CSAP-ESM-AV终端杀毒是否涉及Diffie-Hellman Key Agreement Protocol 资源管理错误漏洞(CVE-2002-20001)(原理扫描)

漏洞相关 **彭钦** 2023-03-13 发表

漏洞相关信息

漏洞编号： CVE-2002-20001

漏洞名称： Diffie-Hellman Key Agreement Protocol 资源管理错误漏洞

产品型号及版本： CSAP-ESM-AV

漏洞描述

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。

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。