V5/V7相关SSH漏洞及解决办法

SSH 加密引擎 **曾嘉明** 2019-09-10 发表

问题描述

CVE-1999-0524
CVE-2008-5161
CVE-2018-15473

解决方法

【CVE-1999-0524】V7涉及，但是未提单修改，使用配置规避
Comware V5：涉及，可通过ACL或者Packet-Filter来规避
Comware V7：同V5
SR88:V5 B106D626 版本解决,问题单201608100213

V5/V7所有的分支都是默认能响应掩码请求，应该是个正常功能
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
88

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 deny icmp icmp-type 17
#

【CVE-2008-5161】 V7不涉及
经分析，此问题有三种解决办法：
1、增加CTR模式的加密算法，且优先级比CBC模式算法高
2、如果是基于OpenSSH的，可以升级OpenSSH的版本，根据OpenSSH的官方文档，从5.2版本开始，已解决该问题
3、对于非基于OpenSSH的，可以根据开源的修改实现来修补该漏洞（V5采用此方法来修改）

ComwareV5涉及
ComwareV7基于OpenSSH 5.3p1，因此V7不涉及
SMB: 使用V5平台的产品，涉及
2013：不涉及
VCX：涉及
iMC：不涉及
Secblade SSL VPN：不涉及

V3/V5的SSH均受影响; 但V3和HP确认，不需要修改；只有还在维护期的Secblade需要响应SSRT问题，但本问题Secblade SSL VPN不涉及

CVE-2018-15473 (这个在最新的R7125P02已经解决了，升级版本吧)