高端路由器是否涉及CVE-2008-5161漏洞

软件升级/降级 **王科** 2023-04-04 发表

问题描述

SSH连接建立过程中，使用CBC 模式加密算法，可能导致密文泄露，进而导致连接断开

VE-2008-5161

解决方法

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

V5路由器：无法通过配置解决或者规避。
因CBC算法破解风险较大，SSH服务不应该再支持该算法。
该漏洞常规检测手段为：与被检测设备进行SSH协商交互，获取被检测设备的算法列表，检查是否支持CBC算法。
除少数安全产品提过特殊需求,大部分设备均默认支持CBC算法。
通过配置取消CBC算法后，我司设备对外SSH协商报文，不会携带CBC算法。

ComwareV5不支持修改ssh算法策略，且支持CBC算法，除非关闭ssh服务
<SR88>ssh2 10.1.1.1 prefer-ctos-cipher ?
  3des   3DES-CBC encryption algorithm
  aes128 AES128-CBC encryption algorithm
  des   DES-CBC encryption algorithm