNCVE编号** | CNCVE-202351384 |
| **漏洞描述** | OpenSSH（OpenBSD Secure Shell）是加拿大OpenBSD计划组的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。 OpenSSH 9.6之前版本存在安全漏洞，该漏洞源于当在添加PKCS11托管私钥的过程中指定目标约束时，这些约束仅应用于第一个密钥。 |
| **修复建议** | 目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：https://www.openssh.com/txt/release-9.6 |

### 低危

|  |  |
| --- | --- |
| **漏洞名称** | OpenSSH 操作系统命令注入漏洞(CVE-2020-15778) |
| **影响主机** | 111.231.21.41:22 |
| **漏洞类型** | SSH |
| **CVSS评分** | 3.5 |
| **CVE编号** | CVE-2020-15778 |
| **CNNVD编号** | CNNVD-202007-1519 |
| **CNVD编号** | CNVD-2020-42668 |
| **CNCVE编号** | CNCVE-202015778 |
| **漏洞描述** | OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。  该漏洞源于外部输入数据构造操作系统可执行命令过程中，网络系统或产品未正确过滤其中的特殊字符、命令等。攻击者可利用该漏洞执行非法操作系统命令。目前openssh社区的答复是不修复该漏洞，因为scp为了传输文件而设计使用，应支持传输linux系统上符合文件名要求的文件，如果加入对特殊字符的校验，会使scp传输文件的范围变小，不符合简单使用的设计初衷。 |
| **修复建议** | 目前厂商暂未发布修复措施解决此安全问题. 临时缓解措施：建议保管好ssh密码，设置较为复杂的密码；或者可以禁用scp(命令:mv /usr/bin/scp /usr/bin/scp.bak )改用rsync等缓解风险，但漏洞依然存在漏扫还会上报提醒，其他信息可参考官方链接：https://www.openssh.com/ |

|  |  |
| --- | --- |
| **漏洞名称** | OpenSSH 授权问题漏洞(CVE-2021-36368) |
| **影响主机** | 111.231.21.41:22 |
| **漏洞类型** | SSH |
| **CVSS评分** | 3.7 |
| **CVE编号** | CVE-2021-36368 |
| **CNNVD编号** | CNNVD-202203-1230 |
| **CNCVE编号** | CNCVE-202136368 |
| **漏洞描述** | OpenSSH（OpenBSD Secure Shell）是Openbsd计划组的一套用于安全访问远程计算机的连接工具。该工具是SSH协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。  OpenSSH 8.9 之前的版本中存在安全漏洞。该漏洞源于客户端使用带代理转发但没有 -oLogLevel=verbose 的公钥身份验证。 |
| **修复建议** | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：  https://www.openssh.com/security.html |

|  |  |
| --- | --- |
| **漏洞名称** | ICMP时间戳检测(原理扫描) |
| **影响主机** | 111.231.21.41:0 |
| **漏洞类型** | Other |
| **CVSS评分** | 2.1 |
| **CVE编号** | CVE-1999-0524 |
| **CNNVD编号** | CNNVD-199708-003 |
| **CNCVE编号** | CNCVE-19990524 |
| **漏洞描述** | 远程主机响应ICMP时间戳请求。 时间戳回复是回复时间戳消息的ICMP消息。 它由时间戳的发送者发送的始发时间戳以及接收时间戳和发送时间戳组成。 这个信息理论上可以用来开发其他服务中基于时间的弱随机数发生器。 |
| **修复建议** | 过滤外来的ICMP timestamp（类型 13）报文以及外出的ICMP timestamp回复报文 |

### 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** | 111.231.21.41:443 |
| **漏洞类型** | Other |
| **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** | 111.231.21.41:443 |
| **漏洞类型** | Other |
| **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** | 允许Traceroute探测 |
| **影响主机** | 111.231.21.41:0 |
| **漏洞类型** | Other |
| **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** | 111.231.21.41:8888,111.231.21.41:443,111.231.21.41:80,111.231.21.41:888 |
| **漏洞类型** | Web Servers |
| **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** | Apache Web服务器版本检测 |
| **影响主机** | 111.231.21.41:443,111.231.21.41:80,111.231.21.41:888 |
| **漏洞类型** | Web Servers |
| **CVSS评分** | 0.0 |
| **漏洞描述** | 检测Apache Web Server的安装版本脚本检测远程主机上的Apache HTTP Server的版本并设置KB。 |
| **修复建议** | 探测Apache服务器信息，无需修改 |

|  |  |
| --- | --- |
| **漏洞名称** | 通过RPC获取所有端口映射器注册程序的列表(原理扫描) |
| **影响主机** | 111.231.21.41:111 |
| **漏洞类型** | Network Control |
| **CVSS评分** | 0.0 |
| **漏洞描述** | 此脚本调用端口映射器上的DUMP RPC，以获取所有注册程序的列表 |
| **修复建议** | 通过防火墙屏蔽对外的端口 |

|  |  |
| --- | --- |
| **漏洞名称** | 检测到RPCBIND/PORTMAP 端口映射表 (TCP)正在运行(CVE-1999-0632)(原理扫描) |
| **影响主机** | 111.231.21.41:111 |
| **漏洞类型** | Other |
| **CVSS评分** | 0.0 |
| **CVE编号** | CVE-1999-0632 |
| **漏洞描述** | RPC portmapper 服务正在运行。历史上存在许多与该服务相关的远程安全漏洞。虽然此次扫描不能确认目标系统确实存在安全漏洞，但将此类服务直接暴露在不可信任的网络环境中，存在潜在危险。 |
| **修复建议** | 在您的防火墙上禁止对内部网络的111(UDP/TCP)端口的访问，以限制未授权的RPC查询请求；如果不需要RPC服务，关闭portmap。 |

|  |  |
| --- | --- |
| **漏洞名称** | SSH版本信息可被获取(原理扫描) |
| **影响主机** | 111.231.21.41:22 |
| **漏洞类型** | SSH |
| **CVSS评分** | 0.0 |
| **漏洞描述** | ssh版本类型和版本可以被远程获取到 |
| **修复建议** | 建议修改配置文件，隐藏ssh的banner信息 |

|  |  |
| --- | --- |
| **漏洞名称** | MySQL/MariaDB检测 |
| **影响主机** | 111.231.21.41:3306 |
| **漏洞类型** | Database |
| **CVSS评分** | 0.0 |
| **漏洞描述** | 检测已安装版本的MySQL/MariaDB。通过获取banner来检测正在运行的MySQL/MariaDB，从banner中提取版本并将信息存储在KB中。 |
| **修复建议** | 探测服务，无需修改 |

|  |  |
| --- | --- |
| **漏洞名称** | 检测到DNS服务正在运行 |
| **影响主机** | 111.231.21.41:53 |
| **漏洞类型** | Other |
| **CVSS评分** | 0.0 |
| **漏洞描述** | DNS服务器正在此主机上运行. |
| **修复建议** | 该策略为探测性策略，不具备危险性. |

|  |  |
| --- | --- |
| **漏洞名称** | SSH协议支持的算法(原理扫描) |
| **影响主机** | 111.231.21.41:22 |
| **漏洞类型** | SSH |
| **CVSS评分** | 0.0 |
| **漏洞描述** | 该脚本检测远程SSH服务支持的算法 |
| **修复建议** | 该漏洞仅做信息获取，可以不用修复 |

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。 |