支持SSL弱密码套件

漏洞相关 王奎银 2022-01-07 发表

漏洞相关信息

漏洞编号： 无

漏洞名称： 支持SSL弱密码套件

产品型号及版本： 防火墙、负载均衡、入侵防御

漏洞描述

远程主机支持使用弱加密甚至未加密的SSL口令。

注意：如果攻击者在同一物理网络中，这很容易被利用。

漏洞解决方案

1. 关闭ssl3.0：

[H3C] ssl version ssl3.0 disable

2. 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：exp_rsa_rc4_md5