

# 知 MSR 和SR6600是否涉及1./ NTP Mode 6 Scanner; 2./ SSH Server CBC Mode Ciphers Enabled; 3./SSH Weak MAC Algorithms Enabled漏洞?

攻击防范及检测 朱玉广 2018-07-12 发表

## 问题描述

MSR G2是否涉及:

- 1./ NTP Mode 6 Scanner;
- 2./ SSH Server CBC Mode Ciphers Enabled;
- 3./SSH Weak MAC Algorithms Enabled漏洞?

## 解决方法

1、NTP Mode 6 Scanner, 路由器V5 V7不涉及该问题, 因为我们没有支持过对应的CVE ID, 不会触发该问题。

2、SSH Weak MAC Algorithms Enabled, V5不涉及; V7, 仅B70及之后版本涉及, 从反馈的版本看, 现场的V7版本包含B49、B59、B64, 无B70的版本, 不涉及该问题, 即使后续有用到B70的版本, 可以通过命令行规避, 命令行如下:

```
[CE_2]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  选择后面的强算法规避
```

3、SSH Server CBC Mode Ciphers Enabled, V7不涉及; V5需要升级版本。

MSR升级至R2514P12及之后版本可以解决, SR6600升级至R3303P12及之后版本可以解决