SSL支持RC4加密算法【POC】

漏洞相关 王奎银 2022-01-07 发表

漏洞相关信息

漏洞编号： 无
漏洞名称： SSL支持RC4加密算法【POC】
产品型号及版本： 防火墙、负载均衡、入侵防御

漏洞描述

安全套接层（Secure Sockets Layer，SSL），一种安全协议，是网景公司（Netscape）在推出Web浏览器首版的同时提出的，目的是为网络通信提供安全及数据完整性。SSL在传输层对网络连接进行加密。传输层安全（Transport Layer Security），IETF对SSL协议标准化（RFC 2246）后的产物，与SSL 3.0差异很小。
SSL/TLS内使用的RC4算法存在单字节偏差安全漏洞，可允许远程攻击者通过分析统计使用的大量相同的明文会话，利用此漏洞恢复纯文本信息。

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_rc4_md5

rsa_rc4_128_md5

rsa_rc4_128_sha