防火墙涉及ntp相关漏洞（Mode 6/7）

漏洞相关 **孔凡安** 2022-04-22 发表

问题描述

Mode 6/7是NTP协议要求的基本功能，但可能存在被恶意利用的风险，所以有如下相关漏洞；

【Mode 6/ 7 功能相关漏洞】

CVE-2016-9310 The control mode (mode 6) functionality in ntpd in NTP before 4.2.8p9 allows remote attackers to set or unset traps via a crafted control mode packet.

CVE-2016-7434 The read_mru_list function in NTP before 4.2.8p9 allows remote attackers to cause a denial of service (crash) via a crafted mrulist query.

CVE-2016-2516 NTP before 4.2.8p7 and 4.3.x before 4.3.92, when mode7 is enabled, allows remote attackers to cause a denial of service (ntpd abort) by using the same IP address multiple times in an unconfig directive.

CVE-2013-5211 The monlist feature in ntp_request.c in ntpd in NTP before 4.2.7p26 allows remote attackers to cause a denial of service (traffic amplification) via forged (1) REQ_MON_GETLIST or (2) REQ_MON_GETLIST_1 requests, as exploited in the wild in December 2013.

CVE-2009-3563 ntp_request.c in ntpd in NTP before 4.2.4p8, and 4.2.5, allows remote attackers to cause a denial of service (CPU and bandwidth consumption) by using MODE_PRIVATE to send a spoofed (1) request or (2) response packet that triggers a continuous exchange of MODE_PRIVATE error responses between two NTP daemons.

解决方法

【规避方式】

（沿用之前的mode6/7漏洞解决方式）

a. 如果目标设备只作为NTP Server（不从外部同步时间）：

配置ntp-service synchronization acl xxx可以关闭掉mode6/7功能。

（只能在仅作为server的设备上使用，在NTP客户端使用会导致无法从外部同步时间）

b. 如果目标设备需要作为NTP Client（从外部同步时间）：

在目标设备上配置ntp-service peer acl xxx，

将下游ntp client（从目标设备同步时间）和上游ntp server（向目标设备同时时间）的地址 加入ACL xxx的permit规则，其他ntp报文拒收。

————拦截非信任来源的报文