【漏洞修复】(CVE-2002-20001)Diffie-Hellman Key Agreement Protocol 资源管理错误漏洞

漏洞相关 孔德飞 2022-06-23 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： 所有comwareV7设备

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

通过命令只选择ecdh相关算法，不使用dh相关算法

ssh2 algorithm key-exchange ecdh-sha2-nistp256 ecdh-sha2-nistp384

并且要同时参考如下案例，新进ssl server policy并且将其中的DHE算法取消

https://zhiliao.h3c.com/Theme/details/206865