启用 SSH 弱密钥交换算法

漏洞相关 **王奎银** 2022-01-07 发表

漏洞相关信息

漏洞编号： 无

漏洞名称： 启用 SSH 弱密钥交换算法

产品型号及版本： 防火墙、负载均衡、入侵防御

漏洞描述

目标主机SSH服务存在RC4、CBC或None弱加密算法，SSH弱加密算法可能会导致认证信息被窃听、破解。

漏洞解决方案

关闭cbc类型的算法。如下所示，选择不含cbc类型的算法：

```
[H3C]ssh2 algorithm cipher ?
  3des-cbc    3DES-CBC
  aes128-cbc  AES128-CBC
  aes128-ctr  AES128-CTR
  aes128-gcm  AES128_GCM
  aes192-ctr  AES192-CTR
  aes256-cbc  AES256-CBC
  aes256-ctr  AES256-CTR
  aes256-gcm  AES256_GCM
 des-cbc     DES-CBC
```