关于Diffie-Hellman Key Agreement Protocol 资源管理错误漏洞的说明（CVE-2002-20001）

堡垒机 zhiliao_StGbE7 2022-12-19 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： 产品型号： CSAP-SA-V 软件版本： E1710P02；SecPath A2000-V(二代) 软件版本：ESS 6112P17

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

对于堡垒机：需将界面系统设置-资产-访问设置-禁止DHE密钥交换配置为“是”，8022端口默认关闭DHE算法，修复该漏洞后，SSH及文件传输客户端必须支持ECDH算法才能正常使用。
综合日志审计平台不涉及。