A2000-G系列（二代）是否涉及使用弱哈希算法签名的 SSL 证书漏洞

漏洞相关 王奎银 2022-02-23 发表

漏洞相关信息

漏洞编号： 无
漏洞名称： 使用弱哈希算法签名的 SSL 证书
产品型号及版本： A2000-G系列（二代）

漏洞描述

远程服务使用已使用加密弱哈希算法（例如 MD2、MD4、MD5、or SHA1）签名的 SSL 证书链。已知这些签名算法容易受到碰撞攻击。攻击者可以利用此漏洞生成具有相同数字签名的另一个证书，从而允许攻击者伪装成受影响的服务。请注意，此 plugin 将所有使用 SHA-1 签名且在 2017 年 1 月 1 日之后过期的 SSL 证书链报告为易受攻击。这符合谷歌逐渐淘汰SHA-1加密哈希算法。请注意，链中在 Nessus CA 数据库 （known_CA.inc） 中附带的证书已被忽略。

漏洞解决方案

客户购买受信任的证书上传到堡垒机中解决问题