漏洞举证报告

导出维度: 按业务名称导出

导出时间: 2024-08-29 18:07

目录

一、漏洞举证详情

1.1 新体检服务器(检后)

1.1.1 终端服务未使用网络级别身份验证（NLA） 建议修复

漏洞等级：	中危
漏洞类型：	系统漏洞
风险描述：	远程终端服务未配置为仅使用网络级别身份验证（NLA）。 NLA使用凭据安全支持提供程序（CredSSP）协议通过TLS / SSL或Kerberos机制执行强大的服务器身份验证，从而防止中间人攻击。除了改善身份验证外，NLA还可以通过在建立完整的RDP连接之前完成用户身份验证来帮助保护远程计算机免受恶意用户和软件的侵害。
风险影响：	1.未使用该认证的远程主机受攻击的风险等级高。
解决方案：	参见《终端服务未使用网络级别身份验证（NLA）-修复方案》

资产IP： 10.69.255.13

风险举证：

端口	资产
3389	10.69.255.13
Sangfor was able to negotiate non-NLA (Network Level Authentication) security.	

1.1.2 SSL 证书到期 建议修复

漏洞等级：	中危
漏洞类型：	系统漏洞
风险描述：	此插件检查目标上与启用了 SSL 的服务关联的证书的到期日期，并报告是否任何证书已到期。
风险影响：	1.SSL 的服务关联的证书的到期日期
解决方案：	1.请购买或生成新的 SSL 证书以替换现有证书。

资产IP： 10.69.255.13

风险举证：

端口	资产
443	10.69.255.13
当前证书过期时间为2024-07-29 23:59:59	