某局点 CR16010H-FA 涉及NTP mode 6漏洞

NTP 林宇阳 2023-01-17 发表

组网及说明

本案例涉及版本范围：comware V7 高端路由器 R82XX（含）之前版本

问题描述

客户在网有多台CR16K-F系列设备，第三方漏扫发现设备会响应NTP mode 6查询报文，因此判断设备存在“网络时间协议 (NTP)模式6(DOS)”漏洞。

漏洞影响：网络时间协议 （NTP）响应模式 6 查询，可导致拒绝服务情况。

利用此漏洞可远程NTP服务器响应模式6查询。响应这些查询的设备有可能用于NTP放大攻击。未经身份验证的远程攻击者可能通过精心设计的模式6查询利用此漏洞，导致反映的拒绝服务情况。

过程分析

我司comware系统缺省响应NTP mode 6查询，因此在收到mode 6 query报文后，就会回复响应报文，即被第三方漏扫设备判断涉及漏洞。

而我司设备NTP功能不支持mode 6报文的settrap和writeclock功能，因此不涉及如“CVE-2016-9310”等需要这些功能的漏洞

解决方法

前述版本范围设备避免mode6查询响应的方式只有提前阻断NTP mode 6 query报文上送到CPU处理：

1、ntp-service peer acl xxx

2、在设备全局或与扫描设备连接接口应用packet-filter过滤目的地址为本机的ntp协议报文（deny前先permit允许同步NTP时间的IP地址）

R83XX以上版本支持“ntp-service noquery enable”命令关闭NTP mode 6/7 报文查询响应，可以避免被扫描检查到。