CVE-70658和71049配置层面解决方法

攻击检测与防范 **陆世叶** 2019-05-24 发表

问题描述

CVE-70658和71049配置层面解决方法

解决方法

漏洞名称	SSH弱MAC算法启用

1、 SSH Weak Algorithms Enabled

这个漏洞不要使用MD5和96位的MAC算法就可以规避，在用户视图下配置以下命令可以规避，

ssh2 algorithm mac { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** | **sm3** } *

MD5 和 md5-96 sha1-96 都不用.

2、 SSH Server CBC Mode Cipher Enabled

这个配置不要使用CBC的加密算法就可以规避。

ssh2 algorithm cipher { 3des-cbc | aes128-cbc | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | aes256-cbc | **aes256-ctr** | **aes256-gcm** | des-cbc } *

标粗的可以用， CBC 的都不用就可以了