目录

二 主机详情

2.1 主机10.20.198.38

2.1.1 主机信息

资产名称	--
所属部门	--
资产类型	--
资产价值	--
NetBios名	--
netbios域名/工作组	--
保护等级	--
主机名	--
主机风险状态	极度危险
操作系统信息	Linux 4.4

2.1.2 账号分布

序号	猜测类型	用户名	密码(隐藏)	描述
暂无数据				

2.1.3 端口/漏洞列表

22__TCP__ssh

序号	危险级别	漏洞编号	漏洞名称	返回信息
1	高危险	00AA5D4F	OpenSSH 安全漏洞(CVE-2023-28531)	openssh-9.0
2	高危险	00AA61E6	OpenSSH 代码问题漏洞(CVE-2023-38408)	openssh-9.0
3	信息	0x0013034A	检测到目标主机SSH服务正在运行	
4	信息	0x1ebb5c	目标主机SSH服务协议版本可列取	
5	信息	0x1ebb5d	目标主机SSH服务加密算法可列取	Found algorithms
6	信息	0xb2d3b141	探测到Openssh版本信息	openssh-9.0

0__其他协议__其他服务

序号	危险级别	漏洞编号	漏洞名称	返回信息
1	低危险	001E93A6	ICMP权限许可和访问控制漏洞CVE-1999-0524	
2	信息	0x1ebc5e	Traceroute探测信息	Here is the route from 175.18.150.12 to 10.20.198.38 : 175.18.150.12 175.18.100.2 10.20.36.1 10.20.241.153 * * * 10.20.198.38

2.2 漏洞详细

【1】OpenSSH 安全漏洞(CVE-2023-28531)

漏洞编号	00AA5D4F
漏洞类型	OpenSSH
危险级别	高危险
影响平台	OpenSSH 8.9 before 9.3
CVSS分值	9.8
bugtraq编号	

CVE编号	CVE-2023-28531
CNCVE编号	CNCVE-202328531
国家漏洞库编号	CNNVD-202303-1391
CNVD编号	
漏洞可利用性	3.9
存在主机	10.20.198.38
简单描述	OpenSSH 9.3之前版本存在安全漏洞
详细描述	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 9.3之前版本存在安全漏洞，该漏洞源于将智能卡密钥添加到ssh-agent。
修补建议	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://www.openwall.com/lists/oss-security/2023/03/15/8
参考网址	
漏洞安全性	

【2】OpenSSH 代码问题漏洞(CVE-2023-38408)

漏洞编号	00AA61E6
漏洞类型	OpenSSH
危险级别	高危险
影响平台	OpenSSH before 9.3p2
CVSS分值	9.8
bugtraq编号	
CVE编号	CVE-2023-38408
CNCVE编号	CNCVE-202338408
国家漏洞库编号	CNNVD-202307-1721
CNVD编号	
漏洞可利用性	3.9
存在主机	10.20.198.38
简单描述	OpenSSH 9.3p2之前版本存在安全漏洞
详细描述	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。
修补建议	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
参考网址	
漏洞安全性	

【3】ICMP权限许可和访问控制漏洞CVE-1999-0524

漏洞编号	001E93A6
漏洞类型	CGI类
危险级别	低危险
影响平台	所有系统
CVSS分值	2.1
bugtraq编号	
CVE编号	CVE-1999-0524
CNCVE编号	CNCVE-19990524
国家漏洞库编号	CNNVD-199708-003
CNVD编号	
漏洞可利用性	3.9
存在主机	10.20.198.38
简单描述	ICMP权限许可和访问控制漏洞
详细描述	ICMP信息如netmask和timestamp允许任意主机访问。
修补建议	配置防火墙或过滤路由器以阻止传出的ICMP数据包。阻止类型13或14和/或代码0的ICMP数据包
参考网址	
漏洞安全性	

【4】检测到目标主机SSH服务正在运行

漏洞编号	0x0013034A
漏洞类型	信息收集类

危险级别	信息
影响平台	
CVSS分值	0.0
bugtraq编号	
CVE编号	
CNCVE编号	
国家漏洞库编号	
CNVD编号	
漏洞可利用性	
存在主机	10.20.198.38
简单描述	SSH 为建立在应用层和传输层基础上的安全协议
详细描述	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。利用 SSH 协议可以有效防止远程管理过程中的信息泄露问题。
修补建议	信息收集，无需修复
参考网址	
漏洞安全性	

【5】目标主机SSH服务协议版本可列取

漏洞编号	0x1ebb5c
漏洞类型	OpenSSH
危险级别	信息
影响平台	SSH
CVSS分值	0.0
bugtraq编号	
CVE编号	
CNCVE编号	
国家漏洞库编号	
CNVD编号	
漏洞可利用性	0
存在主机	10.20.198.38
简单描述	(使用非授权扫描可能存在误报)目标主机SSH服务协议版本可列取
详细描述	SSH协议版本泄露通常会给不法分子进一步渗透提供辅助信息。
修补建议	可以通过修改配置屏蔽SSH的banner信息。
参考网址	
漏洞安全性	

【6】目标主机SSH服务加密算法可列取

漏洞编号	0x1ebb5d
漏洞类型	OpenSSH
危险级别	信息
影响平台	SSH
CVSS分值	0.0
bugtraq编号	
CVE编号	
CNCVE编号	
国家漏洞库编号	
CNVD编号	
漏洞可利用性	0
存在主机	10.20.198.38
简单描述	(使用非授权扫描可能存在误报)目标主机SSH服务加密算法可列取
详细描述	SSH加密算法泄露通常会给不法分子进一步渗透提供辅助信息。
修补建议	可以通过修改配置屏蔽SSH的banner信息。
参考网址	
漏洞安全性	

【7】Traceroute探测信息

漏洞编号	0x1ebc5e

漏洞类型	信息收集类
危险级别	信息
影响平台	Traceroute
CVSS分值	0.0
bugtraq编号	
CVE编号	
CNCVE编号	
国家漏洞库编号	
CNVD编号	
漏洞可利用性	0
存在主机	10.20.198.38
简单描述	目标主机允许Traceroute探测
详细描述	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。
修补建议	信息收集，无需修复
参考网址	
漏洞安全性	

【8】探测到Openssh版本信息

漏洞编号	0xb2d3b141
漏洞类型	信息收集类
危险级别	信息
影响平台	
CVSS分值	0.0
bugtraq编号	
CVE编号	
CNCVE编号	
国家漏洞库编号	
CNVD编号	
漏洞可利用性	0
存在主机	10.20.198.38
简单描述	OpenSSH 是 SSH （Secure SHell） 协议的免费开源实现。
详细描述	OpenSSH 是 SSH （Secure SHell） 协议的免费开源实现。SSH协议族可以用来进行远程控制， 或在计算机之间传送文件。OpenSSH提供了服务端后台程序和客户端工具， 用来加密远程控制和文件传输过程中的数据。
修补建议	信息收集，无需修复
参考网址	
漏洞安全性	