OpenSSL中间人安全绕过漏洞（CNVD-2015-00215）(CVE-2015-0204)

漏洞相关 王奎银 2022-01-07 发表

漏洞相关信息

漏洞编号： CVE-2015-0204

漏洞名称： OpenSSL中间人安全绕过漏洞（CNVD-2015-00215）(CVE-2015-0204)

产品型号及版本： 防火墙、负载均衡、入侵防御

漏洞描述

FREAK攻击全称为Factoring RSA Export Keys，即分解RSA导出密钥攻击。 该攻击利用废弃许久的“出口级”加密套件，目前仍有很多SSL/TLS服务器端及客户端仍然支持此类连接。 利用该漏洞攻击者可以劫持存在漏洞的客户端与存在漏洞的服务端之间的会话，从而进行中间人攻击。

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_des_cbc_sha

exp_rsa_rc2_md5

exp_rsa_rc4_md5