CSAP-ESM-AV终端杀毒是否涉及OpenSSH 信息泄露漏洞(CVE-2020-14145、CVE-2018-15919)

漏洞相关 **彭钦** 2023-03-13 发表

漏洞相关信息

漏洞编号： CVE-2020-14145、CVE-2018-15919
漏洞名称： OpenSSH 信息泄露漏洞
产品型号及版本： CSAP-ESM-AV

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8.4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。

OpenSSH（OpenBSD Secure Shell）是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。 OpenSSH 7.8及之前版本，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。

漏洞解决方案

该漏洞为ssh漏洞，即系统本身的漏洞，而非产品漏洞（CSAP-ESM-AV部署在centos系统内docker上）。ssh服务漏洞可以通过关闭ssh服务或者修改端口来规避。