

# 知 Waf是否涉及(CVE-2002-20001)Diffie-Hellman Key Agreement Protocol 资源管理错误漏洞

漏洞相关 李瑞 2022-08-29 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: 三代waf

## 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

3代wafR6203P14及之前版本涉及该漏洞，升级到R6203P15及更新版本解决该漏洞。

