关于防火墙、IPS和LB产品是否涉及NTP Mode 6 查询漏洞/检测漏洞

漏洞相关 **杨雅伦** 2023-04-20 发表

漏洞相关信息

漏洞编号： 无编号
漏洞名称： NTP Mode 6 查询漏洞/检测漏洞
产品型号及版本： COMWARE V7

漏洞描述

NTP Mode 6 查询漏洞
远程NTP服务允许Mode 6查询，这些查询有可能用于NTP扩展
攻击。未经身份验证的远程攻击者可能通过特制 Mode 6查询，造成拒绝服务条件。
https://ntpscan.shadowserver.org

针对mode 6漏洞
一般情况下，存在该漏洞对设备正常运行是没有任何影响的；
但当有攻击者时，攻击者可能：
a. 通过发送大量ntp mode6请求报文，造成NTPD忙碌，并不会影响整机或其他业务；
b. 通过mode 6采集一些设备基本信息（系统版本，NTP同步状态，层级，leap，rootdisp等信息）
“ntp-service noquery enable”

漏洞解决方案

涉及该漏洞，规避方法为：通过ACL限制NTP service规避