Comware V7防火墙、IPS、负载均衡 Diffie-Hellman Key Agreement Protocol 资源管理错误漏洞 （CVE-2002-20001）

漏洞相关 刘昆 2022-06-24 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Comware V7版本

漏洞描述

漏洞信息详情

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

CNNVD编号：CNNVD-202111-1084

危害等级： 高危

CVE编号： CVE-2002-20001

漏洞类型： 资源管理错误

发布时间： 2021-11-11

威胁类型： 远程

更新时间： 2022-02-23

厂　　商：

漏洞来源：

漏洞简介

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。

漏洞公告

目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：

https://github.com/Balasys/dheater。

漏洞解决方案

1、 漏洞根因为ssl使用的算法本身存在的漏洞，使用相关算法就会扫描出响应漏洞

2、 规避方法为通过配置整改禁用相关算法（默认支持），在SSL server policy中禁用DHE算法即可（SSL serverpolicy中去除DHE算法可以参考如下链接 https://zhiliao.h3c.com/Theme/details/162132 ）