**一、****资产概况**

|  |  |  |  |
| --- | --- | --- | --- |
| **IP地址** | 10.138.128.182 | **资产安全风险** | 高危 |
| **资产类型** | 主机设备 | **操作系统** | Linux |
| **MAC地址** | D0:B6:21:3A:09:D7 | **检测方式** | 安全检测任务 |
| **检测开始时间** | 2023/12/13 14:27 | **检测结束时间** | 2023/12/13 14:58 |

**二、****资产风险**

主机设备10.138.128.182在本次检测中共发现**高危**漏洞 12个， **中危**漏洞 10个， **低危**漏洞 4个。   
其中高危漏洞包括：主机漏洞 12个 ，占100.00%; 行业漏洞 0个 ;   
web漏洞 0个 ; 弱口令漏洞 0个 。   
该设备总体安全风险评级为“ **高危风险** ”。

中危漏洞  
10

主机漏洞  
数量: 26

**安全漏洞汇总表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **漏洞名称** | **漏洞类别** | **漏洞级别** | **CVE编号** |
| 1 | OpenSSH’ssh/kex.c’拒绝服务漏洞(CVE-2016-8858) | 主机漏洞 | **高危** | CVE-2016-8858 |
| 2 | OpenSSH sshd 安全漏洞(CVE-2016-6515) | 主机漏洞 | **高危** | CVE-2016-6515 |
| 3 | OpenSSH 安全漏洞(CVE-2016-1908) | 主机漏洞 | **高危** | CVE-2016-1908 |
| 4 | OpenSSH 安全漏洞(CVE-2016-10012) | 主机漏洞 | **高危** | CVE-2016-10012 |
| 5 | OpenSSH sshd 安全漏洞(CVE-2016-10010) | 主机漏洞 | **高危** | CVE-2016-10010 |
| 6 | OpenSSH 安全漏洞(CVE-2016-10009) | 主机漏洞 | **高危** | CVE-2016-10009 |
| 7 | OpenSSH 拒绝服务漏洞(CVE-2016-0778) | 主机漏洞 | **高危** | CVE-2016-0778 |
| 8 | OpenSSH sshd 安全漏洞(CVE-2015-8325) | 主机漏洞 | **高危** | CVE-2015-8325 |
| 9 | OpenSSH sshd 安全漏洞(CVE-2016-10708) | 主机漏洞 | **高危** | CVE-2016-10708 |
| 10 | OpenSSH 操作系统命令注入漏洞(CVE-2020-15778) | 主机漏洞 | **高危** | CVE-2020-15778 |
| 11 | OpenSSH 资源管理错误漏洞(CVE-2021-28041) | 主机漏洞 | **高危** | CVE-2021-28041 |
| 12 | OpenSSH安全漏洞(CVE-2021-41617) | 主机漏洞 | **高危** | CVE-2021-41617 |
| 13 | OpenSSH 安全漏洞(CVE-2017-15906) | 主机漏洞 | **中危** | CVE-2017-15906 |
| 14 | OpenSSH SSH守护进程安全漏洞(CVE-2016-6210) | 主机漏洞 | **中危** | CVE-2016-6210 |
| 15 | OpenSSH sshd CRLF注入漏洞(CVE-2016-3115) | 主机漏洞 | **中危** | CVE-2016-3115 |
| 16 | OpenSSH 拒绝服务漏洞(CVE-2016-1907) | 主机漏洞 | **中危** | CVE-2016-1907 |
| 17 | OpenSSH sshd 安全漏洞(CVE-2016-10011) | 主机漏洞 | **中危** | CVE-2016-10011 |
| 18 | OpenSSH 安全漏洞(CVE-2016-0777) | 主机漏洞 | **中危** | CVE-2016-0777 |
| 19 | OpenSSH 安全漏洞(CVE-2018-15473) | 主机漏洞 | **中危** | CVE-2018-15473 |
| 20 | OpenSSH 安全漏洞(CVE-2018-15919) | 主机漏洞 | **中危** | CVE-2018-15919 |
| 21 | OpenSSH 信息泄露漏洞(CVE-2020-14145) | 主机漏洞 | **中危** | CVE-2020-14145 |
| 22 | OpenSSH 安全漏洞(CVE-2016-20012) | 主机漏洞 | **中危** | CVE-2016-20012 |
| 23 | 探测到目的主机之间的路由信息 | 主机漏洞 | **低危** |  |
| 24 | ICMP请求远程时间泄漏漏洞(CVE-1999-0524) | 主机漏洞 | **低危** | CVE-1999-0524 |
| 25 | 服务器支持的SSH协议版本检查 | 主机漏洞 | **低危** |  |
| 26 | 服务器支持的TCP/IP时间戳 | 主机漏洞 | **低危** |  |

**三、****开放端口/服务**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **端口** | **协议** | **服务** | **版本** |
| 1 | 22 | tcp | ssh | SSH-2.0-OpenSSH\_7.1 |
| 2 | 80 | tcp | http | web server |
| 3 | 111 | tcp | rpcbind |  |
| 4 | 443 | tcp | https | HTTPS |

**四、****弱口令列表**

本次检测未发现弱口令。

**五、****风险详情**

**5.1.**                **模拟人工渗透详细风险描述及建议**

本次检测中模拟人工渗透未发现漏洞。

**5.2.**                **主机漏洞扫描详细风险描述及建议**

漏洞级别：**高危**  12类， **中危**  10类，**低危**  4类

|  |  |  |
| --- | --- | --- |
| **序号** | **漏洞名称** | **漏洞级别** |
| 1 | OpenSSH 安全漏洞(CVE-2016-1908) | **高危** |
|  | |  |  |  |  | | --- | --- | --- | --- | | **漏洞级别** | **高危** | **CVSS分值** | 9.8 | | **CVE编号** | CVE-2016-1908 | **CNNVD编号** | CNNVD-201603-248 | | **漏洞描述** | OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护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中存在安全漏洞，该漏洞源于OpenSSH客户端没有正确为不可信的X11转发生成身份验证cookie。攻击者可利用该漏洞与本地X服务器建立可信连接。 | | | | **整改建议** | 厂商补丁: 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： http://www.openssh.com/txt/release-7.2 | | | | |
| 2 | OpenSSH安全漏洞(CVE-2021-41617) | **高危** |
|  | |  |  |  |  | | --- | --- | --- | --- | | **漏洞级别** | **高危** | **CVSS分值** | 8.8 | | **CVE编号** | CVE-2021-41617 | **CNNVD编号** | CNNVD-202109-1695 | | **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。 | | | | **整改建议** | 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/security.html | | | | |
| 3 | OpenSSH 拒绝服务漏洞(CVE-2016-0778) | **高危** |
|  | |  |  |  |  | | --- | --- | --- | --- | | **漏洞级别** | **高危** | **CVSS分值** | 8.1 | | **CVE编号** | CVE-2016-0778 | **CNNVD编号** | CNNVD-201601-250 | | **漏洞描述** | OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护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的客户端中的roaming\_common.c文件中的’roaming\_read‘和’roaming\_write‘函数中存在安全漏洞，该漏洞源于程序启用特定的代理和转发选项时，没有正确保持连接文件描述符。远程攻击者可通过发送多个转发请求利用该漏洞造成拒绝服务（基于堆的缓冲区溢出）。以下版本受到影响：OpenSSH 5.x版本，6.x版本，7.1p2之前7.x版本。 | | | | **整改建议** | 厂商补丁: 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： http://www.openssh.com/txt/release-7.1p2 | | | | |
| 4 | OpenSSH 安全漏洞(CVE-2016-10012) | **高危** |
|  | |  |  |  |  | | --- | --- | --- | --- | | **漏洞级别** | **高危** | **CVSS分值** | 7.8 | | **CVE编号** | CVE-2016-10012 | **CNNVD编号** | CNNVD-201612-618 | | **漏洞描述** | OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护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 7.4之前的版本中存在安全绕过漏洞。攻击者可利用该漏洞绕过特定的安全限制和执行未授权操作。 | | | | **整改建议** | 厂商补丁: 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： http://www.openssh.com/txt/release-7.4 | | | | |
| 5 | OpenSSH sshd 安全漏洞(CVE-2015-8325) | **高危** |
|  | |  |  |  |  | | --- | --- | --- | --- | | **漏洞级别** | **高危** | **CVSS分值** | 7.8 | | **CVE编号** | CVE-2015-8325 | **CNNVD编号** | CNNVD-201604-341 | | **漏洞描述** | OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护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。sshd是其中的一个独立守护进程。 OpenSSH 7.2p2及之前版本的sshd中的session.c文件中的’do\_setup\_env‘函数存在安全漏洞。当程序启用UseLogin功能并且PAM被配置成读取用户主目录中的.pam\_environment文件时，本地攻击者可借助/bin/login程序的特制的环境变量利用该漏洞获取权限。 | | | | **整改建议** | 厂商补丁: 目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页： http://www.openssh.com/ | | | | |
| 6 | OpenSSH 操作系统命令注入漏洞(CVE-2020-15778) | **高危** |
|  | |  |  |  |  | | --- | --- | --- | --- | | **漏洞级别** | **高危** | **CVSS分值** | 7.8 | | **CVE编号** | CVE-2020-15778 | **CNNVD编号** | CNNVD-202007-1519 | | **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 8.3p1及之前版本中的scp的scp.c文件存在操作系统命令注入漏洞。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。 | | | | **整改建议** | 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/ | | | | |
| 7 | OpenSSH’ssh/kex.c’拒绝服务漏洞(CVE-2016-8858) | **高危** |
|  | |  |  |  |  | | --- | --- | --- | --- | | **漏洞级别** | **高危** | **CVSS分值** | 7.5 | | **CVE编号** | CVE-2016-8858 | **CNNVD编号** | CNNVD-201610-679 | | **漏洞描述** | OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护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 6.x版本和7.x至7.3版本中的kex.c文件的‘kex\_input\_kexinit’函数存在拒绝服务漏洞。远程攻击者可通过发送许多复制的KEXINIT请求利用该漏洞造成拒绝服务。注意：第三方报告称不将OpenSSH upstream视为安全漏洞。 | | | | **整改建议** | 厂商补丁: 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://ftp.openbsd.org/pub/OpenBSD/patches/6.0/common/013\_ssh\_kexinit.patch.sig | | | | |
| 8 | OpenSSH sshd 安全漏洞(CVE-2016-6515) | **高危** |
|  | |  |  |  |  | | --- | --- | --- | --- | | **漏洞级别** | **高危** | **CVSS分值** | 7.5 | | **CVE编号** | CVE-2016-6515 | **CNNVD编号** | CNNVD-201608-172 | | **漏洞描述** | OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护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。sshd是其中的一个独立守护进程。 OpenSSH 7.3之前的版本中的sshd中的auth-passwd.c文件中的’auth\_password‘函数存在安全漏洞，该漏洞源于程序没有在密码验证中限制密码长度。远程攻击者可借助长的字符串利用该漏洞造成拒绝服务(CPU消耗)。 | | | | **整改建议** | 厂商补丁: 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://github.com/openssh/openssh-portable/commit/fcd135c9df440bcd2d5870405ad3311743d78d97 | | | | |
| 9 | OpenSSH sshd 安全漏洞(CVE-2016-10708) | **高危** |
|  | |  |  |  |  | | --- | --- | --- | --- | | **漏洞级别** | **高危** | **CVSS分值** | 7.5 | | **CVE编号** | CVE-2016-10708 | **CNNVD编号** | CNNVD-201801-812 | | **漏洞描述** | OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护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。sshd是其中的一个独立守护进程。 OpenSSH 7.4之前版本中的sshd存在安全漏洞。远程攻击者可借助乱序的NEWKEYS消息利用该漏洞造成拒绝服务（空指针逆向引用和守护进程崩溃）。 | | | | **整改建议** | 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/releasenotes.html | | | | |
| 10 | OpenSSH 安全漏洞(CVE-2016-10009) | **高危** |
|  | |  |  |  |  | | --- | --- | --- | --- | | **漏洞级别** | **高危** | **CVSS分值** | 7.3 | | **CVE编号** | CVE-2016-10009 | **CNNVD编号** | CNNVD-201612-616 | | **漏洞描述** | OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护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 7.4之前的版本中的ssh-agent的ssh-agent.c文件存在不可信的搜索路径漏洞。远程攻击者可通过控制转发的agent-socket利用该漏洞执行任意本地PKCS#11模块。 | | | | **整改建议** | 厂商补丁: 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： http://www.openssh.com/txt/release-7.4 | | | | |
| 11 | OpenSSH 资源管理错误漏洞(CVE-2021-28041) | **高危** |
|  | |  |  |  |  | | --- | --- | --- | --- | | **漏洞级别** | **高危** | **CVSS分值** | 7.1 | | **CVE编号** | CVE-2021-28041 | **CNNVD编号** | CNNVD-202103-527 | | **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。 | | | | **整改建议** | 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 | | | | |
| 12 | OpenSSH sshd 安全漏洞(CVE-2016-10010) | **高危** |
|  | |  |  |  |  | | --- | --- | --- | --- | | **漏洞级别** | **高危** | **CVSS分值** | 7 | | **CVE编号** | CVE-2016-10010 | **CNNVD编号** | CNNVD-201612-609 | | **漏洞描述** | OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护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。sshd是其中的一个独立守护进程。 OpenSSH 7.4之前的版本中的sshd存在安全漏洞。本地攻击者可利用该漏洞获取权限。 | | | | **整改建议** | 厂商补丁: 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： http://www.openssh.com/txt/release-7.4 | | | | |
| 13 | OpenSSH 安全漏洞(CVE-2016-0777) | **中危** |
|  | |  |  |  |  | | --- | --- | --- | --- | | **漏洞级别** | **中危** | **CVSS分值** | 6.5 | | **CVE编号** | CVE-2016-0777 | **CNNVD编号** | CNNVD-201601-249 | | **漏洞描述** | OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护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的客户端中的roaming\_common.c文件中的’resend\_bytes‘函数存在安全漏洞。远程攻击者可通过请求传输整个缓冲区利用该漏洞获取进程内存中的敏感信息。以下版本受到影响：OpenSSH 5.x版本，6.x版本，7.1p2之前7.x版本。 | | | | **整改建议** | 厂商补丁: 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： http://www.openssh.com/txt/release-7.1p2 | | | | |
| 14 | OpenSSH sshd CRLF注入漏洞(CVE-2016-3115) | **中危** |
|  | |  |  |  |  | | --- | --- | --- | --- | | **漏洞级别** | **中危** | **CVSS分值** | 6.4 | | **CVE编号** | CVE-2016-3115 | **CNNVD编号** | CNNVD-201603-244 | | **漏洞描述** | OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护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 7.2p1及之前版本的sshd中的session.c文件中存在CRLF注入漏洞。远程攻击者可借助特制的X11转发数据利用该漏洞绕过既定的shell-command限制。 | | | | **整改建议** | 厂商补丁: 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： http://www.openssh.com/txt/x11fwd.adv | | | | |
| 15 | OpenSSH SSH守护进程安全漏洞(CVE-2016-6210) | **中危** |
|  | |  |  |  |  | | --- | --- | --- | --- | | **漏洞级别** | **中危** | **CVSS分值** | 5.9 | | **CVE编号** | CVE-2016-6210 | **CNNVD编号** | CNNVD-201607-1067 | | **漏洞描述** | OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护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 SSH守护进程中存在安全漏洞，远程攻击者可通过发送长密码利用该漏洞接收不存在用户较短的响应时间。 | | | | **整改建议** | 厂商补丁: 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-7.3 | | | | |
| 16 | OpenSSH 信息泄露漏洞(CVE-2020-14145) | **中危** |
|  | |  |  |  |  | | --- | --- | --- | --- | | **漏洞级别** | **中危** | **CVSS分值** | 5.9 | | **CVE编号** | CVE-2020-14145 | **CNNVD编号** | CNNVD-202006-1822 | | **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。 | | | | **整改建议** | 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/ | | | | |
| 17 | OpenSSH sshd 安全漏洞(CVE-2016-10011) | **中危** |
|  | |  |  |  |  | | --- | --- | --- | --- | | **漏洞级别** | **中危** | **CVSS分值** | 5.5 | | **CVE编号** | CVE-2016-10011 | **CNNVD编号** | CNNVD-201612-606 | | **漏洞描述** | OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护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。sshd是其中的一个独立守护进程。 OpenSSH 7.4之前的版本中的sshd的authfile.c文件中存在安全漏洞。本地攻击者可通过访问privilege-separated子进程利用该漏洞获取敏感的私钥信息。 | | | | **整改建议** | 厂商补丁: 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-7.4 | | | | |
| 18 | OpenSSH 安全漏洞(CVE-2017-15906) | **中危** |
|  | |  |  |  |  | | --- | --- | --- | --- | | **漏洞级别** | **中危** | **CVSS分值** | 5.3 | | **CVE编号** | CVE-2017-15906 | **CNNVD编号** | CNNVD-201710-1230 | | **漏洞描述** | OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护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 7.6之前的版本中的sftp-server.c文件的‘process\_open’函数存在安全漏洞，该漏洞源于程序在只读模式下没有正确的阻止写入操作。攻击者可利用该漏洞创建长度为零的文件。 | | | | **整改建议** | 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/txt/release-7.6 | | | | |
| 19 | OpenSSH 拒绝服务漏洞(CVE-2016-1907) | **中危** |
|  | |  |  |  |  | | --- | --- | --- | --- | | **漏洞级别** | **中危** | **CVSS分值** | 5.3 | | **CVE编号** | CVE-2016-1907 | **CNNVD编号** | CNNVD-201601-366 | | **漏洞描述** | OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护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 7.1p2之前版本的packet.c文件中的‘ssh\_packet\_read\_poll2’函数中存在安全漏洞。远程攻击者可借助特制的网络流量利用该漏洞造成拒绝服务（越边界读取和应用程序崩溃）。 | | | | **整改建议** | 厂商补丁: 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： http://www.openssh.com/txt/release-7.1p2 | | | | |
| 20 | OpenSSH 安全漏洞(CVE-2018-15473) | **中危** |
|  | |  |  |  |  | | --- | --- | --- | --- | | **漏洞级别** | **中危** | **CVSS分值** | 5.3 | | **CVE编号** | CVE-2018-15473 | **CNNVD编号** | CNNVD-201808-536 | | **漏洞描述** | OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护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 7.7及之前版本中存在安全漏洞，该漏洞源于程序会对有效的和无效的身份验证请求发出不同的响应。攻击者可通过发送特制的请求利用该漏洞枚举用户名称。 | | | | **整改建议** | 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/779974d35b4859c07bc3cb8a12c74b43b0a7d1e0 | | | | |
| 21 | OpenSSH 安全漏洞(CVE-2018-15919) | **中危** |
|  | |  |  |  |  | | --- | --- | --- | --- | | **漏洞级别** | **中危** | **CVSS分值** | 5.3 | | **CVE编号** | CVE-2018-15919 | **CNNVD编号** | CNNVD-201808-902 | | **漏洞描述** | OpenSSH（OpenBSD Secure Shell）是OpenBSD计划组所维护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 7.8及之前版本中的auth-gss2.c文件存在安全漏洞。远程攻击者可利用该漏洞检测其指定的用户是否存在。 | | | | **整改建议** | 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/ | | | | |
| 22 | OpenSSH 安全漏洞(CVE-2016-20012) | **中危** |
|  | |  |  |  |  | | --- | --- | --- | --- | | **漏洞级别** | **中危** | **CVSS分值** | 5.3 | | **CVE编号** | CVE-2016-20012 | **CNNVD编号** | CNNVD-202109-1073 | | **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 8.7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。 | | | | **整改建议** | 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/pull/270 | | | | |
| 23 | 探测到目的主机之间的路由信息 | **低危** |
|  | |  |  |  |  | | --- | --- | --- | --- | | **漏洞级别** | **低危** | **CVSS分值** | 0 | | **CVE编号** | / | **CNNVD编号** | / | | **漏洞描述** | Traceroute经常用于诊断主机或网络间的连接情况，然而Traceroute同样可以被攻击者用于获取网络设备和网络结构的有价值的侦察信息。 | | | | **整改建议** | 临时解决方案： \* 可以通过配置防火墙，过滤掉ICMP报文。 /sbin/iptables -A FORWARD -p icmp --icmp-type 11 -j DROP | | | | |
| 24 | 服务器支持的SSH协议版本检查 | **低危** |
|  | |  |  |  |  | | --- | --- | --- | --- | | **漏洞级别** | **低危** | **CVSS分值** | 0 | | **CVE编号** | / | **CNNVD编号** | / | | **漏洞描述** | SSH 为 Secure Shell 的缩写，由 IETF 的网络工作小组（Network Working Group）所制定；SSH 为建立在应用层和传输层基础上的安全协议。 SSH 是目前较可靠，专为远程登录会话和其他网络服务提供安全性的协议。 此插件探测远程服务器支持的ssh协议版本。 | | | | **整改建议** | 关闭使用该协议的端口或者设置ip白名单 | | | | |
| 25 | 服务器支持的TCP/IP时间戳 | **低危** |
|  | |  |  |  |  | | --- | --- | --- | --- | | **漏洞级别** | **低危** | **CVSS分值** | 0 | | **CVE编号** | / | **CNNVD编号** | / | | **漏洞描述** | 远程主机支持了定义在RFC1323的TCP时间戳，通过这个特征可以计算出远程主机的正常运行时间。 | | | | **整改建议** | 关闭使用该协议的端口或者设置ip白名单 | | | | |
| 26 | ICMP请求远程时间泄漏漏洞(CVE-1999-0524) | **低危** |