防火墙是否涉及SSL/TLS EXPORT_RSA < = 支持的 512 位密码套件 （FREAK）漏洞

漏洞相关 王奎银 2022-02-23 发表

漏洞相关信息

漏洞编号： 无

漏洞名称： SSL/TLS EXPORT_RSA < = 支持的 512 位密码套件 （FREAK）

产品型号及版本： 防火墙、负载均衡、入侵防御

漏洞描述

远程主机支持密钥小于或等于 512 位的EXPORT_RSA密码套件。攻击者可以在短时间内分解 512 位 RSA 模量。 中间人攻击者可能能够将会话降级为使用EXPORT_RSA密码套件（例如 CVE-2015-0204 ）。因此，建议删除对弱密码套件的支持。

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_des_cbc_sha

exp_rsa_rc2_md5

exp_rsa_rc4_md5