H3C Comware V7 平台交换机关于 SSL/TLS 服务器瞬时 Diffie-Hellman 公共密钥过弱漏洞规避方法

配置优化 攻击检测与防范 软件问题 产品特性 丁犁 2022-09-30 发表

问题描述

关于第三方安全扫描工具，可能发现 H3C Comware V7 平台交换机存在“SSL/TLS 服务器瞬时 Diffie-Hellman 公共密钥过弱”漏洞告警提示。

过程分析

该漏洞提示表示：相关被扫描的设备SSH服务存在RC4、CBC或None 弱加密算法。因此，可根据实际设备的加密方式，不启用相关算法即可规避相关漏洞提示告警。

解决方法

Comware V7平台 S10500系列交换机举例：

第一步：查看交换机SSH可采用哪些加密方式：

[S10508]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

其中，红色加密方式，为弱加密算法。

第二步：不使能红色弱加密算法，仅使能强加密算法（上面黑色算法）方式：

[S10508] ssh2 algorithm cipher aes128-ctr aes128-gcm aes192-ctr aes256-ctr aes256-gcm

第三步：重启SSH服务

[S10508] undo ssh server enable

[S10508-V-1] ssh server enable

采用上述三步操作后，相关漏洞即可规避解决。