H3C F1050 扫描漏洞 Network Time Protocol (NTP) Mode 6 Scanner

证书 David1 2020-04-26 发表

组网及说明

无

问题描述

无

过程分析

设备在漏洞检查中涉及“Network Time Protocol (NTP) Mode 6 Scanner” 该漏洞是NTP本身存在漏洞，描述如下： The remote NTP server responds to mode 6 queries. Devices that respond to these queries have the potential to be used in NTP amplification attacks. An unauthenticated, remote attacker could potentially exploit this, via a specially crafted mode 6 query, to cause a reflected denial of service condition. 即ntp server存在被未知网络攻击者利用并放大其响应mode 6查询时的潜在风险。

解决方法

在设备上可以通过如下两种方式配规避： 1、配置ntp-service access { peer | query | server | synchronization } acl-number 举个例子， 服务器为A，客户端为B,C,D， 如果允许B,C,D都对服务器具有时间同步、控制查询权限，可以配置 ntp-service access peer acl 2000， acl 2000 permit B,C,D 需要将配置了从服务器A同步的所有合法客户端设备B,C,D,E,F…… 全部加入acl规并允许其对server进行访问，其他所有ip均无法进行操作 权限等级有4种，分别对应peer、server、synchronization、query。 按客户需要自己配置