



SSH弱MAC算法启用

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：SSH弱MAC算法启用

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MD5、96位MAC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md5和96位的mac算法。如下所示，选择不含md5和96位的mac算法：

```
[H3C]ssh2 algorithm mac ?
```

```
md5    HMAC-MD5
```

```
md5-96 HMAC-MD5-96
```

```
sha1   HMAC-SHA1
```

```
sha1-96 HMAC-SHA1-96
```

```
sha2-256 HMAC-SHA2-256
```

```
sha2-512 HMAC-SHA2-512
```

