CSAP_SA_M是否涉及“CVE-2020-15778”“CVE-2023-38408”“CVE-2023-28531”漏洞

漏洞相关 **孔凡安** 2023-11-20 发表

问题描述

CSAP_SA_M是否涉及“CVE-2020-15778”“CVE-2023-38408”“CVE-2023-28531”漏洞

详细描述	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 9.3p2及之前版本中的scp的scp.c文件存在命令注入漏洞。该漏洞源于外部输入数据构造可执行命令过程中，网络系统或产品未正确过滤其中的特殊元素。攻击者可利用该漏洞执行非法命令。 参考链接：https://github.com/cpandya2909/CVE-2020-15778/
解决办法	厂商补丁： 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/ 临时缓解措施： 可以禁用scp，改用rsync等缓解风险（可能会导致小文件机器内拷贝变慢）
威胁分值	7.8
危险插件	否
发现日期	2020-07-24
CVE编号	CVE-2020-15778
CNNVD编号	CNNVD-202007-1519
CNCVE编号	CNCVE-202015778
CVSS评分	6.8
CNVD编号	CNVD-2020-42668

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。
解决办法	厂商补丁： 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
威胁分值	9.8
危险插件	否
发现日期	2022-03-13
CVE编号	CVE-2023-38408
CNNVD编号	CNNVD-202307-1721
CNCVE编号	CNCVE-202338408

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 8.9版本至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，会导致忽略每次转发的目标约束。
解决办法	厂商补丁： 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
威胁分值	9.8
危险插件	否
发现日期	2023-03-17
CVE编号	CVE-2023-28531
CNNVD编号	CNNVD-202303-1391
CNCVE编号	CNCVE-202328531

解决方法

1. CVE-2020-15778：https://zhiliao.h3c.com/Theme/details/164292
2. CVE-2023-38408：1804P11已解决
3. CVE-2023-28531：E1804P09已解决