A2000-G系列（二代）是否涉及不能信任 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： 不能信任 SSL 证书
产品型号及版本： A2000-G系列（二代）

漏洞描述

服务器的 X.509 证书不可信。这种情况可以通过三种不同的方式发生，其中信任链可能会被破坏，如下所述： - 首先，服务器发送的证书链的顶部可能不是来自已知的公共证书颁发机构。当链的顶部是无法识别的自签名证书时，或者当缺少将 证书链的顶部连接到已知的公共证书颁发机构的中间证书时，可能会发生这种情况。当扫描发生在证书的"notBefore"日期之前或证书的"notAfter"日期之一之后时，可能会发生这种情况。错误签名可以通过让具有错误签名的证书由其颁发者重新签名来修复。无法验证的签名是证书颁发者使用 Nessus 不支持或无法识别的签名算法的结果。如果 远程主机是生产中的公共主机，则链中的任何中断都会使用户更难以验证 Web 服务器的真实性和身份。这样可以更轻松地对远程主机执行中间人攻击。

漏洞解决方案

客户或许受信任的证书上传到堡垒机中解决