

知 关于H3C AR46系列路由器ERPU使用CMW3.4 R0201P07版本导致RSA密钥丢失问题的预警公告

冷志宇 2007-07-17 发表

关于H3C AR46系列路由器ERPU使用CMW3.4 R0201P07版本导致RSA密钥丢失问题的预警公告

【问题描述】

在H3C AR46-ERPU设备上，如果启用了SSH，IKE RSA数字签名方式进行协商或SSL的相关应用，因CMW3.4 R0201P07的版本Bug，之前的版本升级到此版本或此版本升级到后续版本时，会出现RSA密钥丢失，附带造成PKI本地证书丢失问题。

【问题现象】

升级至问题版本，或由问题版本升级至其他版本后，原有正常SSH1.5，IKE或SSL业务协商失败；

执行display rsa local-key-pair public

提示密钥不存在；

执行display pki certificate local domain on

提示：No local certificate!

【问题出现条件】

1. 问题在版本切换时发生（升级至问题版本或由问题版本升级至其他版本）。
2. 该问题仅在ERPU设备上存在。
3. 该问题仅在配置了SSH，IKE，SSL业务时出现。

【解决措施】

1. 如原始版本为非问题版本升级至问题版本，需要重新升级至非问题版本即可恢复。
2. 如原始版本为问题版本，需要升级至非问题版本，并使用命令重新生成RSA密钥，重新申请PKI本地证书。生成方法和业务开通时RSA密钥生成、PKI申请证书的方法一致。