TLS protocol中间人攻击漏洞(CVE-2015-4000)

漏洞相关 王奎银 2022-01-07 发表

漏洞相关信息

漏洞编号： CVE-2015-4000
漏洞名称： TLS protocol中间人攻击漏洞(CVE-2015-4000)
产品型号及版本： 防火墙、负载均衡、入侵防御

漏洞描述

TLS协议1.2及之前版本中存在安全漏洞，该漏洞源于当服务器启用DHE_EXPORT密码套件时，程序没有正确传递DHE_EXPORT选项。攻击者可通过重写ClientHello（使用DHE_EXPORT取代DHE），然后重写ServerHello（使用DHE取代DHE_EXPORT），利用该漏洞实施中间人攻击和cipher-downgrade攻击。

漏洞解决方案

升级2021年年度版本或更新版本后，参照SSL/TLS 受诫礼(BAR-MITZVAH)攻击漏洞(CVE-2015-2808)解决方法进行修复（链接如下：https://zhiliao.h3c.com/Theme/details/130547 ），其中加密套件禁用如下三种：

exp_rsa_rc2_md5

exp_rsa_rc4_md5

exp_rsa_des_cbc_sha