支持SSL中等强度密码套件

漏洞相关 王奎银 2022-01-07 发表

漏洞相关信息

漏洞编号： wu

漏洞名称： 支持SSL中等强度密码套件

产品型号及版本： 防火墙、负载均衡、入侵防御

漏洞描述

远程主机支持的SSL加密算法提供了中等强度的加密算法，目前，使用密钥长度大于等于56bits并且小于112bits的算法都被认为是中等强度的加密算法。

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两种：

rsa_aes_256_cbc_sha

dhe_rsa_aes_256_cbc_sha