MSR系列路由器是否涉及CVE-1999-0524漏洞

软件相关 朱玉广 2018-10-15 发表

问题描述

MSR系列路由器是否涉及CVE-1999-0524漏洞？如何解决？

解决方法

CVE-1999-0524:
ICMP information such as (1) netmask and (2) timestamp is allowed from arbitrary hosts.
ICMP网络掩码请求响应漏洞（CVE-1999-0524）：
ICMP信息如netmask和timestamp允许任意主机访问。
其实这并算不上一个漏洞，V5/V7所有的分支都是默认能响应掩码请求，算是个正常功能 。
如果一定要解决掉，可以用下面这个acl配置来过滤接口入报文，硬转产品应该都有命令来过滤inbound报文
acl number 3000
rule 0 deny icmp icmp-type 17
或者用packet-filter来匹配

MSR等软转设备
可以全局配置
traffic classifier aa operator and
if-match acl 3000
#
traffic behavior be_aa
filter deny
#
qos policy aa
classifier aa behavior be_aa
#
qos apply policy aa global inbound
#
acl advanced 3000
rule 0 permit icmp icmp-type 17
#