漏洞扫描安全评估报告

1 检测结果综述

本次报告中，主机【172.20.221.70】共检测出风险22个，其中系统漏洞22个，Web漏洞0个，弱口令0个。

整体风险值为9.6，安全等级为**非常危险**。所有漏洞中，高危漏洞5个，中危漏洞2个，低危漏洞6个，信息级漏洞9个。（漏洞风险等级的分类规则及资产风险等级分类规则，请参见章节《资产风险等级评定标准》）。

2 资产总体概览

2.1 资产基本信息

系统资产列表：

主机名称	172.20.221.70
主机资产	172.20.221.70
操作系统	Linux 2.6.32
MAC地址	68-05-ca-21-d6-e5
扫描时间	系统扫描： 开始时间：2023-09-12 16:38:53 至 2023-09-12 17:07:29 (耗时：28分36秒)
资产风险值	9.6
漏洞分布	漏洞总计：22 高风险：5 中风险：2 低风险：6 信息风险：9
漏洞状态标识	新增：22 误报：0 已修复：0
资产组	默认资产组、系统资产-生态环境厅、系统扫描-51-70资产、系统扫描-172.20.221.70资产
标签	
系统版本	H3C i-Ware Software, Version 3.1, ESS 6202P07
规则库版本	20230213222655

WEB资产列表：

2.2 整体漏洞统计

本报告中包含【1】个主机资产，该主机中存在【0】个Web站点，对主机和Web进行整体漏洞分析的情况如下表所示。主机和Web详细漏洞信息见章节4，章节5。

IP/URL	高	中	低	信息	总计
系统漏洞	5	2	6	9	22
WEB漏洞	0	0	0	0	0
总计	**5**	**2**	**6**	**9**	**22**

2.3 敏感端口/服务

本次任务检测到开放了以下【5】种敏感端口或服务，具体情况如下表所示:

序号	端口	服务	协议
1	22	ssh/openbsd:openssh:8.2 OpenSSH	TCP
2	111	rpcbind	TCP

3	111	rpcbind	UDP
4	161	snmp/net-snmp:net-snmp net-snmp	UDP
5	9090	https	TCP

说明：敏感端口/服务指根据安全研究表明，容易被黑客利用漏洞发起攻击的端口/服务。

2.4 敏感中间件

本次任务检测到以下【0】种敏感中间件，具体情况如下表所示:

序号	中间件

说明：敏感中间件是指安全研究表明，容易被黑客利用发起攻击的中间件。

3 资产端口服务信息

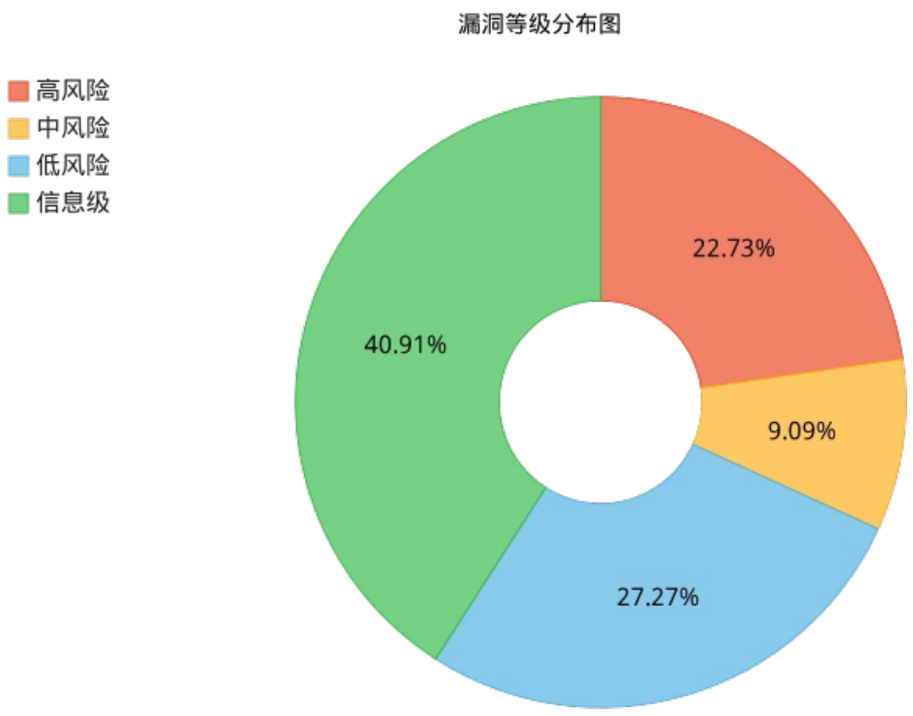
资产的端口/服务开放情况如下表所示，共开放了【5】个端口:

端口	服务	协议	漏洞总数
⊟ 22	ssh/openbsd:openssh:8.2 OpenSSH	TCP	12
⊟ 111	rpcbind	TCP	2
⊟ 111	rpcbind	UDP	2
⊟ 161	snmp/net-snmp:net-snmp net-snmp	UDP	1
⊟ 9090	https	TCP	4
⊟ --	--	ICMP	1

4 主机漏洞信息

4.1 主机漏洞统计概况

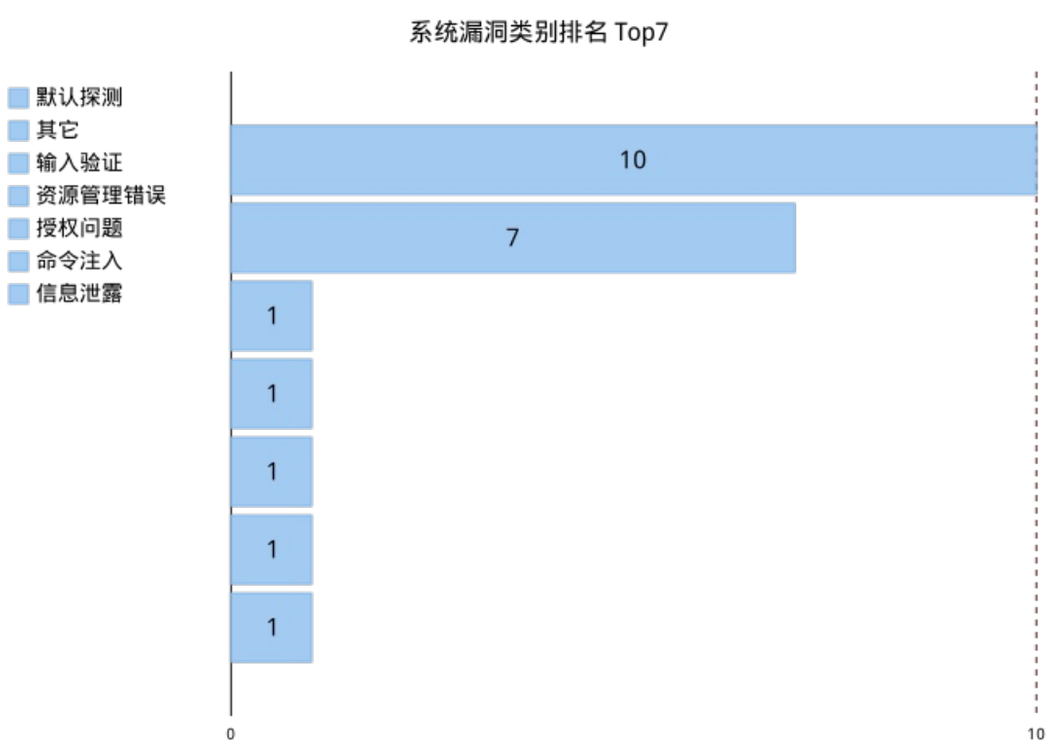
4.1.1 漏洞等级分布



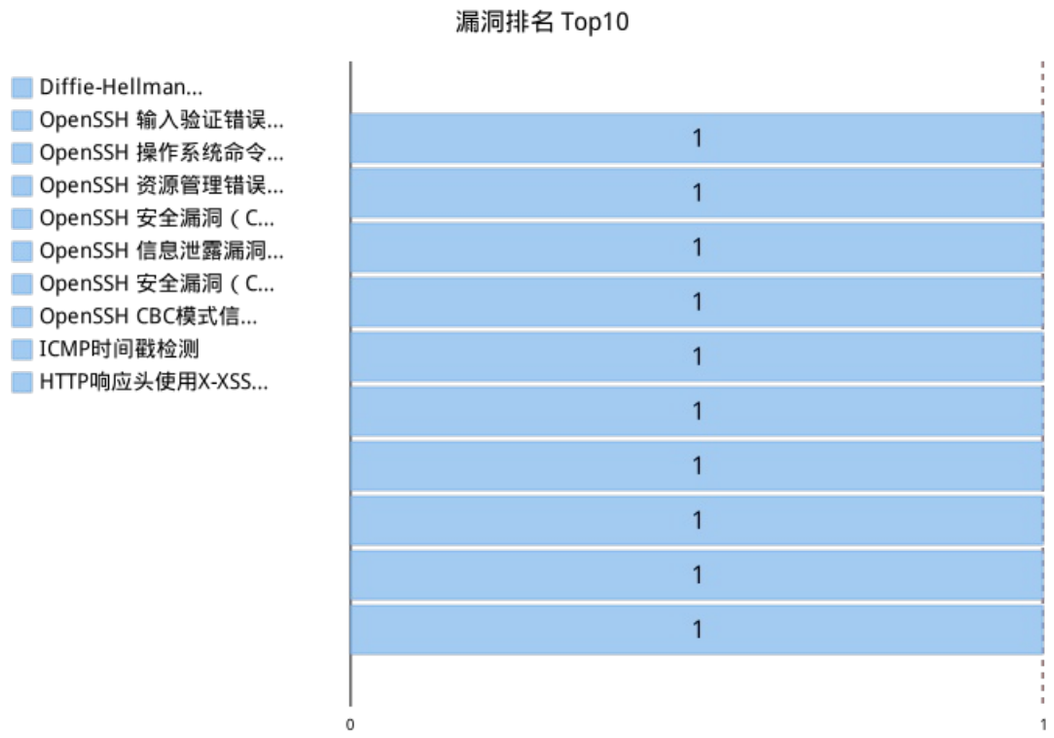
高风险	中风险	低风险	信息级	总计
5	2	6	9	22

4.1.2 漏洞类别统计

4.1.3 漏洞排名



序号	主机漏洞类别（TOP10）	总计
1	默认探测	10
2	其它	7
3	输入验证	1
4	资源管理错误	1
5	授权问题	1
6	命令注入	1
7	信息泄露	1



序号	系统漏洞名称（TOP10）	总计
1	Diffie-Hellman Key Agreement Protocol 资源管理错误漏洞（CVE-2002-20001）	1
2	OpenSSH 输入验证错误漏洞（CVE-2020-12062）	1
3	OpenSSH 操作系统命令注入漏洞（CVE-2020-15778）	1
4	OpenSSH 资源管理错误漏洞（CVE-2021-28041）	1
5	OpenSSH 安全漏洞（CVE-2021-41617）	1
6	OpenSSH 信息泄露漏洞（CVE-2020-14145）	1
7	OpenSSH 安全漏洞（CVE-2016-20012）	1
8	OpenSSH CBC模式信息泄露漏洞（CVE-2008-5161）【原理扫描】	1
9	ICMP时间戳检测	1
10	HTTP响应头使用X-XSS-Protection检查	1

4.2 主机漏洞详情

漏洞名称	漏洞分类	漏洞类型	出现次数
⊟ Diffie-Hellman Key Agreement Protocol 资源管理错误漏洞（CVE-2002-20001）	默认探测	高风险	1

漏洞编号	55005
风险级别	高风险
概要	

描述	Diffie-Hellman Key Agreement Protocol是一种密钥协商协议。它最初在 Diffie 和 Hellman 关于公钥密码学的开创性论文中有所描述。该密钥协商协议允许 Alice 和 Bob 交换公钥值，并根据这些值和他们自己对应的私钥的知识，安全地计算共享密钥K，从而实现进一步的安全通信。仅知道交换的公钥值，窃听者无法计算共享密钥。Diffie-Hellman Key Agreement Protocol 存在安全漏洞，远程攻击者可以发送实际上不是公钥的任意数字，并触发服务器端DHE模幂计算。
解决办法	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://github.com/Balasys/dheater
CVSS	7.5
检测详情	主机：172.20.221.70| 端口：22| 服务：ssh| 协议：TCP diffie-hellman-group14-sha1,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group-exchange-sha1,diffie-hellman-group-exchange-sha256 漏洞状态：新增

OpenSSH 输入验证错误漏洞（CVE-2020-12062）	输入验证	高风险	1

漏洞编号	1145510
风险级别	高风险
概要	其他
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 8.2版本中存在安全漏洞，该漏洞源于在utimes系统调用失败时，scp客户端错误地向服务器发送了重复的响应。攻击者可通过在远程服务器上创建子目录利用该漏洞覆盖客户端下载目录中的任意文件。
解决办法	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-8.3
详情请参阅	https://github.com/openssh/openssh-portable/commit/aad87b88fc2536b1ea023213729aaf4eaabe1894 https://www.openssh.com/txt/release-8.3 https://github.com/openssh/openssh-portable/commit/955854cafca88e0cdcd3d09ca1ad4ada465364a1 https://www.openwall.com/lists/oss-security/2020/05/27/1 https://nvd.nist.gov/vuln/detail/CVE-2020-12062
CVE	CVE-2020-12062
CVSS	7.5
CNNVD	CNNVD-202006-078
检测详情	主机：172.20.221.70| 端口：22| 服务：ssh| 协议：TCP openbsd:openssh 8.2 == 8.2 漏洞状态：新增

OpenSSH 操作系统命令注入漏洞（CVE-2020-15778）	命令注入	高风险	1

漏洞编号	1148318
风险级别	高风险
概要	
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。
解决办法	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/
详情请参阅	https://security.netapp.com/advisory/ntap-20200731-0007/ https://news.ycombinator.com/item?id=25005567 https://github.com/cpandya2909/CVE-2020-15778/ https://www.openssh.com/security.html https://nvd.nist.gov/vuln/detail/CVE-2020-15778 https://vigilance.fr/vulnerability/OpenSSH-code-execution-via-scp-Backticks-32917 https://www.auscert.org.au/bulletins/ESB-2020.3260/ https://www.ibm.com/blogs/psirt/security-bulletin-vulnerability-in-openssh-affects-ibm-integrated-analytics-system-2/ https://www.ibm.com/blogs/psirt/security-bulletin-openssh-vulnerability-affects-ibm-spectrum-protect-plus-cve-2020-15778/ https://www.ibm.com/support/pages/node/6524682 http://www.nsfocus.net/vulndb/47482 https://www.auscert.org.au/bulletins/ESB-2020.3260.2/ https://www.ibm.com/blogs/psirt/security-bulletin-ibm-security-guardium-insights-is-affected-by-multiple-vulnerabilities-2/
CVE	CVE-2020-15778
CVSS	7.8
CNNVD	CNNVD-202007-1519
检测详情	主机：172.20.221.70| 端口：22| 服务：ssh| 协议：TCP openbsd:openssh 8.2 < 8.3 漏洞状态：新增

⊟ OpenSSH 资源管理错误漏洞（CVE-2021-28041）	资源管理错误	高风险	1

漏洞编号	1160852
风险级别	高风险
概要	
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 8.5 版本之前存在资源管理错误漏洞，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。
解决办法	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
详情请参阅	https://github.com/openssh/openssh-portable/commit/e04fd6dde16de1cdc5a4d9946397ff60d96568db https://www.openwall.com/lists/oss-security/2021/03/03/1 https://www.oracle.com//security-alerts/cpujul2021.html https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/KQWGII3LQR4AOTPPFXGMTYE7UDEWIUKI/ https://security.netapp.com/advisory/ntap-20210416-0002/ https://www.openssh.com/txt/release-8.5 https://security.gentoo.org/glsa/202105-35

	https://www.openssh.com/security.html https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/TXST2CML2MWY3PNVUXX7FFJE3ATJMNVZ/ https://packetstormsecurity.com/files/161743/Ubuntu-Security-Notice-USN-4762-1.html https://www.cybersecurity-help.cz/vdb/SB2021052625 https://packetstormsecurity.com/files/162813/Gentoo-Linux-Security-Advisory-202105-35.html https://www.ibm.com/support/pages/node/6524682 https://www.auscert.org.au/bulletins/ESB-2021.0862 https://nvd.nist.gov/vuln/detail/CVE-2021-28041
CVE	CVE-2021-28041
CVSS	7.1
CNNVD	CNNVD-202103-527
检测详情	主机：172.20.221.70| 端口：22| 服务：ssh| 协议：TCP openbsd:openssh 8.2 >= 8.2 openbsd:openssh 8.2 < 8.5 漏洞状态：新增

⊟ OpenSSH 安全漏洞（CVE-2021-41617）	其它	高风险	1

漏洞编号	1173001
风险级别	高风险
概要	
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。
解决办法	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
详情请参阅	https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/KVI7RWM2JLNMWTOFK6BDUSGNOIPZYPUT/ https://www.openwall.com/lists/oss-security/2021/09/26/1 https://security.netapp.com/advisory/ntap-20211014-0004/ https://bugzilla.suse.com/show_bug.cgi?id=1190975 https://www.oracle.com/security-alerts/cpuapr2022.html https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/W44V2PFQH5YLRN6ZJTVRKAD7CU6CYYET/ https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/6XJIONMHMKZDTMH6BQR5TNLF2WDCGWED/ https://www.openssh.com/security.html https://www.oracle.com/security-alerts/cpujul2022.html https://www.openssh.com/txt/release-8.8 https://www.auscert.org.au/bulletins/ESB-2022.0245 https://www.auscert.org.au/bulletins/ESB-2022.3977 https://www.cybersecurity-help.cz/vdb/SB2021120707

	https://www.ibm.com/support/pages/node/6524682 https://www.cybersecurity-help.cz/vdb/SB2022021901 https://www.auscert.org.au/bulletins/ESB-2022.1050 https://packetstormsecurity.com/files/167059/Red-Hat-Security-Advisory-2022-2013-01.html https://www.cybersecurity-help.cz/vdb/SB2022062931 https://www.cybersecurity-help.cz/vdb/SB2022051161 https://www.ibm.com/support/pages/node/6522092 https://www.cybersecurity-help.cz/vdb/SB2021120119 https://www.auscert.org.au/bulletins/ESB-2021.4085 https://packetstormsecurity.com/files/167381/Red-Hat-Security-Advisory-2022-4671-01.html https://www.auscert.org.au/bulletins/ESB-2022.2474 https://www.auscert.org.au/bulletins/ESB-2022.3343 https://vigilance.fr/vulnerability/OpenSSH-privilege-escalation-via-Supplemental-Groups-36535 https://www.auscert.org.au/bulletins/ESB-2021.4120 https://www.cybersecurity-help.cz/vdb/SB2022070643 https://www.cybersecurity-help.cz/vdb/SB2021120214 https://www.cybersecurity-help.cz/vdb/SB2022071832 https://nvd.nist.gov/vuln/detail/CVE-2021-41617 https://www.auscert.org.au/bulletins/ESB-2022.3821 https://packetstormsecurity.com/files/167224/Red-Hat-Security-Advisory-2022-4692-01.html https://www.cybersecurity-help.cz/vdb/SB2021112330 https://packetstormsecurity.com/files/165063/Red-Hat-Security-Advisory-2021-4782-01.html https://www.cybersecurity-help.cz/vdb/SB2022021711 https://www.auscert.org.au/bulletins/ESB-2021.3975 https://www.cybersecurity-help.cz/vdb/SB2022010623 https://www.auscert.org.au/bulletins/ESB-2022.3136 https://www.auscert.org.au/bulletins/ESB-2022.3236 https://www.cybersecurity-help.cz/vdb/SB2022070811
CVE	CVE-2021-41617
CVSS	7.0
CNNVD	CNNVD-202109-1695
检测详情	主机：172.20.221.70| 端口：22| 服务：ssh| 协议：TCP openbsd:openssh 8.2 >= 6.2 openbsd:openssh 8.2 < 8.8 漏洞状态：新增

⊟ OpenSSH 信息泄露漏洞（CVE-2020-14145）	信息泄露	中风险	1

漏洞编号	1147045
风险级别	中风险
概要	
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信息泄露漏洞。攻击者可利用该漏洞获取信息。
解决办法	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/
详情请参阅	https://www.fzi.de/en/news/news/detail-en/artikel/fsa-2020-2-ausnutzung-eines-informationslecks-fuer-gezielte-mitm-angriffe-auf-ssh-clients/ https://github.com/ssh-mitm/ssh-mitm/blob/master/ssh_proxy_server/plugins/session/cve202014145.py https://security.netapp.com/advisory/ntap-20200709-0004/ http://www.openwall.com/lists/oss-security/2020/12/02/1 https://docs.ssh-mitm.at/CVE-2020-14145.html https://anongit.mindrot.org/openssh.git/commit/?id=b3855ff053f5078ec3d3c653cdaedefaa5fc362d https://security.gentoo.org/glsa/202105-35 https://github.com/openssh/openssh-portable/compare/V_8_3_P1...V_8_4_P1 https://www.auscert.org.au/bulletins/ESB-2020.3515/ https://www.auscert.org.au/bulletins/ESB-2022.0245 https://packetstormsecurity.com/files/164823/Red-Hat-Security-Advisory-2021-4368-04.html http://www.nsfocus.net/vulndb/47019 https://www.auscert.org.au/bulletins/ESB-2020.4369/ https://www.auscert.org.au/bulletins/ESB-2020.4466/ https://www.auscert.org.au/bulletins/ESB-2021.3905 https://packetstormsecurity.com/files/165631/Red-Hat-Security-Advisory-2022-0202-04.html https://www.ibm.com/blogs/psirt/security-bulletin-vulnerability-in-openssh-affects-ibm-integrated-analytics-system-4/ https://www.auscert.org.au/bulletins/ESB-2022.0716 https://packetstormsecurity.com/files/165209/Red-Hat-Security-Advisory-2021-5038-04.html https://www.cybersecurity-help.cz/vdb/SB2021052625 https://packetstormsecurity.com/files/162813/Gentoo-Linux-Security-Advisory-202105-35.html https://packetstormsecurity.com/files/165286/Red-Hat-Security-Advisory-2021-5128-06.html https://www.auscert.org.au/bulletins/ESB-2020.3515.2/ https://www.auscert.org.au/bulletins/ESB-2021.4229 https://www.ibm.com/blogs/psirt/security-bulletin-ibm-security-guardium-insights-is-affected-by-multiple-vulnerabilities-2/ https://www.auscert.org.au/bulletins/ESB-2021.0053/ https://packetstormsecurity.com/files/165099/Red-Hat-Security-Advisory-2021-4848-07.html https://www.auscert.org.au/bulletins/ESB-2021.3782 https://packetstormsecurity.com/files/166051/Red-Hat-Security-Advisory-2022-0580-01.html https://vigilance.fr/vulnerability/OpenSSH-information-disclosure-via-Dynamic-Policy-Host-Key-32646 https://www.auscert.org.au/bulletins/ESB-2021.4254 https://www.auscert.org.au/bulletins/ESB-2020.4504/ https://www.auscert.org.au/bulletins/ESB-2021.4172 https://packetstormsecurity.com/files/164967/Red-Hat-Security-Advisory-2021-4627-01.html https://nvd.nist.gov/vuln/detail/CVE-2020-14145
CVE	CVE-2020-14145
CVSS	5.9
CNNVD	CNNVD-202006-1822
检测详情	主机：172.20.221.70| 端口：22| 服务：ssh| 协议：TCP openbsd:openssh 8.2 >= 5.7

openbsd:openssh 8.2 < 8.4

漏洞状态：新增

OpenSSH 安全漏洞（CVE-2016-20012）	其它	中风险	1

漏洞编号	1172469
风险级别	中风险
概要	
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。
解决办法	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
详情请参阅	https://github.com/openssh/openssh-portable/blob/d0fffc88c8fe90c1815c6f4097bc8cbcabc0f3dd/auth2-pubkey.c#L261-L265 https://github.com/openssh/openssh-portable/pull/270 https://security.netapp.com/advisory/ntap-20211014-0005/ https://rushter.com/blog/public-ssh-keys/ https://github.com/openssh/openssh-portable/pull/270#issuecomment-920577097 https://www.openwall.com/lists/oss-security/2018/08/24/1 https://utcc.utoronto.ca/~cks/space/blog/tech/SSHKeysAreInfoLeak https://github.com/openssh/openssh-portable/pull/270#issuecomment-943909185 https://vigilance.fr/vulnerability/OpenSSH-information-disclosure-via-Public-Key-Username-Combination-36441 https://nvd.nist.gov/vuln/detail/CVE-2016-20012
CVE	CVE-2016-20012
CVSS	5.3
CNNVD	CNNVD-202109-1073
检测详情	主机：172.20.221.70| 端口：22| 服务：ssh| 协议：TCP openbsd:openssh 8.2 <= 8.7 漏洞状态：新增

OpenSSH CBC模式信息泄露漏洞（CVE-2008-5161）【原理扫描】	默认探测	低风险	1

漏洞编号	767
风险级别	低风险
概要	远程信息泄露
描述	远程SSH服务器配置为允许使用弱加密算法。 “ arcfour”密码是具有128位密钥的Arcfour流密码。人们认为Arcfour密码与RC4密码[SCHNEIER]兼容。 Arcfour（和RC4）的按键较弱，因此不应该再使用。 “无”算法指定不进行加密。请注意，此方法不提供机密性保护，建议不要使用它。 使用CBC模式的SSH消息中存在一个漏洞，该漏洞可能允许攻击者从密文块中恢复纯文本。
解决办法	临时解决方法：

* 在SSH会话中仅使用CTR模式加密算法，如AES-CTR。

厂商补丁：

OpenSSH

目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：

https://downloads.ssh.com/

RedHat

RedHat已经为此发布了一个安全公告（RHSA-2009:1287-02）以及相应补丁:

RHSA-2009:1287-02：Low: openssh security, bug fix, and enhancement update

链接：https://www.redhat.com/support/errata/RHSA-2009-1287.html

详情请参阅	URL:https://tools.ietf.org/html/rfc4253#section-6.3, URL:https://www.kb.cert.org/vuls/id/958563
CVE	CVE-2008-5161
CVSS	2.6
检测详情	主机：172.20.221.70| 端口：22| 服务：ssh| 协议：TCP CBC mode support 漏洞状态：新增

ICMP时间戳检测	默认探测	低风险	1

漏洞编号	39248
风险级别	低风险
概要	远程信息泄露
描述	远程主机响应了ICMP时间戳请求。时间戳回复是一种ICMP消息，它回复时间戳消息。它由时间戳的发送方发送的始发时间戳以及接收时间戳和发送时间戳组成。从理论上讲，该信息可用于开发其他服务中基于弱时间的随机数生成器。
解决办法	信息检测，无需修复。
详情请参阅	URL:http://www.ietf.org/rfc/rfc0792.txt
CVE	CVE-1999-0524
CVSS	2.1
检测详情	主机：172.20.221.70 漏洞状态：新增

HTTP响应头使用X-XSS-Protection检查	默认探测	低风险	1

漏洞编号	54599
风险级别	低风险

概要	
描述	远程Web应用程序不设置X-XSS-Protection响应头。
解决办法	需要在Web应用程序的所有页面上设置以下响应头：X-XSS-Protection：1; mode=block
CVSS	1.0
检测详情	主机：172.20.221.70| 端口：9090| 服务：https| 协议：TCP 200 OK Content-Type:text/html Content-Security-Policy:connect-src 'self' https://172.20.221.70:9090 wss://172.20.221.70:9090; form-action 'self' https://172.20.221.70:9090; base-uri 'self' https://172.20.221.70:9090; object-src 'none'; font-src 'self' https://172.20.221.70:9090 data:; img-src 'self' https://172.20.221.70:9090 data:; block-all-mixed-content; default-src 'self' https://172.20.221.70:9090 'unsafe-inline' Set-Cookie:cockpit=deleted; PATH=/; Secure; HttpOnly Transfer-Encoding:chunked Cache-Control:no-cache, no-store X-DNS-Prefetch-Control:off Referrer-Policy:no-referrer X-Content-Type-Options:nosniff 漏洞状态：新增

HTTP响应头部使用X-Frame-Options检查	默认探测	低风险	1

漏洞编号	54601
风险级别	低风险
概要	
描述	远程Web应用程序不设置X-Frame-Options响应头。微软已经提出X-Frame-Options作为缓解点击劫持攻击的一种方法，并且已经在Chrome和Safari中实施。
解决办法	需要在Web应用程序的所有页面上设置以下响应头：X-Frame-Options：DENY
CVSS	1.0
检测详情	主机：172.20.221.70| 端口：9090| 服务：https| 协议：TCP 200 OK Content-Type:text/html Content-Security-Policy:connect-src 'self' https://172.20.221.70:9090 wss://172.20.221.70:9090; form-action 'self' https://172.20.221.70:9090; base-uri 'self' https://172.20.221.70:9090; object-src 'none'; font-src 'self' https://172.20.221.70:9090 data:; img-src 'self' https://172.20.221.70:9090 data:; block-all-mixed-content; default-src 'self' https://172.20.221.70:9090 'unsafe-inline' Set-Cookie:cockpit=deleted; PATH=/; Secure; HttpOnly Transfer-Encoding:chunked Cache-Control:no-cache, no-store X-DNS-Prefetch-Control:off Referrer-Policy:no-referrer X-Content-Type-Options:nosniff 漏洞状态：新增

HTTP安全返回头Strict-Transport-Security检查	默认探测	低风险	1

漏洞编号	54602
风险级别	低风险
概要	
描述	远程Web应用程序不设置Strict-Transport-Security响应标头。HTTP严格传输安全（HSTS）强制执行到服务器的安全（HTTP over SSL / TLS）连接。这可以减少网络应用程序中的漏洞通过cookie和外部链接泄漏会话数据的影响，并抵御中间人攻击。 HSTS还禁止用户忽略SSL协商警告的能力。
解决办法	需要在Web应用程序的所有页面上设置以下标题：Strict-Transport-Security：max-age = 16070400;请注意，当您设置此标头时，您需要在端口443上运行的Web服务器。如果你没有它并且应用这个修复你的网站将不再可用
CVSS	1.0
检测详情	主机：172.20.221.70| 端口：9090| 服务：https| 协议：TCP 200 OK Content-Type:text/html Content-Security-Policy:connect-src 'self' https://172.20.221.70:9090 wss://172.20.221.70:9090; form-action 'self' https://172.20.221.70:9090; base-uri 'self' https://172.20.221.70:9090; object-src 'none'; font-src 'self' https://172.20.221.70:9090 data:; img-src 'self' https://172.20.221.70:9090 data:; block-all-mixed-content; default-src 'self' https://172.20.221.70:9090 'unsafe-inline' Set-Cookie:cockpit=deleted; PATH=/; Secure; HttpOnly Transfer-Encoding:chunked Cache-Control:no-cache, no-store X-DNS-Prefetch-Control:off Referrer-Policy:no-referrer X-Content-Type-Options:nosniff 漏洞状态：新增

OpenSSH 授权问题漏洞（CVE-2021-36368）	授权问题	低风险	1

漏洞编号	1183652
风险级别	低风险
概要	
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。
解决办法	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
详情请参阅	https://bugzilla.mindrot.org/show_bug.cgi?id=3316 https://github.com/openssh/openssh-portable/pull/258 https://security-tracker.debian.org/tracker/CVE-2021-36368 https://docs.ssh-mitm.at/trivialauth.html https://www.openssh.com/security.html
CVE	CVE-2021-36368

CVSS	3.7
CNNVD	CNNVD-202203-1230
检测详情	主机：172.20.221.70| 端口：22| 服务：ssh| 协议：TCP openbsd:openssh 8.2 < 8.9 漏洞状态：新增

探测到SSH服务器支持的算法	默认探测	信息	1

漏洞编号	2720
风险级别	信息
概要	
描述	本插件用来获取SSH服务器支持的算法列表。
解决办法	信息检测，可不修复。
CVSS	0.0
检测详情	主机：172.20.221.70| 端口：22| 服务：ssh| 协议：TCP kex_algorithms: curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1 server_host_key_algorithms: rsa-sha2-512,rsa-sha2-256,ssh-rsa,ecdsa-sha2-nistp256,ssh-ed25519 encryption_algorithms_client_to_server: aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes256-ctr,aes256-cbc,aes128-gcm@openssh.com,aes128-ctr,aes128-cbc encryption_algorithms_server_to_client: aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes256-ctr,aes256-cbc,aes128-gcm@openssh.com,aes128-ctr,aes128-cbc mac_algorithms_client_to_server: hmac-sha2-256-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha1,umac-128@openssh.com,hmac-sha2-512 mac_algorithms_server_to_client: hmac-sha2-256-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha1,umac-128@openssh.com,hmac-sha2-512 compression_algorithms_client_to_server: none,zlib@openssh.com

compression_algorithms_server_to_client:

none,zlib@openssh.com

漏洞状态：新增

RPC端口映射器（TCP）	默认探测	信息	1

漏洞编号	32900
风险级别	信息
概要	
描述	在TCP上执行RPC portmapper的检测
解决办法	信息探测，无需修复
CVSS	0.0
检测详情	

主机：172.20.221.70| 端口：111| 服务：rpcbind|

协议：TCP

RPC portmapper is running on this port.

漏洞状态：新增

检测到远程可执行rpcinfo -p	其它	信息	1

漏洞编号	33542
风险级别	信息
概要	
描述	该脚本在端口映射器上调用DUMP RPC，以获取所有已注册程序的列表。
解决办法	限制服务的访问权限。
CVSS	0.0
检测详情	

主机：172.20.221.70| 端口：111| 服务：rpcbind|

协议：TCP

rpc Version:2

漏洞状态：新增

探测到远程主机支持的SSH协议版本	默认探测	信息	1

漏洞编号	33557
风险级别	信息
概要	
描述	识别目标主机SSH服务支持的SSH协议版本
解决办法	信息探测，无需修复
CVSS	0.0
检测详情	

	主机：172.20.221.70| 端口：22| 服务：ssh| 协议：TCP
	1.99 2.0
	漏洞状态：新增

RPC portmapper服务检测	其它	信息	1

漏洞编号	42120
风险级别	信息
概要	不必要的服务
描述	ONC RPC端口映射程序正在远程主机上运行。 RPC portmapper在此端口上运行。 该端口映射器允许某人通过发送多个查找请求或DUMP请求来获取在远程主机上运行的每个RPC服务的端口号。
解决办法	若不适用，建议关闭该程序
CVE	CVE-1999-0632
CVSS	0.0
检测详情	主机：172.20.221.70| 端口：111| 服务：rpcbind| 协议：UDP 漏洞状态：新增

检测到RPC portmapper正在远端运行（UDP）	其它	信息	1

漏洞编号	44631
风险级别	信息
概要	
描述	此脚本在UDP上执行RPC portmapper的检测。
解决办法	检测信息类，无需修复
CVSS	0.0
检测详情	主机：172.20.221.70| 端口：111| 服务：rpcbind| 协议：UDP RPC portmapper is running on this port. 漏洞状态：新增

探测到SSH服务正在运行	其它	信息	1

漏洞编号	52471
风险级别	信息
概要	
描述	通过向服务端发送请求，获取到Banner信息，从而探测到SSH服务得版本信息。
解决办法	通过加固软件的配置，禁止Banner信息的泄露，从而防止服务版本的泄露

CVSS	0.0
检测详情	主机：172.20.221.70| 端口：22| 服务：ssh| 协议：TCP 检测到远端运行着SSH服务 漏洞状态：新增

探测到远端SNMP服务正在运行	其它	信息	1

漏洞编号	52476
风险级别	信息
概要	
描述	通过向服务端发送请求，获取到Banner信息，从而探测到snmp
解决办法	通过加固软件的配置，禁止Banner信息的泄露，从而防止服务版本的泄露
CVSS	0.0
检测详情	主机：172.20.221.70| 端口：161| 服务：snmp| 协议：UDP 检测到远端运行着SNMP服务 漏洞状态：新增

探测支持ssl协议【原理扫描】	默认探测	信息	1

漏洞编号	53908
风险级别	信息
概要	
描述	探测支持ssl协议
解决办法	
CVSS	0.0
检测详情	主机：172.20.221.70| 端口：9090| 服务：https| 协议：TCP | TLSv1.1: | ciphers: | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A | TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A | TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A | compressors: | NULL | cipher preference: client | TLSv1.2:

| ciphers:

| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A

| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A

| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A

| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A

| TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (secp256r1) - A

| TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A

| TLS_RSA_WITH_AES_128_CCM (rsa 2048) - A

| TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A

| TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A

| TLS_RSA_WITH_AES_256_CCM (rsa 2048) - A

| TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A

| compressors:

| NULL

| cipher preference: client

|_

漏洞状态：新增

5 WEB漏洞信息

5.1 WEB漏洞统计概况

5.1.1 漏洞等级分布

高风险	中风险	低风险	信息级	总计
0	**0**	**0**	**0**	**0**

5.1.2 漏洞类别统计

序号	WEB漏洞类别	总计

5.1.3 漏洞排名

序号	WEB漏洞名称（TOP10）	总计

5.2 WEB漏洞详情

漏洞名称	漏洞分类	漏洞类型	出现次数

6 弱口令

序号	主机地址	用户名	密码	服务	端口

7 参考标准

7.1 单一漏洞风险等级评定标准

危险程度	危险值区域	危险程度说明
高	7 <= 漏洞风险值 <= 10	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。
中	4 <= 漏洞风险值 < 7	攻击者可以远程创建、修改、删除文件或数据，或对普通服务进行拒绝服务攻击。
低	0 < 漏洞风险值 < 4	攻击者可以获取某些系统、服务的信息，或读取系统文件和数据。
信息	漏洞风险值 = 0	攻击者可以获取服务及组件等版本信息。

1. 可远程获取漏洞组件的版本信息。
2. 目标系统服务器开放了不必要的服务。
3. 可远程访问到某些不在目录树中的文件或读取服务器动态脚本的源码。
4. 可远程因为会话管理的问题导致身份冒用。
5. 可远程利用受影响的系统服务器攻击其他浏览网站的用户。
6. 可远程读取系统文件或后台数据库。
7. 可远程读写系统文件、操作后台数据库。
8. 可远程以普通用户身份执行命令或进行拒绝服务攻击。
9. 可远程以管理用户身份执行命令（受限、不太容易利用）。
10. 可远程以管理用户身份执行命令（不受限、容易利用）。

7.2 资产风险等级评定标准

资产风险等级	资产风险值区域
非常危险	8 <= 资产风险值 <= 10
比较危险	5 <= 资产风险值 < 8
比较安全	2 <= 资产风险值 < 5
非常安全	0 <= 资产风险值 < 2

1. 将资产的漏洞按照分数的高低排序，依据漏洞的分数将漏洞威胁划分为高、中、低三个类别。
2. 单个资产的风险值按照风险评估模型计算来得到；网络的风险值是由最危险资产决定，即最大的资产风险值。
3. 高、中、低漏洞威胁的定义参见《单一漏洞风险等级评定标准》。
4. 资产的风险等级定位为四级：非常危险、比较危险、比较安全和非常安全。具体的评判标准请参考《资产风险等级评定标准》。

8 安全建议

随着越来越多的网络访问通过系统漏洞进行操作，系统漏洞已成为互联网安全的一个热点，基于系统漏洞的攻击广为流行，CGI攻击检测、网络设备和防火墙、本地安全检查等问题严重威胁着系统管理者和系统用户的安全，我们有必要采取措施消除这些风险。

建议对存在漏洞的资产参考附件中提出的解决方案进行漏洞修补、安全增强。

请专业的安全研究人员或安全公司对系统架构做全面的安全审计，修补所有发现的安全漏洞，这种白盒安全测试比较深入全面。

对系统的开发人员进行安全编码方面的培训，在开发过程避免漏洞的引入能起到事半功倍的效果。

采用专业的系统安全产品，可以在不修改系统本身的情况下对大多数的基于漏洞攻击起到有效的阻断作用。

建议网络管理员、系统管理员、安全管理员关注安全信息、安全动态及最新的高危漏洞，特别是影响到漏洞站点所使用的系统和软件的漏洞，应该在事前设计好应对规划，一旦发现系统受漏洞影响及时采取措施。

9 联系我们

公司：新华三技术有限公司

网址：http://www.h3c.com/

热线：400-810-0504

传真：-

地址：杭州市滨江区长河路466号