

|  |  |
| --- | --- |
| 文档编号 | Hypdncy-DW-0707 |
| 日期 | 2021-07-07 |

|  |
| --- |
| 懂王  主机扫描报告 |

|  |
| --- |
| **Copyright (c) 2020 Hypdncy** |
| **版权所有，未经授权，严禁复制、编辑和传播** |

* 适用性声明
* 版权声明

Copyright (c) 2020 Hypdncy。

* 版本变更记录

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本号** | **拟制／修改日期** | **拟制／修改人** | **修改记录** | **批准人** |
| V1 | 2020-01-01 | Hypdncy | 创建文档 | 懂王 |

目录

[一. 懂 3](#_Toc72775988)

[二. 的 3](#_Toc72775989)

[三. 都 3](#_Toc72775990)

[四. 懂 3](#_Toc72775991)

1. 懂
2. 的

主机扫描限定于以下对象：

|  |  |  |
| --- | --- | --- |
| 序号 | 测试对象 | 对象名称 |
| 1 | 222.222.222.91 | HIS系统 |
| 2 | 222.222.222.92 | HIS系统 |
| 3 | 222.222.100.5 | PACS系统 |
| 4 | 222.222.100.6 | PACS系统 |
| 5 | 222.222.222.61 | LIS系统 |
| 6 | 222.222.222.62 | LIS系统 |
| 7 | 222.222.222.40 | 医保前置机 |
| 8 | 10.10.14.23 | 微信缴费 |
| 9 | 222.222.222.41 | 体检系统 |
| 10 | 222.222.222.50 | OA系统 |
| 11 | 10.10.14.62 | 康软体检，LIS服务器 |
| 12 | 10.10.14.63 | 康软体检，LIS服务器 |
| 13 | 10.10.14.64 | 康软体检，LIS服务器 |
| 14 | 10.10.14.65 | 康软体检，LIS服务器 |
| 15 | 10.10.14.67 | 互联网医保前置机 |
| 16 | 10.10.14.54 | 院感系统 |
| 17 | 10.10.14.57 | 医保移动支付前置机 |
| 18 | 47.111.106.89 | 门户网站 |
| 19 | 10.10.14.39 | 国药SPD前置机 |
| 20 | 222.222.222.48 | 信息发布服务器 |
| 21 | 10.10.14.78 | 医保分值付费服务器 |
| 22 | 10.10.14.69 | 广州市全民健康档案前置机 |
| 23 | 10.10.14.74 | 移动护理前置 |
| 24 | 10.10.14.75 | 应用服务器 |
| 25 | 10.10.14.76 | 临床路径服务器 |
| 26 | 10.10.14.77 | 移动护理数据服务器 |
| 27 | 10.10.14.83 | 电子病历360视图服务器 |
| 28 | 10.10.14.84 | 电子病历361视图服务器 |
| 29 | 10.10.14.85 | 电子病历362视图服务器 |
| 30 | 10.10.14.86 | 电子病历363视图服务器 |
| 31 | 10.10.14.87 | 电子病历364视图服务器 |
| 32 | 10.10.14.88 | 电子病历365视图服务器 |
| 33 | 10.10.14.89 | 电子病历应用服务器 |
| 34 | 10.10.14.90 | 电子病历应用服务器 |
| 35 | 10.10.14.91 | 电子病历应用服务器 |
| 36 | 10.10.14.92 | 电子病历应用服务器 |
| 37 | 10.10.14.93 | 电子病历应用服务器 |
| 38 | 10.10.14.94 | 电子病历应用服务器 |
| 39 | 10.10.14.95 | 电子病历应用服务器 |
| 40 | 10.10.14.96 | 电子病历应用服务器 |
| 41 | 10.10.14.97 | 电子病历应用服务器 |
| 42 | 10.10.14.98 | 电子病历应用服务器 |

1. 都
2. 懂

经过此次检测，共发现安全漏洞主机35个，其中紧急主机22个、高危主机2个、中危主机8个、低危主机3个。存在的安全隐患主要包括HTTP TRACE / TRAC方法未禁用、Sun ONE Application Server源泄露漏洞、当前Web Server版本厂商已不再支持等安全漏洞，可能将导致等严重危害。

* 1. 【紧急】院感系统（10.10.14.54）
     1. 【紧急】Microsoft SQL Server不支持的版本检测（远程检查）
* 漏洞描述：

根据其自我报告的版本号，不再支持在远程主机上安装Microsoft SQL Server。缺少支持意味着供应商不会发布产品的新安全修补程序。因此，它很可能包含安全漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.54 | 1433 |

* 加固建议：

升级到当前支持的Microsoft SQL Server版本。

* + 1. 【高危】SSL 2.0协议未禁用
* 漏洞描述：

远程服务使用SSL 2.0进行通信连接加密，根据公开的漏洞曝露报告，此版本的协议存在一些加密缺陷，并已废弃多年。攻击者可以利用这个漏洞发动中间人攻击或解密受此影响的客户端之间的通信内容。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.54 | 1433 |

* 加固建议：

禁用SSL 2.0，使用TLS 1.0或更高版本代替

* + 1. 【中危】SSL证书签名使用弱强度的哈希算法
* 漏洞描述：

远程服务器的SSL证书签名使用弱强度的哈希加密算法，例如MD2、MD4或者MD5。这些签名算法显示容易遭到破解。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.54 | 1433 |

* 加固建议：

联系证书认证机构发布新的证书。 如果服务器使用自签名证书，则可自己

* + 1. 【中危】允许SSL采用中强度加密
* 漏洞描述：

远程主机支持SSL使用的密码采用中强度解密，即使用的KEY解密长度至少64位，但少于112位。注意：如果攻击者在同一个物理网段，密码很容易暴露。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.54 | 1433 |
| 10.10.14.54 | 3389 |

* 加固建议：

重新设置受影响的应用程序，可能的话，避免使用中强度加密，改为强度较高的加密算法。

* + 1. 【中危】SSL证书主机名不匹配
* 漏洞描述：

SSL现有认证的commonName (CN)是供其它主机使用的。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.54 | 1433 |

* 加固建议：

为此项服务购买或生产一个合适的证书

* + 1. 【中危】SSL证书不被信任
* 漏洞描述：

此项服务的SSL证书不被信任。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.54 | 1433 |
| 10.10.14.54 | 3389 |

* 加固建议：

为此项服务购买或生成合适的证书

* + 1. 【中危】SSL自签名证书
* 漏洞描述：

服务器所使用的X.509签署的证书链不是权威的证书颁发机构所颁发的。这削弱了使用SSL的效果，因为任何人都可以建立一个中间人攻击远程主机。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.54 | 1433 |
| 10.10.14.54 | 3389 |

* 加固建议：

购买或者生成被认可的证书

* + 1. 【中危】SMB数字签名通信禁用
* 漏洞描述：

SMB 协议为 Microsoft 文件和打印共享以及许多其他网络操作（例如远程 Windows 管理）提供基础。为了防止在传输过程中修改 SMB 数据包的拦截攻击，SMB 协议支持对 SMB 数据包的数字签名。 主机禁用了SMB数字签名通信，这可能导致潜在攻击者针对SMB通信服务进行中间人攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.54 | 445 |

* 加固建议：

在本地策略中--安全选项设置如下： Microsoft 网络客户端：对通信进行数字签名（若服务器同意）（启用） Microsoft 网络服务器：对通信进行数字签名（若客户同意）（启用）

* + 1. 【中危】远程主机支持SSL RC4加密套件
* 漏洞描述：

远程主机在一个或多个支持使用RC4密码套件，RC4密码是有缺陷的生成伪随机流的字节数, 如果明文重复加密(如HTTP cookie),攻击者能够获得许多(即数以百万计)明文密文配对,攻击者可以获得密文后，对比获得明文。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.54 | 1433 |
| 10.10.14.54 | 3389 |

* 加固建议：

重新设置受影响的应用程序，可能的话，避免使用RC4密钥算法，可以考虑给浏览器或WEB服务支持的带有AES-GCM 的TLS 1.2，相关链接： http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/ http://www.imperva.com/docs/HII\_Attacking\_SSL\_when\_using\_RC4.pdf

* + 1. 【中危】SSLv3 POODLE 安全漏洞
* 漏洞描述：

支持SSLv3 协议的网站存在被中间人攻击的风险，“Poodle”攻击（全称为Padding Oracle On Downloaded Legacy Encryption）可以提取出SSL连接中的加密数据相应的明文信息。攻击者可以利用这个漏洞发动中间人攻击或解密受此影响的客户端之间的通信内容。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.54 | 1433 |

* 加固建议：

禁用SSL 3.0

* + 1. 【中危】TLS版本1.0协议检测
* 漏洞描述：

远程服务接受使用TLS 1.0加密的连接。TLS 1.0有许多密码设计缺陷。TLS 1.0的现代实现减轻了这些问题，但是像1.2和1.3这样的TLS的新版本是针对这些缺陷而设计的，应该尽可能使用。截至2020年3月31日，为TLS 1.2及更高版本启用的终结点将不再与主要web浏览器和主要供应商正常工作。PCI DSS v3.2要求在2018年6月30日之前完全禁用TLS 1.0，但POS POI终端（及其连接的SSL/TLS终端点）除外，这些终端可以被验证为不易受任何已知漏洞攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.54 | 1433 |
| 10.10.14.54 | 3389 |

* 加固建议：

启用对TLS 1.2和1.3的支持，并禁用对TLS 1.0的支持。

* + 1. 【低危】SSL证书链包含小于2048位的RSA密钥
* 漏洞描述：

远程主机发送的X.509证书中至少有一个具有短于2048位的密钥。根据证书颁发机构/浏览器（CA/B）论坛制定的行业标准，2014年1月1日之后颁发的证书必须至少为2048位。一些浏览器SSL实现可能会在2014年1月1日之后拒绝小于2048位的密钥。此外，一些SSL证书供应商可能会在2014年1月1日之前吊销小于2048位的证书。请注意，如果在2010年12月31日之前颁发RSA密钥小于2048位的根证书，Nessus将不会标记这些根证书，因为标准认为它们是免税的。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.54 | 1433 |

* 加固建议：

用长度小于2048位的RSA密钥替换链中的证书，然后重新颁发由旧证书签名的所有证书。

* 1. 【紧急】康软体检，LIS服务器（10.10.14.63）
     1. 【紧急】Microsoft SQL Server不支持的版本检测（远程检查）
* 漏洞描述：

根据其自我报告的版本号，不再支持在远程主机上安装Microsoft SQL Server。缺少支持意味着供应商不会发布产品的新安全修补程序。因此，它很可能包含安全漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.63 | 1433 |

* 加固建议：

升级到当前支持的Microsoft SQL Server版本。

* + 1. 【高危】SSL 2.0协议未禁用
* 漏洞描述：

远程服务使用SSL 2.0进行通信连接加密，根据公开的漏洞曝露报告，此版本的协议存在一些加密缺陷，并已废弃多年。攻击者可以利用这个漏洞发动中间人攻击或解密受此影响的客户端之间的通信内容。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.63 | 1433 |

* 加固建议：

禁用SSL 2.0，使用TLS 1.0或更高版本代替

* + 1. 【中危】SSL证书签名使用弱强度的哈希算法
* 漏洞描述：

远程服务器的SSL证书签名使用弱强度的哈希加密算法，例如MD2、MD4或者MD5。这些签名算法显示容易遭到破解。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.63 | 1433 |

* 加固建议：

联系证书认证机构发布新的证书。 如果服务器使用自签名证书，则可自己

* + 1. 【中危】允许SSL采用中强度加密
* 漏洞描述：

远程主机支持SSL使用的密码采用中强度解密，即使用的KEY解密长度至少64位，但少于112位。注意：如果攻击者在同一个物理网段，密码很容易暴露。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.63 | 1433 |
| 10.10.14.63 | 3389 |

* 加固建议：

重新设置受影响的应用程序，可能的话，避免使用中强度加密，改为强度较高的加密算法。

* + 1. 【中危】SSL证书主机名不匹配
* 漏洞描述：

SSL现有认证的commonName (CN)是供其它主机使用的。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.63 | 1433 |
| 10.10.14.63 | 3389 |

* 加固建议：

为此项服务购买或生产一个合适的证书

* + 1. 【中危】SSL证书不被信任
* 漏洞描述：

此项服务的SSL证书不被信任。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.63 | 1433 |
| 10.10.14.63 | 3389 |

* 加固建议：

为此项服务购买或生成合适的证书

* + 1. 【中危】SSL自签名证书
* 漏洞描述：

服务器所使用的X.509签署的证书链不是权威的证书颁发机构所颁发的。这削弱了使用SSL的效果，因为任何人都可以建立一个中间人攻击远程主机。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.63 | 1433 |
| 10.10.14.63 | 3389 |

* 加固建议：

购买或者生成被认可的证书

* + 1. 【中危】远程主机支持SSL RC4加密套件
* 漏洞描述：

远程主机在一个或多个支持使用RC4密码套件，RC4密码是有缺陷的生成伪随机流的字节数, 如果明文重复加密(如HTTP cookie),攻击者能够获得许多(即数以百万计)明文密文配对,攻击者可以获得密文后，对比获得明文。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.63 | 1433 |
| 10.10.14.63 | 3389 |

* 加固建议：

重新设置受影响的应用程序，可能的话，避免使用RC4密钥算法，可以考虑给浏览器或WEB服务支持的带有AES-GCM 的TLS 1.2，相关链接： http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/ http://www.imperva.com/docs/HII\_Attacking\_SSL\_when\_using\_RC4.pdf

* + 1. 【中危】SSLv3 POODLE 安全漏洞
* 漏洞描述：

支持SSLv3 协议的网站存在被中间人攻击的风险，“Poodle”攻击（全称为Padding Oracle On Downloaded Legacy Encryption）可以提取出SSL连接中的加密数据相应的明文信息。攻击者可以利用这个漏洞发动中间人攻击或解密受此影响的客户端之间的通信内容。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.63 | 1433 |

* 加固建议：

禁用SSL 3.0

* + 1. 【中危】TLS版本1.0协议检测
* 漏洞描述：

远程服务接受使用TLS 1.0加密的连接。TLS 1.0有许多密码设计缺陷。TLS 1.0的现代实现减轻了这些问题，但是像1.2和1.3这样的TLS的新版本是针对这些缺陷而设计的，应该尽可能使用。截至2020年3月31日，为TLS 1.2及更高版本启用的终结点将不再与主要web浏览器和主要供应商正常工作。PCI DSS v3.2要求在2018年6月30日之前完全禁用TLS 1.0，但POS POI终端（及其连接的SSL/TLS终端点）除外，这些终端可以被验证为不易受任何已知漏洞攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.63 | 1433 |
| 10.10.14.63 | 3389 |

* 加固建议：

启用对TLS 1.2和1.3的支持，并禁用对TLS 1.0的支持。

* + 1. 【低危】SSL证书链包含小于2048位的RSA密钥
* 漏洞描述：

远程主机发送的X.509证书中至少有一个具有短于2048位的密钥。根据证书颁发机构/浏览器（CA/B）论坛制定的行业标准，2014年1月1日之后颁发的证书必须至少为2048位。一些浏览器SSL实现可能会在2014年1月1日之后拒绝小于2048位的密钥。此外，一些SSL证书供应商可能会在2014年1月1日之前吊销小于2048位的证书。请注意，如果在2010年12月31日之前颁发RSA密钥小于2048位的根证书，Nessus将不会标记这些根证书，因为标准认为它们是免税的。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.63 | 1433 |

* 加固建议：

用长度小于2048位的RSA密钥替换链中的证书，然后重新颁发由旧证书签名的所有证书。

* 1. 【紧急】康软体检，LIS服务器（10.10.14.64）
     1. 【紧急】Microsoft SQL Server不支持的版本检测（远程检查）
* 漏洞描述：

根据其自我报告的版本号，不再支持在远程主机上安装Microsoft SQL Server。缺少支持意味着供应商不会发布产品的新安全修补程序。因此，它很可能包含安全漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.64 | 1433 |

* 加固建议：

升级到当前支持的Microsoft SQL Server版本。

* + 1. 【高危】SSL 2.0协议未禁用
* 漏洞描述：

远程服务使用SSL 2.0进行通信连接加密，根据公开的漏洞曝露报告，此版本的协议存在一些加密缺陷，并已废弃多年。攻击者可以利用这个漏洞发动中间人攻击或解密受此影响的客户端之间的通信内容。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.64 | 1433 |

* 加固建议：

禁用SSL 2.0，使用TLS 1.0或更高版本代替

* + 1. 【中危】SSL证书签名使用弱强度的哈希算法
* 漏洞描述：

远程服务器的SSL证书签名使用弱强度的哈希加密算法，例如MD2、MD4或者MD5。这些签名算法显示容易遭到破解。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.64 | 1433 |

* 加固建议：

联系证书认证机构发布新的证书。 如果服务器使用自签名证书，则可自己

* + 1. 【中危】允许SSL采用中强度加密
* 漏洞描述：

远程主机支持SSL使用的密码采用中强度解密，即使用的KEY解密长度至少64位，但少于112位。注意：如果攻击者在同一个物理网段，密码很容易暴露。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.64 | 1433 |
| 10.10.14.64 | 3389 |

* 加固建议：

重新设置受影响的应用程序，可能的话，避免使用中强度加密，改为强度较高的加密算法。

* + 1. 【中危】SSL证书主机名不匹配
* 漏洞描述：

SSL现有认证的commonName (CN)是供其它主机使用的。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.64 | 1433 |

* 加固建议：

为此项服务购买或生产一个合适的证书

* + 1. 【中危】SSL证书不被信任
* 漏洞描述：

此项服务的SSL证书不被信任。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.64 | 1433 |
| 10.10.14.64 | 3389 |

* 加固建议：

为此项服务购买或生成合适的证书

* + 1. 【中危】SSL自签名证书
* 漏洞描述：

服务器所使用的X.509签署的证书链不是权威的证书颁发机构所颁发的。这削弱了使用SSL的效果，因为任何人都可以建立一个中间人攻击远程主机。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.64 | 1433 |
| 10.10.14.64 | 3389 |

* 加固建议：

购买或者生成被认可的证书

* + 1. 【中危】远程主机支持SSL RC4加密套件
* 漏洞描述：

远程主机在一个或多个支持使用RC4密码套件，RC4密码是有缺陷的生成伪随机流的字节数, 如果明文重复加密(如HTTP cookie),攻击者能够获得许多(即数以百万计)明文密文配对,攻击者可以获得密文后，对比获得明文。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.64 | 1433 |
| 10.10.14.64 | 3389 |

* 加固建议：

重新设置受影响的应用程序，可能的话，避免使用RC4密钥算法，可以考虑给浏览器或WEB服务支持的带有AES-GCM 的TLS 1.2，相关链接： http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/ http://www.imperva.com/docs/HII\_Attacking\_SSL\_when\_using\_RC4.pdf

* + 1. 【中危】SSLv3 POODLE 安全漏洞
* 漏洞描述：

支持SSLv3 协议的网站存在被中间人攻击的风险，“Poodle”攻击（全称为Padding Oracle On Downloaded Legacy Encryption）可以提取出SSL连接中的加密数据相应的明文信息。攻击者可以利用这个漏洞发动中间人攻击或解密受此影响的客户端之间的通信内容。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.64 | 1433 |

* 加固建议：

禁用SSL 3.0

* + 1. 【中危】TLS版本1.0协议检测
* 漏洞描述：

远程服务接受使用TLS 1.0加密的连接。TLS 1.0有许多密码设计缺陷。TLS 1.0的现代实现减轻了这些问题，但是像1.2和1.3这样的TLS的新版本是针对这些缺陷而设计的，应该尽可能使用。截至2020年3月31日，为TLS 1.2及更高版本启用的终结点将不再与主要web浏览器和主要供应商正常工作。PCI DSS v3.2要求在2018年6月30日之前完全禁用TLS 1.0，但POS POI终端（及其连接的SSL/TLS终端点）除外，这些终端可以被验证为不易受任何已知漏洞攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.64 | 1433 |
| 10.10.14.64 | 3389 |

* 加固建议：

启用对TLS 1.2和1.3的支持，并禁用对TLS 1.0的支持。

* + 1. 【低危】SSL证书链包含小于2048位的RSA密钥
* 漏洞描述：

远程主机发送的X.509证书中至少有一个具有短于2048位的密钥。根据证书颁发机构/浏览器（CA/B）论坛制定的行业标准，2014年1月1日之后颁发的证书必须至少为2048位。一些浏览器SSL实现可能会在2014年1月1日之后拒绝小于2048位的密钥。此外，一些SSL证书供应商可能会在2014年1月1日之前吊销小于2048位的证书。请注意，如果在2010年12月31日之前颁发RSA密钥小于2048位的根证书，Nessus将不会标记这些根证书，因为标准认为它们是免税的。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.64 | 1433 |

* 加固建议：

用长度小于2048位的RSA密钥替换链中的证书，然后重新颁发由旧证书签名的所有证书。

* 1. 【紧急】移动护理前置（10.10.14.74）
     1. 【紧急】MS14-066：Schannel 远程代码执行漏洞
* 漏洞描述：

MS14-066 (CVE-2014-6321) 是存在于Microsoft的schannel.dll中的TLS堆缓冲区溢出漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.74 | 3389 |

* 加固建议：

目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： https://technet.microsoft.com/library/security/ms14-066

* + 1. 【中危】SSL证书签名使用弱强度的哈希算法
* 漏洞描述：

远程服务器的SSL证书签名使用弱强度的哈希加密算法，例如MD2、MD4或者MD5。这些签名算法显示容易遭到破解。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.74 | 3389 |

* 加固建议：

联系证书认证机构发布新的证书。 如果服务器使用自签名证书，则可自己

* + 1. 【中危】允许SSL采用中强度加密
* 漏洞描述：

远程主机支持SSL使用的密码采用中强度解密，即使用的KEY解密长度至少64位，但少于112位。注意：如果攻击者在同一个物理网段，密码很容易暴露。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.74 | 3389 |

* 加固建议：

重新设置受影响的应用程序，可能的话，避免使用中强度加密，改为强度较高的加密算法。

* + 1. 【中危】SSL证书不被信任
* 漏洞描述：

此项服务的SSL证书不被信任。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.74 | 3389 |

* 加固建议：

为此项服务购买或生成合适的证书

* + 1. 【中危】SSL自签名证书
* 漏洞描述：

服务器所使用的X.509签署的证书链不是权威的证书颁发机构所颁发的。这削弱了使用SSL的效果，因为任何人都可以建立一个中间人攻击远程主机。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.74 | 3389 |

* 加固建议：

购买或者生成被认可的证书

* + 1. 【中危】远程主机支持SSL RC4加密套件
* 漏洞描述：

远程主机在一个或多个支持使用RC4密码套件，RC4密码是有缺陷的生成伪随机流的字节数, 如果明文重复加密(如HTTP cookie),攻击者能够获得许多(即数以百万计)明文密文配对,攻击者可以获得密文后，对比获得明文。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.74 | 3389 |

* 加固建议：

重新设置受影响的应用程序，可能的话，避免使用RC4密钥算法，可以考虑给浏览器或WEB服务支持的带有AES-GCM 的TLS 1.2，相关链接： http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/ http://www.imperva.com/docs/HII\_Attacking\_SSL\_when\_using\_RC4.pdf

* + 1. 【中危】Windows SAM 和 LSAD 降级漏洞
* 漏洞描述：

当安全帐户管理器 (SAM) 和本地安全机构（域策略）(LSAD) 远程协议接受不充分保护它们的验证级别时，它们中会存在一个特权提升漏洞。此漏洞是由 SAM 和 LSAD 远程协议建立远程过程调用 (RPC) 通道的方式导致的。成功利用此漏洞的攻击者可以获得对 SAM 数据库的访问权限。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.74 | 49164 |

* 加固建议：

请选择合适的版本的补丁进行Windows 更新https://technet.microsoft.com/zh-cn/library/security/ms16-047.aspx#ID0EPOAC

* + 1. 【中危】TLS版本1.0协议检测
* 漏洞描述：

远程服务接受使用TLS 1.0加密的连接。TLS 1.0有许多密码设计缺陷。TLS 1.0的现代实现减轻了这些问题，但是像1.2和1.3这样的TLS的新版本是针对这些缺陷而设计的，应该尽可能使用。截至2020年3月31日，为TLS 1.2及更高版本启用的终结点将不再与主要web浏览器和主要供应商正常工作。PCI DSS v3.2要求在2018年6月30日之前完全禁用TLS 1.0，但POS POI终端（及其连接的SSL/TLS终端点）除外，这些终端可以被验证为不易受任何已知漏洞攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.74 | 3389 |

* 加固建议：

启用对TLS 1.2和1.3的支持，并禁用对TLS 1.0的支持。

* + 1. 【中危】JQuery 1.2<3.5.0多个XSS
* 漏洞描述：

根据脚本中自我报告的版本，远程web服务器上托管的JQuery版本大于或等于1.2且早于3.5.0。因此，它受到多个跨站点脚本漏洞的影响。注意，此插件中引用的漏洞对PAN-OS没有安全影响，并且/或者运行PAN-OS版本的设备上不存在成功利用漏洞所需的场景。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.74 | 8000 |

* 加固建议：

升级到JQuery 3.5.0或更高版本。

* 1. 【紧急】应用服务器（10.10.14.75）
     1. 【紧急】MS14-066：Schannel 远程代码执行漏洞
* 漏洞描述：

MS14-066 (CVE-2014-6321) 是存在于Microsoft的schannel.dll中的TLS堆缓冲区溢出漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.75 | 3389 |

* 加固建议：

目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： https://technet.microsoft.com/library/security/ms14-066

* + 1. 【中危】SSL证书签名使用弱强度的哈希算法
* 漏洞描述：

远程服务器的SSL证书签名使用弱强度的哈希加密算法，例如MD2、MD4或者MD5。这些签名算法显示容易遭到破解。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.75 | 3389 |

* 加固建议：

联系证书认证机构发布新的证书。 如果服务器使用自签名证书，则可自己

* + 1. 【中危】SSL证书不被信任
* 漏洞描述：

此项服务的SSL证书不被信任。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.75 | 3389 |

* 加固建议：

为此项服务购买或生成合适的证书

* + 1. 【中危】SSL自签名证书
* 漏洞描述：

服务器所使用的X.509签署的证书链不是权威的证书颁发机构所颁发的。这削弱了使用SSL的效果，因为任何人都可以建立一个中间人攻击远程主机。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.75 | 3389 |

* 加固建议：

购买或者生成被认可的证书

* + 1. 【中危】Windows SAM 和 LSAD 降级漏洞
* 漏洞描述：

当安全帐户管理器 (SAM) 和本地安全机构（域策略）(LSAD) 远程协议接受不充分保护它们的验证级别时，它们中会存在一个特权提升漏洞。此漏洞是由 SAM 和 LSAD 远程协议建立远程过程调用 (RPC) 通道的方式导致的。成功利用此漏洞的攻击者可以获得对 SAM 数据库的访问权限。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.75 | 49159 |

* 加固建议：

请选择合适的版本的补丁进行Windows 更新https://technet.microsoft.com/zh-cn/library/security/ms16-047.aspx#ID0EPOAC

* + 1. 【中危】TLS版本1.0协议检测
* 漏洞描述：

远程服务接受使用TLS 1.0加密的连接。TLS 1.0有许多密码设计缺陷。TLS 1.0的现代实现减轻了这些问题，但是像1.2和1.3这样的TLS的新版本是针对这些缺陷而设计的，应该尽可能使用。截至2020年3月31日，为TLS 1.2及更高版本启用的终结点将不再与主要web浏览器和主要供应商正常工作。PCI DSS v3.2要求在2018年6月30日之前完全禁用TLS 1.0，但POS POI终端（及其连接的SSL/TLS终端点）除外，这些终端可以被验证为不易受任何已知漏洞攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.75 | 3389 |

* 加固建议：

启用对TLS 1.2和1.3的支持，并禁用对TLS 1.0的支持。

* 1. 【紧急】临床路径服务器（10.10.14.76）
     1. 【紧急】MS14-066：Schannel 远程代码执行漏洞
* 漏洞描述：

MS14-066 (CVE-2014-6321) 是存在于Microsoft的schannel.dll中的TLS堆缓冲区溢出漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.76 | 3389 |

* 加固建议：

目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： https://technet.microsoft.com/library/security/ms14-066

* + 1. 【中危】SSL证书签名使用弱强度的哈希算法
* 漏洞描述：

远程服务器的SSL证书签名使用弱强度的哈希加密算法，例如MD2、MD4或者MD5。这些签名算法显示容易遭到破解。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.76 | 3389 |

* 加固建议：

联系证书认证机构发布新的证书。 如果服务器使用自签名证书，则可自己

* + 1. 【中危】允许SSL采用中强度加密
* 漏洞描述：

远程主机支持SSL使用的密码采用中强度解密，即使用的KEY解密长度至少64位，但少于112位。注意：如果攻击者在同一个物理网段，密码很容易暴露。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.76 | 3389 |

* 加固建议：

重新设置受影响的应用程序，可能的话，避免使用中强度加密，改为强度较高的加密算法。

* + 1. 【中危】SSL证书不被信任
* 漏洞描述：

此项服务的SSL证书不被信任。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.76 | 3389 |

* 加固建议：

为此项服务购买或生成合适的证书

* + 1. 【中危】SSL自签名证书
* 漏洞描述：

服务器所使用的X.509签署的证书链不是权威的证书颁发机构所颁发的。这削弱了使用SSL的效果，因为任何人都可以建立一个中间人攻击远程主机。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.76 | 3389 |

* 加固建议：

购买或者生成被认可的证书

* + 1. 【中危】远程主机支持SSL RC4加密套件
* 漏洞描述：

远程主机在一个或多个支持使用RC4密码套件，RC4密码是有缺陷的生成伪随机流的字节数, 如果明文重复加密(如HTTP cookie),攻击者能够获得许多(即数以百万计)明文密文配对,攻击者可以获得密文后，对比获得明文。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.76 | 3389 |

* 加固建议：

重新设置受影响的应用程序，可能的话，避免使用RC4密钥算法，可以考虑给浏览器或WEB服务支持的带有AES-GCM 的TLS 1.2，相关链接： http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/ http://www.imperva.com/docs/HII\_Attacking\_SSL\_when\_using\_RC4.pdf

* + 1. 【中危】Windows SAM 和 LSAD 降级漏洞
* 漏洞描述：

当安全帐户管理器 (SAM) 和本地安全机构（域策略）(LSAD) 远程协议接受不充分保护它们的验证级别时，它们中会存在一个特权提升漏洞。此漏洞是由 SAM 和 LSAD 远程协议建立远程过程调用 (RPC) 通道的方式导致的。成功利用此漏洞的攻击者可以获得对 SAM 数据库的访问权限。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.76 | 49160 |

* 加固建议：

请选择合适的版本的补丁进行Windows 更新https://technet.microsoft.com/zh-cn/library/security/ms16-047.aspx#ID0EPOAC

* + 1. 【中危】TLS版本1.0协议检测
* 漏洞描述：

远程服务接受使用TLS 1.0加密的连接。TLS 1.0有许多密码设计缺陷。TLS 1.0的现代实现减轻了这些问题，但是像1.2和1.3这样的TLS的新版本是针对这些缺陷而设计的，应该尽可能使用。截至2020年3月31日，为TLS 1.2及更高版本启用的终结点将不再与主要web浏览器和主要供应商正常工作。PCI DSS v3.2要求在2018年6月30日之前完全禁用TLS 1.0，但POS POI终端（及其连接的SSL/TLS终端点）除外，这些终端可以被验证为不易受任何已知漏洞攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.76 | 3389 |

* 加固建议：

启用对TLS 1.2和1.3的支持，并禁用对TLS 1.0的支持。

* 1. 【紧急】移动护理数据服务器（10.10.14.77）
     1. 【紧急】当前ORACLE数据库版本厂商已不支持
* 漏洞描述：

根据远程主机安装的数据库版本，厂家已不再支持，将会缺少安全补丁包，因此，可能存在安全威胁。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.77 | 1521 |

* 加固建议：

升级数据库版本至当前最新版本，至少升级至厂家支持的版本。

* + 1. 【高危】Oracle TNS侦听器远程毒化
* 漏洞描述：

Oracle Database Server是一个对象关系数据库管理系统。 Oracle Database Server在实现上存在可允许攻击者向远程“TNS Listener”组件处理的数据投毒的漏洞。攻击者可利用此漏洞将数据库服务器的合法“TNS Listener”组件中的数据转向到攻击者控制的系统，导致控制远程组件的数据库实例，造成组件和合法数据库之间的攻击者攻击、会话劫持或拒绝服务攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.77 | 1521 |

* 加固建议：

目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://www.oracle.com/technetwork/topics/security/alert-cve-2012-1675-1608180.html

* + 1. 【中危】SSH弱算法支持
* 漏洞描述：

目前该ssh服务采用的算法较低

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.77 | 22 |

* 加固建议：

修改ssh算法采用aes128-cbc或者aes256-cbc

* + 1. 【低危】SSH服务器CBC模式密码已启用
* 漏洞描述：

SSH服务器配置为支持密码块链接（CBC）加密。这可能允许攻击者从密文中恢复明文消息。注意，这个插件只检查SSH服务器的选项，不检查易受攻击的软件版本。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.77 | 22 |

* 加固建议：

联系供应商或查阅产品文档以禁用CBC模式密码加密，并启用CTR或GCM密码模式加密。

* + 1. 【低危】SSH弱MAC算法已启用
* 漏洞描述：

远程SSH服务器配置为允许MD5或96位MAC算法，这两种算法都被认为是较弱的。注意，这个插件只检查SSH服务器的选项，不检查易受攻击的软件版本。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.77 | 22 |

* 加固建议：

请与供应商联系或查阅产品文档以禁用MD5和96位MAC算法。

* 1. 【紧急】医保分值付费服务器（10.10.14.78）
     1. 【紧急】Microsoft SQL Server不支持的版本检测（远程检查）
* 漏洞描述：

根据其自我报告的版本号，不再支持在远程主机上安装Microsoft SQL Server。缺少支持意味着供应商不会发布产品的新安全修补程序。因此，它很可能包含安全漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.78 | 1433 |

* 加固建议：

升级到当前支持的Microsoft SQL Server版本。

* + 1. 【紧急】MS14-066：Schannel 远程代码执行漏洞
* 漏洞描述：

MS14-066 (CVE-2014-6321) 是存在于Microsoft的schannel.dll中的TLS堆缓冲区溢出漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.78 | 3389 |

* 加固建议：

目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： https://technet.microsoft.com/library/security/ms14-066

* + 1. 【中危】SSL证书签名使用弱强度的哈希算法
* 漏洞描述：

远程服务器的SSL证书签名使用弱强度的哈希加密算法，例如MD2、MD4或者MD5。这些签名算法显示容易遭到破解。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.78 | 1433 |
| 10.10.14.78 | 3389 |

* 加固建议：

联系证书认证机构发布新的证书。 如果服务器使用自签名证书，则可自己

* + 1. 【中危】SSL证书主机名不匹配
* 漏洞描述：

SSL现有认证的commonName (CN)是供其它主机使用的。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.78 | 1433 |

* 加固建议：

为此项服务购买或生产一个合适的证书

* + 1. 【中危】SSL证书不被信任
* 漏洞描述：

此项服务的SSL证书不被信任。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.78 | 1433 |
| 10.10.14.78 | 3389 |

* 加固建议：

为此项服务购买或生成合适的证书

* + 1. 【中危】SSL自签名证书
* 漏洞描述：

服务器所使用的X.509签署的证书链不是权威的证书颁发机构所颁发的。这削弱了使用SSL的效果，因为任何人都可以建立一个中间人攻击远程主机。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.78 | 1433 |
| 10.10.14.78 | 3389 |

* 加固建议：

购买或者生成被认可的证书

* + 1. 【中危】Windows SAM 和 LSAD 降级漏洞
* 漏洞描述：

当安全帐户管理器 (SAM) 和本地安全机构（域策略）(LSAD) 远程协议接受不充分保护它们的验证级别时，它们中会存在一个特权提升漏洞。此漏洞是由 SAM 和 LSAD 远程协议建立远程过程调用 (RPC) 通道的方式导致的。成功利用此漏洞的攻击者可以获得对 SAM 数据库的访问权限。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.78 | 49158 |

* 加固建议：

请选择合适的版本的补丁进行Windows 更新https://technet.microsoft.com/zh-cn/library/security/ms16-047.aspx#ID0EPOAC

* + 1. 【中危】TLS版本1.0协议检测
* 漏洞描述：

远程服务接受使用TLS 1.0加密的连接。TLS 1.0有许多密码设计缺陷。TLS 1.0的现代实现减轻了这些问题，但是像1.2和1.3这样的TLS的新版本是针对这些缺陷而设计的，应该尽可能使用。截至2020年3月31日，为TLS 1.2及更高版本启用的终结点将不再与主要web浏览器和主要供应商正常工作。PCI DSS v3.2要求在2018年6月30日之前完全禁用TLS 1.0，但POS POI终端（及其连接的SSL/TLS终端点）除外，这些终端可以被验证为不易受任何已知漏洞攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.78 | 1433 |
| 10.10.14.78 | 3389 |

* 加固建议：

启用对TLS 1.2和1.3的支持，并禁用对TLS 1.0的支持。

* + 1. 【低危】SSL证书链包含小于2048位的RSA密钥
* 漏洞描述：

远程主机发送的X.509证书中至少有一个具有短于2048位的密钥。根据证书颁发机构/浏览器（CA/B）论坛制定的行业标准，2014年1月1日之后颁发的证书必须至少为2048位。一些浏览器SSL实现可能会在2014年1月1日之后拒绝小于2048位的密钥。此外，一些SSL证书供应商可能会在2014年1月1日之前吊销小于2048位的证书。请注意，如果在2010年12月31日之前颁发RSA密钥小于2048位的根证书，Nessus将不会标记这些根证书，因为标准认为它们是免税的。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.78 | 1433 |

* 加固建议：

用长度小于2048位的RSA密钥替换链中的证书，然后重新颁发由旧证书签名的所有证书。

* 1. 【紧急】电子病历364视图服务器（10.10.14.87）
     1. 【紧急】NFS 共享信息泄露漏洞
* 漏洞描述：

远程攻击者可以装载Ultrix或OSF中的NFS文件系统，即使它在访问列表中被否认。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.87 | 2049 |

* 加固建议：

配置NFS，限制为仅允许已通过授权的远程主机可以进行远程挂载NFS共享。

* + 1. 【高危】NFS 共享允许远程挂载
* 漏洞描述：

服务器的NFS共享允许通过远程挂载，攻击者可能会利用此漏洞获取远程主机文件的读权限（甚至是写）。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.87 | 2049 |

* 加固建议：

配置NFS，限制为仅允许已通过授权的远程主机可以进行远程挂载NFS共享。

* + 1. 【中危】NFS 共享可读
* 漏洞描述：

远程NFS服务器允许导出一个或更多的共享，而没有限制访问（如基于主机名，IP或IP范围）。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.87 | 2049 |

* 加固建议：

配置NFS，限制为仅允许已通过授权的远程主机可以进行远程挂载NFS共享。

* + 1. 【低危】SSH服务器CBC模式密码已启用
* 漏洞描述：

SSH服务器配置为支持密码块链接（CBC）加密。这可能允许攻击者从密文中恢复明文消息。注意，这个插件只检查SSH服务器的选项，不检查易受攻击的软件版本。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.87 | 22 |

* 加固建议：

联系供应商或查阅产品文档以禁用CBC模式密码加密，并启用CTR或GCM密码模式加密。

* 1. 【紧急】电子病历应用服务器（10.10.14.89）
     1. 【紧急】MS14-066：Schannel 远程代码执行漏洞
* 漏洞描述：

MS14-066 (CVE-2014-6321) 是存在于Microsoft的schannel.dll中的TLS堆缓冲区溢出漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.89 | 3389 |

* 加固建议：

目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： https://technet.microsoft.com/library/security/ms14-066

* + 1. 【中危】SSL证书签名使用弱强度的哈希算法
* 漏洞描述：

远程服务器的SSL证书签名使用弱强度的哈希加密算法，例如MD2、MD4或者MD5。这些签名算法显示容易遭到破解。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.89 | 3389 |

* 加固建议：

联系证书认证机构发布新的证书。 如果服务器使用自签名证书，则可自己

* + 1. 【中危】允许SSL采用中强度加密
* 漏洞描述：

远程主机支持SSL使用的密码采用中强度解密，即使用的KEY解密长度至少64位，但少于112位。注意：如果攻击者在同一个物理网段，密码很容易暴露。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.89 | 3389 |

* 加固建议：

重新设置受影响的应用程序，可能的话，避免使用中强度加密，改为强度较高的加密算法。

* + 1. 【中危】SSL证书不被信任
* 漏洞描述：

此项服务的SSL证书不被信任。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.89 | 3389 |

* 加固建议：

为此项服务购买或生成合适的证书

* + 1. 【中危】SSL自签名证书
* 漏洞描述：

服务器所使用的X.509签署的证书链不是权威的证书颁发机构所颁发的。这削弱了使用SSL的效果，因为任何人都可以建立一个中间人攻击远程主机。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.89 | 3389 |

* 加固建议：

购买或者生成被认可的证书

* + 1. 【中危】远程主机支持SSL RC4加密套件
* 漏洞描述：

远程主机在一个或多个支持使用RC4密码套件，RC4密码是有缺陷的生成伪随机流的字节数, 如果明文重复加密(如HTTP cookie),攻击者能够获得许多(即数以百万计)明文密文配对,攻击者可以获得密文后，对比获得明文。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.89 | 3389 |

* 加固建议：

重新设置受影响的应用程序，可能的话，避免使用RC4密钥算法，可以考虑给浏览器或WEB服务支持的带有AES-GCM 的TLS 1.2，相关链接： http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/ http://www.imperva.com/docs/HII\_Attacking\_SSL\_when\_using\_RC4.pdf

* + 1. 【中危】TLS版本1.0协议检测
* 漏洞描述：

远程服务接受使用TLS 1.0加密的连接。TLS 1.0有许多密码设计缺陷。TLS 1.0的现代实现减轻了这些问题，但是像1.2和1.3这样的TLS的新版本是针对这些缺陷而设计的，应该尽可能使用。截至2020年3月31日，为TLS 1.2及更高版本启用的终结点将不再与主要web浏览器和主要供应商正常工作。PCI DSS v3.2要求在2018年6月30日之前完全禁用TLS 1.0，但POS POI终端（及其连接的SSL/TLS终端点）除外，这些终端可以被验证为不易受任何已知漏洞攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.89 | 3389 |

* 加固建议：

启用对TLS 1.2和1.3的支持，并禁用对TLS 1.0的支持。

* 1. 【紧急】电子病历应用服务器（10.10.14.90）
     1. 【紧急】MS14-066：Schannel 远程代码执行漏洞
* 漏洞描述：

MS14-066 (CVE-2014-6321) 是存在于Microsoft的schannel.dll中的TLS堆缓冲区溢出漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.90 | 3389 |

* 加固建议：

目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： https://technet.microsoft.com/library/security/ms14-066

* + 1. 【中危】SSL证书签名使用弱强度的哈希算法
* 漏洞描述：

远程服务器的SSL证书签名使用弱强度的哈希加密算法，例如MD2、MD4或者MD5。这些签名算法显示容易遭到破解。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.90 | 3389 |

* 加固建议：

联系证书认证机构发布新的证书。 如果服务器使用自签名证书，则可自己

* + 1. 【中危】SSL证书不被信任
* 漏洞描述：

此项服务的SSL证书不被信任。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.90 | 3389 |

* 加固建议：

为此项服务购买或生成合适的证书

* + 1. 【中危】SSL自签名证书
* 漏洞描述：

服务器所使用的X.509签署的证书链不是权威的证书颁发机构所颁发的。这削弱了使用SSL的效果，因为任何人都可以建立一个中间人攻击远程主机。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.90 | 3389 |

* 加固建议：

购买或者生成被认可的证书

* + 1. 【中危】Windows SAM 和 LSAD 降级漏洞
* 漏洞描述：

当安全帐户管理器 (SAM) 和本地安全机构（域策略）(LSAD) 远程协议接受不充分保护它们的验证级别时，它们中会存在一个特权提升漏洞。此漏洞是由 SAM 和 LSAD 远程协议建立远程过程调用 (RPC) 通道的方式导致的。成功利用此漏洞的攻击者可以获得对 SAM 数据库的访问权限。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.90 | 49159 |

* 加固建议：

请选择合适的版本的补丁进行Windows 更新https://technet.microsoft.com/zh-cn/library/security/ms16-047.aspx#ID0EPOAC

* + 1. 【中危】TLS版本1.0协议检测
* 漏洞描述：

远程服务接受使用TLS 1.0加密的连接。TLS 1.0有许多密码设计缺陷。TLS 1.0的现代实现减轻了这些问题，但是像1.2和1.3这样的TLS的新版本是针对这些缺陷而设计的，应该尽可能使用。截至2020年3月31日，为TLS 1.2及更高版本启用的终结点将不再与主要web浏览器和主要供应商正常工作。PCI DSS v3.2要求在2018年6月30日之前完全禁用TLS 1.0，但POS POI终端（及其连接的SSL/TLS终端点）除外，这些终端可以被验证为不易受任何已知漏洞攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.90 | 3389 |

* 加固建议：

启用对TLS 1.2和1.3的支持，并禁用对TLS 1.0的支持。

* 1. 【紧急】电子病历应用服务器（10.10.14.92）
     1. 【紧急】MS14-066：Schannel 远程代码执行漏洞
* 漏洞描述：

MS14-066 (CVE-2014-6321) 是存在于Microsoft的schannel.dll中的TLS堆缓冲区溢出漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.92 | 3389 |

* 加固建议：

目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： https://technet.microsoft.com/library/security/ms14-066

* + 1. 【中危】SSL证书签名使用弱强度的哈希算法
* 漏洞描述：

远程服务器的SSL证书签名使用弱强度的哈希加密算法，例如MD2、MD4或者MD5。这些签名算法显示容易遭到破解。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.92 | 3389 |

* 加固建议：

联系证书认证机构发布新的证书。 如果服务器使用自签名证书，则可自己

* + 1. 【中危】允许SSL采用中强度加密
* 漏洞描述：

远程主机支持SSL使用的密码采用中强度解密，即使用的KEY解密长度至少64位，但少于112位。注意：如果攻击者在同一个物理网段，密码很容易暴露。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.92 | 3389 |

* 加固建议：

重新设置受影响的应用程序，可能的话，避免使用中强度加密，改为强度较高的加密算法。

* + 1. 【中危】SSL证书不被信任
* 漏洞描述：

此项服务的SSL证书不被信任。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.92 | 3389 |

* 加固建议：

为此项服务购买或生成合适的证书

* + 1. 【中危】SSL自签名证书
* 漏洞描述：

服务器所使用的X.509签署的证书链不是权威的证书颁发机构所颁发的。这削弱了使用SSL的效果，因为任何人都可以建立一个中间人攻击远程主机。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.92 | 3389 |

* 加固建议：

购买或者生成被认可的证书

* + 1. 【中危】SMB数字签名通信禁用
* 漏洞描述：

SMB 协议为 Microsoft 文件和打印共享以及许多其他网络操作（例如远程 Windows 管理）提供基础。为了防止在传输过程中修改 SMB 数据包的拦截攻击，SMB 协议支持对 SMB 数据包的数字签名。 主机禁用了SMB数字签名通信，这可能导致潜在攻击者针对SMB通信服务进行中间人攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.92 | 445 |

* 加固建议：

在本地策略中--安全选项设置如下： Microsoft 网络客户端：对通信进行数字签名（若服务器同意）（启用） Microsoft 网络服务器：对通信进行数字签名（若客户同意）（启用）

* + 1. 【中危】远程主机支持SSL RC4加密套件
* 漏洞描述：

远程主机在一个或多个支持使用RC4密码套件，RC4密码是有缺陷的生成伪随机流的字节数, 如果明文重复加密(如HTTP cookie),攻击者能够获得许多(即数以百万计)明文密文配对,攻击者可以获得密文后，对比获得明文。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.92 | 3389 |

* 加固建议：

重新设置受影响的应用程序，可能的话，避免使用RC4密钥算法，可以考虑给浏览器或WEB服务支持的带有AES-GCM 的TLS 1.2，相关链接： http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/ http://www.imperva.com/docs/HII\_Attacking\_SSL\_when\_using\_RC4.pdf

* + 1. 【中危】Windows SAM 和 LSAD 降级漏洞
* 漏洞描述：

当安全帐户管理器 (SAM) 和本地安全机构（域策略）(LSAD) 远程协议接受不充分保护它们的验证级别时，它们中会存在一个特权提升漏洞。此漏洞是由 SAM 和 LSAD 远程协议建立远程过程调用 (RPC) 通道的方式导致的。成功利用此漏洞的攻击者可以获得对 SAM 数据库的访问权限。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.92 | 49157 |

* 加固建议：

请选择合适的版本的补丁进行Windows 更新https://technet.microsoft.com/zh-cn/library/security/ms16-047.aspx#ID0EPOAC

* + 1. 【中危】TLS版本1.0协议检测
* 漏洞描述：

远程服务接受使用TLS 1.0加密的连接。TLS 1.0有许多密码设计缺陷。TLS 1.0的现代实现减轻了这些问题，但是像1.2和1.3这样的TLS的新版本是针对这些缺陷而设计的，应该尽可能使用。截至2020年3月31日，为TLS 1.2及更高版本启用的终结点将不再与主要web浏览器和主要供应商正常工作。PCI DSS v3.2要求在2018年6月30日之前完全禁用TLS 1.0，但POS POI终端（及其连接的SSL/TLS终端点）除外，这些终端可以被验证为不易受任何已知漏洞攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.92 | 3389 |

* 加固建议：

启用对TLS 1.2和1.3的支持，并禁用对TLS 1.0的支持。

* 1. 【紧急】电子病历应用服务器（10.10.14.96）
     1. 【紧急】MS14-066：Schannel 远程代码执行漏洞
* 漏洞描述：

MS14-066 (CVE-2014-6321) 是存在于Microsoft的schannel.dll中的TLS堆缓冲区溢出漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.96 | 3389 |

* 加固建议：

目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： https://technet.microsoft.com/library/security/ms14-066

* + 1. 【中危】SSL证书签名使用弱强度的哈希算法
* 漏洞描述：

远程服务器的SSL证书签名使用弱强度的哈希加密算法，例如MD2、MD4或者MD5。这些签名算法显示容易遭到破解。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.96 | 3389 |

* 加固建议：

联系证书认证机构发布新的证书。 如果服务器使用自签名证书，则可自己

* + 1. 【中危】SSL证书不被信任
* 漏洞描述：

此项服务的SSL证书不被信任。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.96 | 3389 |

* 加固建议：

为此项服务购买或生成合适的证书

* + 1. 【中危】SSL自签名证书
* 漏洞描述：

服务器所使用的X.509签署的证书链不是权威的证书颁发机构所颁发的。这削弱了使用SSL的效果，因为任何人都可以建立一个中间人攻击远程主机。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.96 | 3389 |

* 加固建议：

购买或者生成被认可的证书

* + 1. 【中危】TLS版本1.0协议检测
* 漏洞描述：

远程服务接受使用TLS 1.0加密的连接。TLS 1.0有许多密码设计缺陷。TLS 1.0的现代实现减轻了这些问题，但是像1.2和1.3这样的TLS的新版本是针对这些缺陷而设计的，应该尽可能使用。截至2020年3月31日，为TLS 1.2及更高版本启用的终结点将不再与主要web浏览器和主要供应商正常工作。PCI DSS v3.2要求在2018年6月30日之前完全禁用TLS 1.0，但POS POI终端（及其连接的SSL/TLS终端点）除外，这些终端可以被验证为不易受任何已知漏洞攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.96 | 3389 |

* 加固建议：

启用对TLS 1.2和1.3的支持，并禁用对TLS 1.0的支持。

* 1. 【紧急】电子病历应用服务器（10.10.14.97）
     1. 【紧急】MS14-066：Schannel 远程代码执行漏洞
* 漏洞描述：

MS14-066 (CVE-2014-6321) 是存在于Microsoft的schannel.dll中的TLS堆缓冲区溢出漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.97 | 3389 |

* 加固建议：

目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： https://technet.microsoft.com/library/security/ms14-066

* + 1. 【中危】SSL证书签名使用弱强度的哈希算法
* 漏洞描述：

远程服务器的SSL证书签名使用弱强度的哈希加密算法，例如MD2、MD4或者MD5。这些签名算法显示容易遭到破解。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.97 | 3389 |

* 加固建议：

联系证书认证机构发布新的证书。 如果服务器使用自签名证书，则可自己

* + 1. 【中危】SSL证书不被信任
* 漏洞描述：

此项服务的SSL证书不被信任。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.97 | 3389 |

* 加固建议：

为此项服务购买或生成合适的证书

* + 1. 【中危】SSL自签名证书
* 漏洞描述：

服务器所使用的X.509签署的证书链不是权威的证书颁发机构所颁发的。这削弱了使用SSL的效果，因为任何人都可以建立一个中间人攻击远程主机。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.97 | 3389 |

* 加固建议：

购买或者生成被认可的证书

* + 1. 【中危】TLS版本1.0协议检测
* 漏洞描述：

远程服务接受使用TLS 1.0加密的连接。TLS 1.0有许多密码设计缺陷。TLS 1.0的现代实现减轻了这些问题，但是像1.2和1.3这样的TLS的新版本是针对这些缺陷而设计的，应该尽可能使用。截至2020年3月31日，为TLS 1.2及更高版本启用的终结点将不再与主要web浏览器和主要供应商正常工作。PCI DSS v3.2要求在2018年6月30日之前完全禁用TLS 1.0，但POS POI终端（及其连接的SSL/TLS终端点）除外，这些终端可以被验证为不易受任何已知漏洞攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.97 | 3389 |

* 加固建议：

启用对TLS 1.2和1.3的支持，并禁用对TLS 1.0的支持。

* 1. 【紧急】电子病历应用服务器（10.10.14.98）
     1. 【紧急】MS14-066：Schannel 远程代码执行漏洞
* 漏洞描述：

MS14-066 (CVE-2014-6321) 是存在于Microsoft的schannel.dll中的TLS堆缓冲区溢出漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.98 | 3389 |

* 加固建议：

目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： https://technet.microsoft.com/library/security/ms14-066

* + 1. 【中危】SSL证书签名使用弱强度的哈希算法
* 漏洞描述：

远程服务器的SSL证书签名使用弱强度的哈希加密算法，例如MD2、MD4或者MD5。这些签名算法显示容易遭到破解。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.98 | 3389 |

* 加固建议：

联系证书认证机构发布新的证书。 如果服务器使用自签名证书，则可自己

* + 1. 【中危】SSL证书不被信任
* 漏洞描述：

此项服务的SSL证书不被信任。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.98 | 3389 |

* 加固建议：

为此项服务购买或生成合适的证书

* + 1. 【中危】SSL自签名证书
* 漏洞描述：

服务器所使用的X.509签署的证书链不是权威的证书颁发机构所颁发的。这削弱了使用SSL的效果，因为任何人都可以建立一个中间人攻击远程主机。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.98 | 3389 |

* 加固建议：

购买或者生成被认可的证书

* + 1. 【中危】TLS版本1.0协议检测
* 漏洞描述：

远程服务接受使用TLS 1.0加密的连接。TLS 1.0有许多密码设计缺陷。TLS 1.0的现代实现减轻了这些问题，但是像1.2和1.3这样的TLS的新版本是针对这些缺陷而设计的，应该尽可能使用。截至2020年3月31日，为TLS 1.2及更高版本启用的终结点将不再与主要web浏览器和主要供应商正常工作。PCI DSS v3.2要求在2018年6月30日之前完全禁用TLS 1.0，但POS POI终端（及其连接的SSL/TLS终端点）除外，这些终端可以被验证为不易受任何已知漏洞攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.98 | 3389 |

* 加固建议：

启用对TLS 1.2和1.3的支持，并禁用对TLS 1.0的支持。

* 1. 【紧急】PACS系统（222.222.100.5）
     1. 【紧急】当前ORACLE数据库版本厂商已不支持
* 漏洞描述：

根据远程主机安装的数据库版本，厂家已不再支持，将会缺少安全补丁包，因此，可能存在安全威胁。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.100.5 | 1521 |

* 加固建议：

升级数据库版本至当前最新版本，至少升级至厂家支持的版本。

* + 1. 【高危】Oracle TNS侦听器远程毒化
* 漏洞描述：

Oracle Database Server是一个对象关系数据库管理系统。 Oracle Database Server在实现上存在可允许攻击者向远程“TNS Listener”组件处理的数据投毒的漏洞。攻击者可利用此漏洞将数据库服务器的合法“TNS Listener”组件中的数据转向到攻击者控制的系统，导致控制远程组件的数据库实例，造成组件和合法数据库之间的攻击者攻击、会话劫持或拒绝服务攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.100.5 | 1521 |

* 加固建议：

目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://www.oracle.com/technetwork/topics/security/alert-cve-2012-1675-1608180.html

* + 1. 【中危】SSL证书主机名不匹配
* 漏洞描述：

SSL现有认证的commonName (CN)是供其它主机使用的。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.100.5 | 3389 |

* 加固建议：

为此项服务购买或生产一个合适的证书

* + 1. 【中危】SSL证书不被信任
* 漏洞描述：

此项服务的SSL证书不被信任。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.100.5 | 3389 |

* 加固建议：

为此项服务购买或生成合适的证书

* + 1. 【中危】SSL自签名证书
* 漏洞描述：

服务器所使用的X.509签署的证书链不是权威的证书颁发机构所颁发的。这削弱了使用SSL的效果，因为任何人都可以建立一个中间人攻击远程主机。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.100.5 | 3389 |

* 加固建议：

购买或者生成被认可的证书

* + 1. 【中危】TLS版本1.0协议检测
* 漏洞描述：

远程服务接受使用TLS 1.0加密的连接。TLS 1.0有许多密码设计缺陷。TLS 1.0的现代实现减轻了这些问题，但是像1.2和1.3这样的TLS的新版本是针对这些缺陷而设计的，应该尽可能使用。截至2020年3月31日，为TLS 1.2及更高版本启用的终结点将不再与主要web浏览器和主要供应商正常工作。PCI DSS v3.2要求在2018年6月30日之前完全禁用TLS 1.0，但POS POI终端（及其连接的SSL/TLS终端点）除外，这些终端可以被验证为不易受任何已知漏洞攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.100.5 | 3389 |

* 加固建议：

启用对TLS 1.2和1.3的支持，并禁用对TLS 1.0的支持。

* 1. 【紧急】医保前置机（222.222.222.40）
     1. 【紧急】Microsoft SQL Server不支持的版本检测（远程检查）
* 漏洞描述：

根据其自我报告的版本号，不再支持在远程主机上安装Microsoft SQL Server。缺少支持意味着供应商不会发布产品的新安全修补程序。因此，它很可能包含安全漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.40 | 1433 |

* 加固建议：

升级到当前支持的Microsoft SQL Server版本。

* + 1. 【高危】SSL 2.0协议未禁用
* 漏洞描述：

远程服务使用SSL 2.0进行通信连接加密，根据公开的漏洞曝露报告，此版本的协议存在一些加密缺陷，并已废弃多年。攻击者可以利用这个漏洞发动中间人攻击或解密受此影响的客户端之间的通信内容。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.40 | 1433 |

* 加固建议：

禁用SSL 2.0，使用TLS 1.0或更高版本代替

* + 1. 【中危】SSL证书签名使用弱强度的哈希算法
* 漏洞描述：

远程服务器的SSL证书签名使用弱强度的哈希加密算法，例如MD2、MD4或者MD5。这些签名算法显示容易遭到破解。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.40 | 1433 |

* 加固建议：

联系证书认证机构发布新的证书。 如果服务器使用自签名证书，则可自己

* + 1. 【中危】允许SSL采用中强度加密
* 漏洞描述：

远程主机支持SSL使用的密码采用中强度解密，即使用的KEY解密长度至少64位，但少于112位。注意：如果攻击者在同一个物理网段，密码很容易暴露。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.40 | 1433 |

* 加固建议：

重新设置受影响的应用程序，可能的话，避免使用中强度加密，改为强度较高的加密算法。

* + 1. 【中危】SSL证书不被信任
* 漏洞描述：

此项服务的SSL证书不被信任。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.40 | 1433 |

* 加固建议：

为此项服务购买或生成合适的证书

* + 1. 【中危】SSL自签名证书
* 漏洞描述：

服务器所使用的X.509签署的证书链不是权威的证书颁发机构所颁发的。这削弱了使用SSL的效果，因为任何人都可以建立一个中间人攻击远程主机。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.40 | 1433 |

* 加固建议：

购买或者生成被认可的证书

* + 1. 【中危】远程主机支持SSL RC4加密套件
* 漏洞描述：

远程主机在一个或多个支持使用RC4密码套件，RC4密码是有缺陷的生成伪随机流的字节数, 如果明文重复加密(如HTTP cookie),攻击者能够获得许多(即数以百万计)明文密文配对,攻击者可以获得密文后，对比获得明文。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.40 | 1433 |

* 加固建议：

重新设置受影响的应用程序，可能的话，避免使用RC4密钥算法，可以考虑给浏览器或WEB服务支持的带有AES-GCM 的TLS 1.2，相关链接： http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/ http://www.imperva.com/docs/HII\_Attacking\_SSL\_when\_using\_RC4.pdf

* + 1. 【中危】SSLv3 POODLE 安全漏洞
* 漏洞描述：

支持SSLv3 协议的网站存在被中间人攻击的风险，“Poodle”攻击（全称为Padding Oracle On Downloaded Legacy Encryption）可以提取出SSL连接中的加密数据相应的明文信息。攻击者可以利用这个漏洞发动中间人攻击或解密受此影响的客户端之间的通信内容。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.40 | 1433 |

* 加固建议：

禁用SSL 3.0

* + 1. 【中危】TLS版本1.0协议检测
* 漏洞描述：

远程服务接受使用TLS 1.0加密的连接。TLS 1.0有许多密码设计缺陷。TLS 1.0的现代实现减轻了这些问题，但是像1.2和1.3这样的TLS的新版本是针对这些缺陷而设计的，应该尽可能使用。截至2020年3月31日，为TLS 1.2及更高版本启用的终结点将不再与主要web浏览器和主要供应商正常工作。PCI DSS v3.2要求在2018年6月30日之前完全禁用TLS 1.0，但POS POI终端（及其连接的SSL/TLS终端点）除外，这些终端可以被验证为不易受任何已知漏洞攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.40 | 1433 |

* 加固建议：

启用对TLS 1.2和1.3的支持，并禁用对TLS 1.0的支持。

* + 1. 【低危】SSL证书链包含小于2048位的RSA密钥
* 漏洞描述：

远程主机发送的X.509证书中至少有一个具有短于2048位的密钥。根据证书颁发机构/浏览器（CA/B）论坛制定的行业标准，2014年1月1日之后颁发的证书必须至少为2048位。一些浏览器SSL实现可能会在2014年1月1日之后拒绝小于2048位的密钥。此外，一些SSL证书供应商可能会在2014年1月1日之前吊销小于2048位的证书。请注意，如果在2010年12月31日之前颁发RSA密钥小于2048位的根证书，Nessus将不会标记这些根证书，因为标准认为它们是免税的。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.40 | 1433 |

* 加固建议：

用长度小于2048位的RSA密钥替换链中的证书，然后重新颁发由旧证书签名的所有证书。

* 1. 【紧急】体检系统（222.222.222.41）
     1. 【紧急】Microsoft SQL Server不支持的版本检测（远程检查）
* 漏洞描述：

根据其自我报告的版本号，不再支持在远程主机上安装Microsoft SQL Server。缺少支持意味着供应商不会发布产品的新安全修补程序。因此，它很可能包含安全漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.41 | 1433 |

* 加固建议：

升级到当前支持的Microsoft SQL Server版本。

* + 1. 【高危】SSL 2.0协议未禁用
* 漏洞描述：

远程服务使用SSL 2.0进行通信连接加密，根据公开的漏洞曝露报告，此版本的协议存在一些加密缺陷，并已废弃多年。攻击者可以利用这个漏洞发动中间人攻击或解密受此影响的客户端之间的通信内容。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.41 | 1433 |

* 加固建议：

禁用SSL 2.0，使用TLS 1.0或更高版本代替

* + 1. 【中危】SSL证书签名使用弱强度的哈希算法
* 漏洞描述：

远程服务器的SSL证书签名使用弱强度的哈希加密算法，例如MD2、MD4或者MD5。这些签名算法显示容易遭到破解。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.41 | 1433 |

* 加固建议：

联系证书认证机构发布新的证书。 如果服务器使用自签名证书，则可自己

* + 1. 【中危】允许SSL采用中强度加密
* 漏洞描述：

远程主机支持SSL使用的密码采用中强度解密，即使用的KEY解密长度至少64位，但少于112位。注意：如果攻击者在同一个物理网段，密码很容易暴露。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.41 | 1433 |
| 222.222.222.41 | 3389 |

* 加固建议：

重新设置受影响的应用程序，可能的话，避免使用中强度加密，改为强度较高的加密算法。

* + 1. 【中危】SSL证书主机名不匹配
* 漏洞描述：

SSL现有认证的commonName (CN)是供其它主机使用的。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.41 | 1433 |

* 加固建议：

为此项服务购买或生产一个合适的证书

* + 1. 【中危】SSL证书不被信任
* 漏洞描述：

此项服务的SSL证书不被信任。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.41 | 1433 |
| 222.222.222.41 | 3389 |

* 加固建议：

为此项服务购买或生成合适的证书

* + 1. 【中危】SSL自签名证书
* 漏洞描述：

服务器所使用的X.509签署的证书链不是权威的证书颁发机构所颁发的。这削弱了使用SSL的效果，因为任何人都可以建立一个中间人攻击远程主机。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.41 | 1433 |
| 222.222.222.41 | 3389 |

* 加固建议：

购买或者生成被认可的证书

* + 1. 【中危】SMB数字签名通信禁用
* 漏洞描述：

SMB 协议为 Microsoft 文件和打印共享以及许多其他网络操作（例如远程 Windows 管理）提供基础。为了防止在传输过程中修改 SMB 数据包的拦截攻击，SMB 协议支持对 SMB 数据包的数字签名。 主机禁用了SMB数字签名通信，这可能导致潜在攻击者针对SMB通信服务进行中间人攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.41 | 445 |

* 加固建议：

在本地策略中--安全选项设置如下： Microsoft 网络客户端：对通信进行数字签名（若服务器同意）（启用） Microsoft 网络服务器：对通信进行数字签名（若客户同意）（启用）

* + 1. 【中危】远程主机支持SSL RC4加密套件
* 漏洞描述：

远程主机在一个或多个支持使用RC4密码套件，RC4密码是有缺陷的生成伪随机流的字节数, 如果明文重复加密(如HTTP cookie),攻击者能够获得许多(即数以百万计)明文密文配对,攻击者可以获得密文后，对比获得明文。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.41 | 1433 |
| 222.222.222.41 | 3389 |

* 加固建议：

重新设置受影响的应用程序，可能的话，避免使用RC4密钥算法，可以考虑给浏览器或WEB服务支持的带有AES-GCM 的TLS 1.2，相关链接： http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/ http://www.imperva.com/docs/HII\_Attacking\_SSL\_when\_using\_RC4.pdf

* + 1. 【中危】SSLv3 POODLE 安全漏洞
* 漏洞描述：

支持SSLv3 协议的网站存在被中间人攻击的风险，“Poodle”攻击（全称为Padding Oracle On Downloaded Legacy Encryption）可以提取出SSL连接中的加密数据相应的明文信息。攻击者可以利用这个漏洞发动中间人攻击或解密受此影响的客户端之间的通信内容。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.41 | 1433 |

* 加固建议：

禁用SSL 3.0

* + 1. 【中危】TLS版本1.0协议检测
* 漏洞描述：

远程服务接受使用TLS 1.0加密的连接。TLS 1.0有许多密码设计缺陷。TLS 1.0的现代实现减轻了这些问题，但是像1.2和1.3这样的TLS的新版本是针对这些缺陷而设计的，应该尽可能使用。截至2020年3月31日，为TLS 1.2及更高版本启用的终结点将不再与主要web浏览器和主要供应商正常工作。PCI DSS v3.2要求在2018年6月30日之前完全禁用TLS 1.0，但POS POI终端（及其连接的SSL/TLS终端点）除外，这些终端可以被验证为不易受任何已知漏洞攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.41 | 1433 |
| 222.222.222.41 | 3389 |

* 加固建议：

启用对TLS 1.2和1.3的支持，并禁用对TLS 1.0的支持。

* + 1. 【低危】SSL证书链包含小于2048位的RSA密钥
* 漏洞描述：

远程主机发送的X.509证书中至少有一个具有短于2048位的密钥。根据证书颁发机构/浏览器（CA/B）论坛制定的行业标准，2014年1月1日之后颁发的证书必须至少为2048位。一些浏览器SSL实现可能会在2014年1月1日之后拒绝小于2048位的密钥。此外，一些SSL证书供应商可能会在2014年1月1日之前吊销小于2048位的证书。请注意，如果在2010年12月31日之前颁发RSA密钥小于2048位的根证书，Nessus将不会标记这些根证书，因为标准认为它们是免税的。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.41 | 1433 |

* 加固建议：

用长度小于2048位的RSA密钥替换链中的证书，然后重新颁发由旧证书签名的所有证书。

* 1. 【紧急】信息发布服务器（222.222.222.48）
     1. 【紧急】Apache版本低于2.2.15
* 漏洞描述：

Apache版本低，可能会受到多个漏洞影响。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级apache版本到2.2.15以上 http://httpd.apache.org/

* + 1. 【紧急】Apache版本于2.2.13导致“apr\_palloc”缓冲区溢出漏洞
* 漏洞描述：

Apache版本低，可能会受到“apr\_palloc”缓冲区溢出漏洞攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级apache版本到2.2.13以上 http://httpd.apache.org/security/vulnerabilities\_22.html

* + 1. 【紧急】当前PHP版本厂商已不支持
* 漏洞描述：

根据现有版本，远程主机安装的PHP版本不再被厂商支持，意味着不再发布相关的安全补丁包，结果可能存在多个安全漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级至当前的支持版本 http://php.net/eol.php https://wiki.php.net/rfc/releaseprocess

* + 1. 【紧急】Microsoft SQL Server不支持的版本检测（远程检查）
* 漏洞描述：

根据其自我报告的版本号，不再支持在远程主机上安装Microsoft SQL Server。缺少支持意味着供应商不会发布产品的新安全修补程序。因此，它很可能包含安全漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 49249 |

* 加固建议：

升级到当前支持的Microsoft SQL Server版本。

* + 1. 【紧急】OpenSSL版本已不再支持
* 漏洞描述：

当前主机的OpenSSL版本已不再受厂商支持，这意味着厂商不再为当前版本发布安全补丁包，即可能存在安全漏洞

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级版本至厂商支持的版本 相关链接： https://www.openssl.org/news/openssl-old-notes.html

* + 1. 【紧急】低版本的Windows系统
* 漏洞描述：

低版本的Windows系统

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 0 |

* 加固建议：

升级操作系统

* + 1. 【高危】OpenSSL版本低于0.9.8p / 1.0.0b，存在缓冲区溢出漏洞
* 漏洞描述：

OpenSSL是一种开放源码的SSL实现，用来实现网络通信的高强度加密，现被广泛地用于各种网络应用程序中。当TLS服务器中的多线程和内部缓存被启用时，OpenSSL 0.9.8f至0.9.8o版本，1.0.0版本，以及1.0.0a版本中的ssl/t1\_lib.c文件中存在多个竞争条件漏洞。远程攻击者可以借助能够触发堆缓冲区溢出的客户端数据执行任意代码。该漏洞与(1)TLS服务器名称扩展以及(2)椭圆曲线密码系统有关。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级 OpenSSL版本至0.9.8p / 1.0.0b及以上版本。 相关链接： http://openssl.org/news/secadv\_20101116.txt

* + 1. 【高危】SSL 2.0协议未禁用
* 漏洞描述：

远程服务使用SSL 2.0进行通信连接加密，根据公开的漏洞曝露报告，此版本的协议存在一些加密缺陷，并已废弃多年。攻击者可以利用这个漏洞发动中间人攻击或解密受此影响的客户端之间的通信内容。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 443 |

* 加固建议：

禁用SSL 2.0，使用TLS 1.0或更高版本代替

* + 1. 【高危】当前Web Server版本厂商已不再支持
* 漏洞描述：

根据现有版本，远程主机web服务已不在厂商支持范围内，缺少厂商的支持，意味着没有新的安全补丁包发布，结果主机存在多个安全威胁。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |
| 222.222.222.48 | 81 |

* 加固建议：

如果不需要此项服务，关闭它。如果可能，升级新的版本，或更换其它的Web服务器。

* + 1. 【高危】Apache 版本低于 2.2.12
* 漏洞描述：

Apache版本较低，导致存在多处漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级apache版本到2.2.12以上 http://httpd.apache.org/

* + 1. 【高危】PHP版本低于5.2.11
* 漏洞描述：

Apache版本低，可能会受到多个漏洞影响。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级PHP版本到5.2.11以上

* + 1. 【高危】Apache版本低于2.2.14
* 漏洞描述：

Apache版本较低，导致存在多处漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级apache版本到2.2.29以上 http://httpd.apache.org/

* + 1. 【高危】PHP版本低于5.2.14
* 漏洞描述：

Apache版本低，可能会受到多个漏洞影响。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级PHP版本到5.2.14以上

* + 1. 【高危】OpenSSL版本低于0.9.8s，存在多个安全漏洞
* 漏洞描述：

主机OpenSSL版本低于0.9.8s,这使得主机存在多个安全漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级OpenSSL版本至0.9.8s及以上版本，或者使用厂家发布的补丁包进行升级 相关链接： http://openssl.org/news/secadv\_20120104.txt http://www.openssl.org/news/changelog.html http://www.nessus.org/u?c0f10f36 http://eprint.iacr.org/2011/232.pdf http://cvs.openssl.org/chngview?cn=21301

* + 1. 【高危】PHP版本低于5.3.9 导致多个漏洞
* 漏洞描述：

Apache版本低，可能会受到多个漏洞影响。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级PHP版本到5.3.9以上

* + 1. 【高危】OpenSSL版本低于0.9.8w，ASN.1 asn1\_d2i\_read\_bio内存破坏漏洞
* 漏洞描述：

OpenSSL是一种开放源码的SSL实现，用来实现网络通信的高强度加密，现在被广泛地用于各种网络应用程序中。 （1）OpenSSL 0.9.8v之前版本，1.0.0i之前的1.0.0版本和1.0.1a之前的1.0.1版本中的asn1\_d2i\_read\_bio函数中存在漏洞，该漏洞源于未正确解释整数数据。远程攻击者可利用该漏洞借助特制DER数据导致缓冲区溢出攻击，拒绝服务（内存破坏）或造成其他未明影响。此漏洞已被X.509证书或RSA公钥证实。 （2）OpenSSL 0.9.8v版本中的crypto/buffer/buffer.c中存在多个整数字符串错误漏洞。远程攻击者可利用这些漏洞借助特制DER数据导致缓冲区溢出攻击，造成拒绝服务（内存损坏）或可能有其他未明影响。该漏洞已被X.509证书或RSA公钥证实。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级OpenSSL版本至0.9.8w及以上版本 相关链接： http://openssl.org/news/secadv\_20120419.txt http://seclists.org/fulldisclosure/2012/Apr/210 http://openssl.org/news/secadv\_20120424.txt http://cvs.openssl.org/chngview?cn=22479 http://www.openssl.org/news/changelog.html

* + 1. 【高危】PHP版本低于5.3.12 / 5.4.2导致CGI查询语句代码执行漏洞
* 漏洞描述：

PHP版本较低，可能导致CGI查询语句代码执行漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级PHP版本到5.4.2以上 http://httpd.apache.org/

* + 1. 【高危】Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 多个漏洞
* 漏洞描述：

此版本受到以下漏洞影响： - httpd中存在身份验证绕过漏洞 由于第三方模块使用 ap\_get\_basic\_auth\_pw（）函数之外 验证阶段。远程攻击者可以利用此来绕过身份验证 要求。 （CVE-2017-3167） - httpd由于存在拒绝服务漏洞 一个NULL指针解除引用的缺陷，当 第三方模块调用mod\_ssl 一个HTTP期间的ap\_hook\_process\_connection（）函数 请求HTTPS端口。远程攻击者可以利用这一点导致拒绝服务 条件。 （CVE-2017-3169） - httpd由于存在拒绝服务漏洞 ap\_find\_token（）中的out-of-bounds读取错误 在特殊处理时触发的功能 制作的请求头序列。 远程攻击者可以利用这个来破坏它 服务或强制ap\_find\_token（）返回一个不正确的 值。 （CVE-2017-7668） - httpd由于存在拒绝服务漏洞 mod\_mime中出现超出范围的读取错误 在处理特制Content-Type时触发 响应头。远程攻击者可以 利用这一点来披露敏感信息或原因 拒绝服务条件。 （CVE-2017-7679） - httpd由于存在拒绝服务漏洞 无法初始化或重置值占位符 在[代理 - ]授权标题类型'Digest'之前 或在连续的键=值分配之间 mod\_auth\_digest的。远程攻击者可以 利用这个，通过提供没有'='的初始密钥 转让，披露敏感信息或导致 拒绝服务条件。 （CVE-2017-9788）

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级Apache版本至2.2.33-dev / 2.4.26或之后的版本

* + 1. 【高危】Apache 2.2.x < 2.2.34 多个漏洞
* 漏洞描述：

此版本受到以下漏洞的影响： - 由于存在身份验证绕过漏洞 第三方模块使用ap\_get\_basic\_auth\_pw（） 功能在认证阶段之外。远程攻击者可以利用这一点 旁路认证要求。 （CVE-2017-3167） - 由于存在NULL指针解除引用缺陷 第三方模块调用mod\_ssl 一个HTTP期间的ap\_hook\_process\_connection（）函数 请求HTTPS端口。远程攻击者可以利用这一点导致拒绝服务 条件。 （CVE-2017-3169） - mod\_http2中存在NULL指针解引用缺陷 在处理特制HTTP / 2时被触发 请求。远程攻击者可以利用这导致拒绝服务条件。注意 此漏洞不影响2.2.x. （CVE-2017-7659） - 存在超出范围的读取错误 ap\_find\_token（）函数由于处理不当而导致 标题序列。远程攻击者可以通过一个特制的标题来利用这个 导致拒绝服务条件。 （CVE-2017-7668） - 由于mod\_mime，存在超出限制的读取错误 Content-Type响应标头的不当处理。远程攻击者可以通过a进行利用 特制的Content-Type响应头，引起拒绝服务条件或披露 敏感信息。 （CVE-2017-7679）

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

2.2.34升级Apache版本至2.2.34或之后的版本

* + 1. 【中危】SSL证书过期
* 漏洞描述：

远程主机的SSL证书已经过期。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 443 |

* 加固建议：

购买或生成一个新的SSL证书来替换现有的。

* + 1. 【中危】OpenSSL版本低于0.9.8j，存在签名验证漏洞
* 漏洞描述：

OpenSSL是一种开放源码的SSL实现，用来实现网络通信的高强度加密，现在被广泛地用于各种网络应用程序中。某些OpenSSL函数在验证DSA和ECDSA密钥签名时没有正确地验证函数EVP\_VerifyFinal()的返回值，畸形的签名可能被处理为有效签名而不是错误。恶意服务器或中间人攻击者可以在证书链中向客户端特制SSL/TLS签名来绕过有效性验证，诱骗客户端错误的信任恶意站点。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级OpenSSL版本至0.9.8j及以上版本 相关链接： http://www.us-cert.gov/cas/techalerts/TA09-133A.html

* + 1. 【中危】OpenSSL版本低于0.9.8k，存在拒绝服务攻击漏洞
* 漏洞描述：

主机OpenSSL版本低于0.9.8K,这使得远程攻击者通过伪造ASN.1数据发起拒绝服务攻击

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级OpenSSL版本至0.9.8k及以上版本 相关链接： http://www.openssl.org/news/secadv\_20090325.txt

* + 1. 【中危】OpenSSL版本低于0.9.8l，存在多个安全漏洞
* 漏洞描述：

主机OpenSSL版本低于0.9.8l,这使得主机存在多个安全漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级OpenSSL版本至0.9.8l及以上版本 相关链接： http://voodoo-circle.sourceforge.net/sa/sa-20090326-01.html http://www.openssl.org/news/secadv\_20090325.txt http://voodoo-circle.sourceforge.net/sa/sa-20091012-01.html http://rt.openssl.org/Ticket/Display.html?id=1930&user=guest&pass=guest http://rt.openssl.org/Ticket/Display.html?id=1931&user=guest&pass=guest http://cvs.openssl.org/chngview?cn=18187 http://cvs.openssl.org/chngview?cn=18188

* + 1. 【中危】OpenSSL版本低于0.9.8p / 1.0.0e，存在双重释放漏洞
* 漏洞描述：

OpenSSL是一种开放源码的SSL实现，用来实现网络通信的高强度加密，现在被广泛地用于各种网络应用程序中。OpenSSL 1.0.0a，0.9.8，0.9.7版本和其他可能版本中的OpenSSL客户端(ssl/s3\_clnt.c)中的ssl3\_get\_key\_exchange函数存在双重释放漏洞，当ECDH启用时，附近攻击者可以借助特制的无效质数私钥导致拒绝服务（崩溃）。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级 OpenSSL版本至0.9.8p / 1.0.0e及以上版本。 相关链接： http://www.mail-archive.com/openssl-dev@openssl.org/msg28049.html

* + 1. 【中危】SSL 允许采用弱加密组件
* 漏洞描述：

远程主机支持采用弱加密或完全不用加密的SSL加密。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 443 |

* 加固建议：

重新配置可能受影响的应用程序；如果可能，避免使用弱加密。

* + 1. 【中危】SSL证书签名使用弱强度的哈希算法
* 漏洞描述：

远程服务器的SSL证书签名使用弱强度的哈希加密算法，例如MD2、MD4或者MD5。这些签名算法显示容易遭到破解。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 3389 |
| 222.222.222.48 | 49249 |

* 加固建议：

联系证书认证机构发布新的证书。 如果服务器使用自签名证书，则可自己

* + 1. 【中危】PHP版本低于5.2.9
* 漏洞描述：

PHP版本低于5.2.9，可能会受到多个漏洞影响。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级PHP版本到5.2.9以上

* + 1. 【中危】PHP版本低于5.2.10 ，导致多个漏洞
* 漏洞描述：

PHP版本低，可能会受到多个漏洞影响。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级PHP版本到5.2.10以上

* + 1. 【中危】允许SSL采用中强度加密
* 漏洞描述：

远程主机支持SSL使用的密码采用中强度解密，即使用的KEY解密长度至少64位，但少于112位。注意：如果攻击者在同一个物理网段，密码很容易暴露。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 443 |

* 加固建议：

重新设置受影响的应用程序，可能的话，避免使用中强度加密，改为强度较高的加密算法。

* + 1. 【中危】SSL/TLS握手过程中间人明文注入攻击
* 漏洞描述：

在SSL/TLS握手协议连接过程中，数据通信过程采用明文数据，这可能遭受中间人攻击，攻击者通过篡改明文数据，实现伪装。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 443 |

* 加固建议：

联系厂商获取相关补丁包。 http://www.ietf.org/mail-archive/web/tls/current/msg03948.html http://www.g-sec.lu/practicaltls.pdf http://tools.ietf.org/html/rfc5746

* + 1. 【中危】PHP版本低导致多个漏洞
* 漏洞描述：

Apache版本低，可能会受到多个漏洞影响。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级PHP版本到5.2.12以上

* + 1. 【中危】PHP版本低于5.3.2 / 5.2.13
* 漏洞描述：

Apache版本低，可能会受到多个漏洞影响。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级PHP版本到5.3.2以上

* + 1. 【中危】FileZilla版本低于0.9.31 导致拒绝服务攻击漏洞
* 漏洞描述：

经过测试，发现服务器上FileZilla版本低于0.9.31，这种版本的SSL代码未知漏洞可被远程攻击者引发拒绝服务的情况。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 21 |

* 加固建议：

升级到FileZilla到0.9.31或者更新版本

* + 1. 【中危】SSL证书主机名不匹配
* 漏洞描述：

SSL现有认证的commonName (CN)是供其它主机使用的。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 443 |
| 222.222.222.48 | 49249 |

* 加固建议：

为此项服务购买或生产一个合适的证书

* + 1. 【中危】Apache版本低于2.2.16
* 漏洞描述：

Apache版本较低，导致存在多处漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级apache版本到2.2.16以上 http://httpd.apache.org/

* + 1. 【中危】Apache版本较低于2.2.17
* 漏洞描述：

Apache版本较低，导致存在多处漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级apache版本到2.2.17以上 http://httpd.apache.org/

* + 1. 【中危】PHP版本低于5.2.15
* 漏洞描述：

Apache版本低，可能会受到多个漏洞影响。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级PHP版本到5.2.15以上

* + 1. 【中危】SSL证书不被信任
* 漏洞描述：

此项服务的SSL证书不被信任。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 3389 |
| 222.222.222.48 | 443 |
| 222.222.222.48 | 49249 |

* 加固建议：

为此项服务购买或生成合适的证书

* + 1. 【中危】PHP 版本低于5.2.17 / 5.3 < 5.3.5 拒绝服务攻击漏洞
* 漏洞描述：

PHP版本低于5.2.17或低于5.3.5，这可能受到拒绝服务攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级PHP版本至5.3.5及以上版本。

* + 1. 【中危】OpenSSL密码集降级安全漏洞
* 漏洞描述：

OpenSSL是一种开放源码的SSL实现，用来实现网络通信的高强度加密，现在被广泛地用于各种网络应用程序中。当SSL\_OP\_NETSCAPE\_REUSE\_CIPHER\_CHANGE\_BUG启用时，OpenSSL 0.9.8q之前版本及1.0.0c之前的1.0.x版本不能正确阻止会话缓存中对加密套接字的修改。远程攻击者可借助和嗅探网络通信以发现会话标识符有关的向量强迫意外密码降低保密程度。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 443 |

* 加固建议：

升级版本至 OpenSSL 0.9.8q / 1.0.0.c或者联系厂商。 相关链接： http://openssl.org/news/secadv\_20101202.txt

* + 1. 【中危】Apache版本低于2.2.18
* 漏洞描述：

Apache版本较低，由于发生在 'apr\_fnmatch'函数的错误，可能会受到DOS攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

确保 'IndexOptions' 设置选项设置为 'IgnoreClient'，或者升级Apache版本至2.2.18及以上。

* + 1. 【中危】Apache版本低于2.2.21 导致mod\_proxy\_ajp 漏洞
* 漏洞描述：

Apache版本较低，由于发生在 'mod\_proxy\_ajp '函数的错误，可能会受到DOS攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级Apache版本至2.2.21及以上。

* + 1. 【中危】SSL自签名证书
* 漏洞描述：

服务器所使用的X.509签署的证书链不是权威的证书颁发机构所颁发的。这削弱了使用SSL的效果，因为任何人都可以建立一个中间人攻击远程主机。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 3389 |
| 222.222.222.48 | 443 |
| 222.222.222.48 | 49249 |

* 加固建议：

购买或者生成被认可的证书

* + 1. 【中危】Apache版本低于2.2.22
* 漏洞描述：

Apache版本较低，导致存在多处漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级apache版本到2.2.22以上 http://httpd.apache.org/

* + 1. 【中危】OpenSSL版本低于0.9.9s，存在多个安全漏洞
* 漏洞描述：

主机OpenSSL版本低于0.9.9u,这使得主机存在多个安全漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级OpenSSL版本至0.9.8u及以上版本，或者使用厂家发布的补丁包进行升级 相关链接： http://marc.info/?l=openssl-dev&amp;m=115685408414194&amp;w=2 http://openssl.org/news/secadv\_20120312.txt http://www.openssl.org/news/changelog.html http://www.openwall.com/lists/oss-security/2012/03/13/2 http://www.openwall.com/lists/oss-security/2012/02/28/14 http://www.nessus.org/u?4a3e3c8e http://rt.openssl.org/Ticket/Display.html?id=2711&user=guest&pass=guest

* + 1. 【中危】PHP版本低于5.3.11导致多个漏洞
* 漏洞描述：

Apache版本低，可能会受到多个漏洞影响。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级PHP版本到5.3.11以上

* + 1. 【中危】OpenSSL版本低于0.9.8x，DTLS CBC拒绝服务攻击漏洞
* 漏洞描述：

OpenSSL是一种开放源码的SSL实现，用来实现网络通信的高强度加密，现在被广泛地用于各种网络应用程序中。 OpenSSL 0.9.8x之前版本，1.0.0j之前的1.0.0版本以及1.0.1c之前的1.0.1版本中存在整数下溢漏洞，该漏洞源于TLS 1.1版本、TLS 1.2版本或者DTLS用于CBC加密。远程攻击者可利用该漏洞借助在某些明确IV计算过程中未正确处理的特制TLS数据包导致拒绝服务（缓冲区越界读取），或者产生其他未明影响。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级OpenSSL版本至0.9.8x及以上版本 相关链接： http://openssl.org/news/secadv\_20120510.txt http://www.openssl.org/news/changelog.html http://cvs.openssl.org/chngview?cn=22538 https://bugzilla.redhat.com/show\_bug.cgi?id=820686

* + 1. 【中危】Apache版本低于2.2.23
* 漏洞描述：

Apache版本较低，导致存在多处漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级apache版本到2.2.23以上 http://httpd.apache.org/

* + 1. 【中危】Apache版本低于2.2.24导致多个XSS漏洞
* 漏洞描述：

Apache版本低于2.2.24导致多个XSS漏洞，主要为以下模块：mod\_info, mod\_status, mod\_imagemap, mod\_ldap, and mod\_proxy\_ftp

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级Apache版本至2.2.24及以上。

* + 1. 【中危】远程主机支持SSL RC4加密套件
* 漏洞描述：

远程主机在一个或多个支持使用RC4密码套件，RC4密码是有缺陷的生成伪随机流的字节数, 如果明文重复加密(如HTTP cookie),攻击者能够获得许多(即数以百万计)明文密文配对,攻击者可以获得密文后，对比获得明文。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 443 |

* 加固建议：

重新设置受影响的应用程序，可能的话，避免使用RC4密钥算法，可以考虑给浏览器或WEB服务支持的带有AES-GCM 的TLS 1.2，相关链接： http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/ http://www.imperva.com/docs/HII\_Attacking\_SSL\_when\_using\_RC4.pdf

* + 1. 【中危】Apache版本低于2.2.25
* 漏洞描述：

Apache版本较低，导致存在多处漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级apache版本到2.2.25以上 http://httpd.apache.org/

* + 1. 【中危】PHP\_RSHUTDOWN\_FUNCTION模块绕过漏洞
* 漏洞描述：

PHP 5.x版本中的‘libxml RSHUTDOWN’函数中存在信息泄露漏洞。远程攻击者可通过调用stream\_close方法利用该漏洞绕过open\_basedir保护机制，读取任意文件。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级PHP版本至5.3.11 / 5.4.1及以上。

* + 1. 【中危】Apache版本2.2 低于2.2.27 导致多个漏洞
* 漏洞描述：

Apache版本低，可能会受到多个漏洞影响。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级apache版本到2.2.27以上 http://httpd.apache.org/

* + 1. 【中危】OpenSSL版本低于0.9.8za，存在多种安全漏洞
* 漏洞描述：

主机OpenSSL版本低于0.9.8za,这使得主机存在多个安全漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级OpenSSL版本至0.9.8za及以上版本。 相关链接： http://www.openssl.org/news/vulnerabilities.html#2014-0076 http://www.openssl.org/news/vulnerabilities.html#CVE-2014-0221 http://www.openssl.org/news/vulnerabilities.html#CVE-2014-0224 http://www.openssl.org/news/vulnerabilities.html#CVE-2014-3470 http://www.openssl.org/news/secadv\_20140605.txt http://ccsinjection.lepidum.co.jp/ https://www.imperialviolet.org/2014/06/05/earlyccs.html

* + 1. 【中危】OpenSSL版本低于0.9.8zb，存在多种安全漏洞
* 漏洞描述：

主机OpenSSL版本低于0.9.8zb,这使得主机存在多个安全漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级OpenSSL版本至0.9.8zB及以上版本。 相关链接： https://www.openssl.org/news/openssl-0.9.8-notes.html https://www.openssl.org/news/secadv\_20140806.txt https://www.openssl.org/news/vulnerabilities.html

* + 1. 【中危】Apache版本2.2 低于2.2.28
* 漏洞描述：

Apache版本较低，导致存在多处漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级apache版本到2.2.28以上 http://httpd.apache.org/

* + 1. 【中危】SSLv3 POODLE 安全漏洞
* 漏洞描述：

支持SSLv3 协议的网站存在被中间人攻击的风险，“Poodle”攻击（全称为Padding Oracle On Downloaded Legacy Encryption）可以提取出SSL连接中的加密数据相应的明文信息。攻击者可以利用这个漏洞发动中间人攻击或解密受此影响的客户端之间的通信内容。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 443 |

* 加固建议：

禁用SSL 3.0

* + 1. 【中危】OpenSSL版本低于0.9.8zc，存在多种安全漏洞
* 漏洞描述：

主机OpenSSL版本低于0.9.8zc,这使得主机存在多个安全漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级OpenSSL版本至0.9.8zc及以上版本。 相关链接： https://www.openssl.org/news/openssl-0.9.8-notes.html https://www.openssl.org/news/secadv\_20141015.txt https://www.openssl.org/news/vulnerabilities.html https://www.imperialviolet.org/2014/10/14/poodle.html https://www.openssl.org/~bodo/ssl-poodle.pdf https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

* + 1. 【中危】OpenSSL版本低于0.9.8zd，存在多个安全漏洞
* 漏洞描述：

OpenSSL版本低于0.9.8zd，存在多个安全漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级OpenSSL版本至0.9.8zd 及以上。 相关链接： https://www.openssl.org/news/openssl-0.9.8-notes.html https://www.openssl.org/news/secadv\_20150108.txt https://www.openssl.org/news/vulnerabilities.html https://www.smacktls.com/#freak

* + 1. 【中危】Jetty HttpParser错误远程内存泄漏
* 漏洞描述：

Jetty的远程实例受到HttpParser模块中远程内存泄漏漏洞的影响，该漏洞是由于头值中非法字符的处理不正确造成的。当HTTP请求中遇到非法字符时，Jetty会在前一个请求中使用的共享缓冲区中写入响应。Jetty对客户机的响应包括这个共享缓冲区，其中包含来自上一个请求的潜在敏感数据。攻击者使用包含可变长度非法字符字符串的巧尽心思构建的请求，可以窃取敏感的头数据（例如cookie、身份验证令牌）或敏感的POST数据（例如凭据）。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 86 |

* 加固建议：

升级至Jetty 9.2.9.v20150224或更高版本。对于Jetty 9.3.x，请联系供应商寻求解决方案。

* + 1. 【中危】SSL/TLS EXPORT\_RSA密钥算法位数小于或等于512位
* 漏洞描述：

远程主机运行着弱密钥算法，攻击者可以在短时间内破解密文。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 443 |

* 加固建议：

重新设置服务，或移除支持EXPORT\_RSA的密钥层。 相关链接： https://www.smacktls.com/#freak https://www.openssl.org/news/secadv\_20150108.txt http://www.nessus.org/u?b78da2c4

* + 1. 【中危】OpenSSL版本低于0.9.9zf，存在多个安全漏洞
* 漏洞描述：

OpenSSL版本低于0.9.9zf，存在多个安全漏洞

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级OpenSSL版本至0.9.8zf及以上。 相关链接： https://www.openssl.org/news/secadv\_20150319.txt

* + 1. 【中危】OpenSSL BN\_GF2m\_mod\_inv函数拒绝服务漏洞
* 漏洞描述：

OpenSSL是一种开放源码的SSL实现，用来实现网络通信的高强度加密，现在被广泛地用于各种网络应用程序中。OpenSSL 0.9.8s、1.0.0e、1.0.1n、1.0.2b之前版本，crypto/bn/bn\_gf2m.c内的函数BN\_GF2m\_mod\_inv没有正确处理ECParameters结构，远程攻击者通过使用Elliptic Curve算法的会话，利用此漏洞可造成拒绝服务(无限循环）。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

OpenSSL Project已经为此发布了一个安全公告（secadv\_20150611）以及相应补丁: secadv\_20150611：OpenSSL Security Advisory [11 Jun 2015] 链接：https://www.openssl.org/news/secadv\_20150611.txt

* + 1. 【中危】OpenSSL 0.9.8 <0.9.8zh X509\_ATTRIBUTE内存泄漏DoS
* 漏洞描述：

根据其banner判断，远程主机正在运行一个0.9.8zh版本之前的OpenSSL 0.9.8。 此版本受到与处理格式错误的X509\_ATTRIBUTE结构相关的文件tasn\_dec.c中的ASN1\_TFLG\_COMBINE实现中的缺陷的影响。 远程攻击者可以通过触发解码失败来利用这个漏洞在PKCS＃7或CMS应用程序中引起内存泄漏，导致拒绝服务。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级到OpenSSL 0.9.8zh或更高版本。

* + 1. 【中危】SSL DROWN攻击漏洞（解密RSA（使用过时的弱加密算法））
* 漏洞描述：

远程主机受到此漏洞影响，可允许远程攻击者试图解密捕获的TLS流量。 SSLv2协议中存在一个填充内容缺陷，攻击者可以利用这个缺陷解密使用新版SSL/TLS协议会话中由RSA算法加密的内容。通过这种利用方式，可造成DROWN攻击。 受影响的版本：Apache(非2.4.X版本)、Nginx(0.7.64、0.8.18及更早版本)、Postfix（早于2.9.14、2.10.8、2.11.6、3.0.2的版本 (在2015.07.20之前发布)）、Openssl: 1.0.2a、1.0.1m、1.0.0r、0.9.8zf及更早版本。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 443 |

* 加固建议：

1、升级OpenSSL软件包： （1）.CentOS、Redhat 可以通过以下命令来升级 #yum clean #yum update openssl 对应的RPM包： CentOS 5: openssl-0.9.8e-39.el5\_11、openssl-devel-0.9.8e-39.el5\_11、 openssl-perl-0.9.8e-39.el5\_11 CentOS 6:openssl-1.0.1e-42.el6\_7.4、openssl-devel-1.0.1e-42.el6\_7.4、openssl-perl-1.0.1e-42.el6\_7.4、 openssl-static-1.0.1e-42.el6\_7.4 CentOS 7:openssl-1.0.1e-51.el7\_2.4、openssl-devel-1.0.1e-51.el7\_2.4、openssl-libs-1.0.1e-51.el7\_2.4、openssl-perl-1.0.1e-51.el7\_2.4、openssl-static-1.0.1e-51.el7\_2.4 (2). ubuntu 版本可以通过以下命令来升级 #apt-get upgrade openssl 2、禁用 Apache、Nginx、Postfix 中的SSLv2 在Apache 的 SSL 配置文件中禁用SSLv2 SSLProtocol all -SSLv2 重启apache服务 在 Nginx 的 SSL 配置文件中设置只允许使用 TLS 协议： ssl\_protocols TLSv1 TLSv1.1 TLSv1.2; 重启nginx服务 在Postfix配置中禁用SSLv2 # Minimal recommended settings. Whenever the built-in defaults are # sufficient, let the built-in defaults stand by deleting any explicit # overrides. The default mandatory TLS protocols have never included # SSLv2, check to make sure you have not inadvertently enabled it. smtpd\_tls\_protocols = !SSLv2, !SSLv3 smtpd\_tls\_mandatory\_protocols = !SSLv2, !SSLv3 tlsproxy\_tls\_protocols = $smtpd\_tls\_protocols tlsproxy\_tls\_mandatory\_protocols = $smtpd\_tls\_mandatory\_protocols smtp\_tls\_protocols = !SSLv2, !SSLv3 smtp\_tls\_mandatory\_protocols = !SSLv2, !SSLv3 lmtp\_tls\_protocols = !SSLv2, !SSLv3 lmtp\_tls\_mandatory\_protocols = !SSLv2, !SSLv3 smtpd\_tls\_ciphers = medium smtp\_tls\_ciphers = medium # Other best practices # Strongly recommended: # http://www.postfix.org/FORWARD\_SECRECY\_README.html#server\_fs smtpd\_tls\_dh1024\_param\_file=${config\_directory}/dh2048.pem smtpd\_tls\_eecdh\_grade = strong # Suggested, not strictly needed: smtpd\_tls\_exclude\_ciphers = EXPORT, LOW, MD5, SEED, IDEA, RC2 smtp\_tls\_exclude\_ciphers = EXPORT, LOW, MD5, aDSS, kECDHe, kECDHr, kDHd, kDHr, SEED, IDEA, RC2

* + 1. 【中危】TLS版本1.0协议检测
* 漏洞描述：

远程服务接受使用TLS 1.0加密的连接。TLS 1.0有许多密码设计缺陷。TLS 1.0的现代实现减轻了这些问题，但是像1.2和1.3这样的TLS的新版本是针对这些缺陷而设计的，应该尽可能使用。截至2020年3月31日，为TLS 1.2及更高版本启用的终结点将不再与主要web浏览器和主要供应商正常工作。PCI DSS v3.2要求在2018年6月30日之前完全禁用TLS 1.0，但POS POI终端（及其连接的SSL/TLS终端点）除外，这些终端可以被验证为不易受任何已知漏洞攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 3389 |
| 222.222.222.48 | 443 |
| 222.222.222.48 | 49249 |

* 加固建议：

启用对TLS 1.2和1.3的支持，并禁用对TLS 1.0的支持。

* + 1. 【中危】PHP<7.3.24多个漏洞
* 漏洞描述：

根据其自报的版本号，在远程web服务器上运行的PHP版本早于7.3.24。因此，它受到多个漏洞的影响

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级至PHP版本7.3.24或更高版本。

* + 1. 【低危】OpenSSL<0.9.8k签名否认
* 漏洞描述：

根据它的横幅，远程服务器运行的是早于0.9.8k的OpenSSL版本。因此，它可以允许有效的签名生成无效的签名，这些签名看起来是有效的，并且可以在以后被拒绝。这只影响CMS用户。CMS出现在openssl0.9.8h中。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级至OpenSSL 0.9.8k或更高版本。

* + 1. 【低危】OpenSSL版本低于0.9.8y，存在多个安全漏洞
* 漏洞描述：

主机OpenSSL版本低于0.9.8y,这使得主机存在多个安全漏洞。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 80 |

* 加固建议：

升级OpenSSL版本至0.9.8y及以上版本，或者使用厂家发布的补丁包进行升级 相关链接： http://www.openssl.org/news/secadv\_20130204.txt

* + 1. 【低危】SSL证书链包含小于2048位的RSA密钥
* 漏洞描述：

远程主机发送的X.509证书中至少有一个具有短于2048位的密钥。根据证书颁发机构/浏览器（CA/B）论坛制定的行业标准，2014年1月1日之后颁发的证书必须至少为2048位。一些浏览器SSL实现可能会在2014年1月1日之后拒绝小于2048位的密钥。此外，一些SSL证书供应商可能会在2014年1月1日之前吊销小于2048位的证书。请注意，如果在2010年12月31日之前颁发RSA密钥小于2048位的根证书，Nessus将不会标记这些根证书，因为标准认为它们是免税的。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 49249 |

* 加固建议：

用长度小于2048位的RSA密钥替换链中的证书，然后重新颁发由旧证书签名的所有证书。

* + 1. 【低危】SSL/TLS EXPORT\_DHE密钥算法位数小于或等于512位
* 漏洞描述：

远程主机运行的EXPORT\_DHE密钥算法小于或等于512位，通过密文分析，第三方攻击者可以在短时间内获取共享密钥。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.48 | 443 |

* 加固建议：

重新设置服务，或移除支持EXPORT\_DHE的密钥层。 相关链接： https://weakdh.org/

* 1. 【紧急】LIS系统（222.222.222.62）
     1. 【紧急】当前ORACLE数据库版本厂商已不支持
* 漏洞描述：

根据远程主机安装的数据库版本，厂家已不再支持，将会缺少安全补丁包，因此，可能存在安全威胁。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.62 | 1521 |

* 加固建议：

升级数据库版本至当前最新版本，至少升级至厂家支持的版本。

* + 1. 【高危】Oracle TNS侦听器远程毒化
* 漏洞描述：

Oracle Database Server是一个对象关系数据库管理系统。 Oracle Database Server在实现上存在可允许攻击者向远程“TNS Listener”组件处理的数据投毒的漏洞。攻击者可利用此漏洞将数据库服务器的合法“TNS Listener”组件中的数据转向到攻击者控制的系统，导致控制远程组件的数据库实例，造成组件和合法数据库之间的攻击者攻击、会话劫持或拒绝服务攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.62 | 1521 |

* 加固建议：

目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://www.oracle.com/technetwork/topics/security/alert-cve-2012-1675-1608180.html

* + 1. 【中危】SSL证书签名使用弱强度的哈希算法
* 漏洞描述：

远程服务器的SSL证书签名使用弱强度的哈希加密算法，例如MD2、MD4或者MD5。这些签名算法显示容易遭到破解。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.62 | 3389 |

* 加固建议：

联系证书认证机构发布新的证书。 如果服务器使用自签名证书，则可自己

* + 1. 【中危】允许SSL采用中强度加密
* 漏洞描述：

远程主机支持SSL使用的密码采用中强度解密，即使用的KEY解密长度至少64位，但少于112位。注意：如果攻击者在同一个物理网段，密码很容易暴露。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.62 | 3389 |

* 加固建议：

重新设置受影响的应用程序，可能的话，避免使用中强度加密，改为强度较高的加密算法。

* + 1. 【中危】SSL证书不被信任
* 漏洞描述：

此项服务的SSL证书不被信任。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.62 | 3389 |

* 加固建议：

为此项服务购买或生成合适的证书

* + 1. 【中危】SSL自签名证书
* 漏洞描述：

服务器所使用的X.509签署的证书链不是权威的证书颁发机构所颁发的。这削弱了使用SSL的效果，因为任何人都可以建立一个中间人攻击远程主机。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.62 | 3389 |

* 加固建议：

购买或者生成被认可的证书

* + 1. 【中危】TLS版本1.0协议检测
* 漏洞描述：

远程服务接受使用TLS 1.0加密的连接。TLS 1.0有许多密码设计缺陷。TLS 1.0的现代实现减轻了这些问题，但是像1.2和1.3这样的TLS的新版本是针对这些缺陷而设计的，应该尽可能使用。截至2020年3月31日，为TLS 1.2及更高版本启用的终结点将不再与主要web浏览器和主要供应商正常工作。PCI DSS v3.2要求在2018年6月30日之前完全禁用TLS 1.0，但POS POI终端（及其连接的SSL/TLS终端点）除外，这些终端可以被验证为不易受任何已知漏洞攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.62 | 3389 |

* 加固建议：

启用对TLS 1.2和1.3的支持，并禁用对TLS 1.0的支持。

* 1. 【紧急】HIS系统（222.222.222.91）
     1. 【紧急】当前ORACLE数据库版本厂商已不支持
* 漏洞描述：

根据远程主机安装的数据库版本，厂家已不再支持，将会缺少安全补丁包，因此，可能存在安全威胁。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.91 | 1521 |

* 加固建议：

升级数据库版本至当前最新版本，至少升级至厂家支持的版本。

* + 1. 【高危】Oracle TNS侦听器远程毒化
* 漏洞描述：

Oracle Database Server是一个对象关系数据库管理系统。 Oracle Database Server在实现上存在可允许攻击者向远程“TNS Listener”组件处理的数据投毒的漏洞。攻击者可利用此漏洞将数据库服务器的合法“TNS Listener”组件中的数据转向到攻击者控制的系统，导致控制远程组件的数据库实例，造成组件和合法数据库之间的攻击者攻击、会话劫持或拒绝服务攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.91 | 1521 |

* 加固建议：

目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://www.oracle.com/technetwork/topics/security/alert-cve-2012-1675-1608180.html

* + 1. 【中危】SSL证书签名使用弱强度的哈希算法
* 漏洞描述：

远程服务器的SSL证书签名使用弱强度的哈希加密算法，例如MD2、MD4或者MD5。这些签名算法显示容易遭到破解。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.91 | 5000 |

* 加固建议：

联系证书认证机构发布新的证书。 如果服务器使用自签名证书，则可自己

* + 1. 【中危】允许SSL采用中强度加密
* 漏洞描述：

远程主机支持SSL使用的密码采用中强度解密，即使用的KEY解密长度至少64位，但少于112位。注意：如果攻击者在同一个物理网段，密码很容易暴露。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.91 | 5000 |

* 加固建议：

重新设置受影响的应用程序，可能的话，避免使用中强度加密，改为强度较高的加密算法。

* + 1. 【中危】SSL证书不被信任
* 漏洞描述：

此项服务的SSL证书不被信任。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.91 | 5000 |

* 加固建议：

为此项服务购买或生成合适的证书

* + 1. 【中危】SSL自签名证书
* 漏洞描述：

服务器所使用的X.509签署的证书链不是权威的证书颁发机构所颁发的。这削弱了使用SSL的效果，因为任何人都可以建立一个中间人攻击远程主机。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.91 | 5000 |

* 加固建议：

购买或者生成被认可的证书

* + 1. 【中危】SSH弱算法支持
* 漏洞描述：

目前该ssh服务采用的算法较低

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.91 | 22 |

* 加固建议：

修改ssh算法采用aes128-cbc或者aes256-cbc

* + 1. 【中危】TLS版本1.0协议检测
* 漏洞描述：

远程服务接受使用TLS 1.0加密的连接。TLS 1.0有许多密码设计缺陷。TLS 1.0的现代实现减轻了这些问题，但是像1.2和1.3这样的TLS的新版本是针对这些缺陷而设计的，应该尽可能使用。截至2020年3月31日，为TLS 1.2及更高版本启用的终结点将不再与主要web浏览器和主要供应商正常工作。PCI DSS v3.2要求在2018年6月30日之前完全禁用TLS 1.0，但POS POI终端（及其连接的SSL/TLS终端点）除外，这些终端可以被验证为不易受任何已知漏洞攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.91 | 5000 |

* 加固建议：

启用对TLS 1.2和1.3的支持，并禁用对TLS 1.0的支持。

* + 1. 【低危】SSH服务器CBC模式密码已启用
* 漏洞描述：

SSH服务器配置为支持密码块链接（CBC）加密。这可能允许攻击者从密文中恢复明文消息。注意，这个插件只检查SSH服务器的选项，不检查易受攻击的软件版本。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.91 | 22 |

* 加固建议：

联系供应商或查阅产品文档以禁用CBC模式密码加密，并启用CTR或GCM密码模式加密。

* + 1. 【低危】SSH弱MAC算法已启用
* 漏洞描述：

远程SSH服务器配置为允许MD5或96位MAC算法，这两种算法都被认为是较弱的。注意，这个插件只检查SSH服务器的选项，不检查易受攻击的软件版本。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.91 | 22 |

* 加固建议：

请与供应商联系或查阅产品文档以禁用MD5和96位MAC算法。

* 1. 【紧急】HIS系统（222.222.222.92）
     1. 【紧急】当前ORACLE数据库版本厂商已不支持
* 漏洞描述：

根据远程主机安装的数据库版本，厂家已不再支持，将会缺少安全补丁包，因此，可能存在安全威胁。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.92 | 1521 |

* 加固建议：

升级数据库版本至当前最新版本，至少升级至厂家支持的版本。

* + 1. 【高危】Oracle TNS侦听器远程毒化
* 漏洞描述：

Oracle Database Server是一个对象关系数据库管理系统。 Oracle Database Server在实现上存在可允许攻击者向远程“TNS Listener”组件处理的数据投毒的漏洞。攻击者可利用此漏洞将数据库服务器的合法“TNS Listener”组件中的数据转向到攻击者控制的系统，导致控制远程组件的数据库实例，造成组件和合法数据库之间的攻击者攻击、会话劫持或拒绝服务攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.92 | 1521 |

* 加固建议：

目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://www.oracle.com/technetwork/topics/security/alert-cve-2012-1675-1608180.html

* + 1. 【中危】SSL证书签名使用弱强度的哈希算法
* 漏洞描述：

远程服务器的SSL证书签名使用弱强度的哈希加密算法，例如MD2、MD4或者MD5。这些签名算法显示容易遭到破解。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.92 | 5000 |

* 加固建议：

联系证书认证机构发布新的证书。 如果服务器使用自签名证书，则可自己

* + 1. 【中危】允许SSL采用中强度加密
* 漏洞描述：

远程主机支持SSL使用的密码采用中强度解密，即使用的KEY解密长度至少64位，但少于112位。注意：如果攻击者在同一个物理网段，密码很容易暴露。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.92 | 5000 |

* 加固建议：

重新设置受影响的应用程序，可能的话，避免使用中强度加密，改为强度较高的加密算法。

* + 1. 【中危】SSL证书不被信任
* 漏洞描述：

此项服务的SSL证书不被信任。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.92 | 5000 |

* 加固建议：

为此项服务购买或生成合适的证书

* + 1. 【中危】SSL自签名证书
* 漏洞描述：

服务器所使用的X.509签署的证书链不是权威的证书颁发机构所颁发的。这削弱了使用SSL的效果，因为任何人都可以建立一个中间人攻击远程主机。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.92 | 5000 |

* 加固建议：

购买或者生成被认可的证书

* + 1. 【中危】SSH弱算法支持
* 漏洞描述：

目前该ssh服务采用的算法较低

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.92 | 22 |

* 加固建议：

修改ssh算法采用aes128-cbc或者aes256-cbc

* + 1. 【中危】TLS版本1.0协议检测
* 漏洞描述：

远程服务接受使用TLS 1.0加密的连接。TLS 1.0有许多密码设计缺陷。TLS 1.0的现代实现减轻了这些问题，但是像1.2和1.3这样的TLS的新版本是针对这些缺陷而设计的，应该尽可能使用。截至2020年3月31日，为TLS 1.2及更高版本启用的终结点将不再与主要web浏览器和主要供应商正常工作。PCI DSS v3.2要求在2018年6月30日之前完全禁用TLS 1.0，但POS POI终端（及其连接的SSL/TLS终端点）除外，这些终端可以被验证为不易受任何已知漏洞攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.92 | 5000 |

* 加固建议：

启用对TLS 1.2和1.3的支持，并禁用对TLS 1.0的支持。

* + 1. 【低危】SSH服务器CBC模式密码已启用
* 漏洞描述：

SSH服务器配置为支持密码块链接（CBC）加密。这可能允许攻击者从密文中恢复明文消息。注意，这个插件只检查SSH服务器的选项，不检查易受攻击的软件版本。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.92 | 22 |

* 加固建议：

联系供应商或查阅产品文档以禁用CBC模式密码加密，并启用CTR或GCM密码模式加密。

* + 1. 【低危】SSH弱MAC算法已启用
* 漏洞描述：

远程SSH服务器配置为允许MD5或96位MAC算法，这两种算法都被认为是较弱的。注意，这个插件只检查SSH服务器的选项，不检查易受攻击的软件版本。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.92 | 22 |

* 加固建议：

请与供应商联系或查阅产品文档以禁用MD5和96位MAC算法。

* 1. 【高危】微信缴费（10.10.14.23）
     1. 【高危】当前Web Server版本厂商已不再支持
* 漏洞描述：

根据现有版本，远程主机web服务已不在厂商支持范围内，缺少厂商的支持，意味着没有新的安全补丁包发布，结果主机存在多个安全威胁。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.23 | 80 |

* 加固建议：

如果不需要此项服务，关闭它。如果可能，升级新的版本，或更换其它的Web服务器。

* + 1. 【中危】HTTP TRACE / TRAC方法未禁用
* 漏洞描述：

主机支持TRACE和/或TRACK方法。 TRACE和TRACK是HTTP用来调试web服务器连接的方法。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.23 | 1000 |

* 加固建议：

禁用TRACE / TRAC方法，参考如下： 1、IIS下：IIS信息服务－web服务扩展：禁止"WebDAV； 2、apache下：修改httpd.conf配置文件中"TraceEnable on"为"TraceEnable off"

* + 1. 【中危】Sun ONE Application Server源泄露漏洞
* 漏洞描述：

Windows 2000/XP平台下的Sun ONE Application Server 7.0存在漏洞。远程攻击者可以借助一个用大写“.JSP”扩展名代替小写.jsp的请求获得JSP源代码。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.23 | 1000 |

* 加固建议：

补丁下载地址如下： http://wwws.sun.com/software/download/app\_servers.html

* 1. 【高危】国药SPD前置机（10.10.14.39）
     1. 【高危】当前Web Server版本厂商已不再支持
* 漏洞描述：

根据现有版本，远程主机web服务已不在厂商支持范围内，缺少厂商的支持，意味着没有新的安全补丁包发布，结果主机存在多个安全威胁。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.39 | 9090 |

* 加固建议：

如果不需要此项服务，关闭它。如果可能，升级新的版本，或更换其它的Web服务器。

* 1. 【中危】康软体检，LIS服务器（10.10.14.62）
     1. 【中危】微软Windows远程桌面协议服务器中间人攻击漏洞
* 漏洞描述：

Microsoft Windows远程桌面协议的实现在处理密钥的交换时存在漏洞，远程攻击者可能利用此漏洞窃取服务器的加密密钥。 起因是尽管通过网络传输的信息已经过加密，但在建立会话的加密密钥时没有核实服务器的身份，导致攻击者可以获得密钥，计算出有效的签名，然后发动中间人攻击。成功利用这个漏洞的攻击者可以完全控制连接在服务器上的客户端。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.62 | 3389 |

* 加固建议：

[1]如果支持的话，RDP使用SSL作为传输层 [2]“只允许使用网络级身份验证的电脑运行远程桌面建立连接”设置为启用

* + 1. 【中危】SSL证书不被信任
* 漏洞描述：

此项服务的SSL证书不被信任。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.62 | 3389 |

* 加固建议：

为此项服务购买或生成合适的证书

* + 1. 【中危】SSL自签名证书
* 漏洞描述：

服务器所使用的X.509签署的证书链不是权威的证书颁发机构所颁发的。这削弱了使用SSL的效果，因为任何人都可以建立一个中间人攻击远程主机。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.62 | 3389 |

* 加固建议：

购买或者生成被认可的证书

* + 1. 【中危】终端服务加密级别是中等或低
* 漏洞描述：

远程终端服务加密级别不够强，会降低攻击者窃听通信（包含获取截图和键盘记录）的难度。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.62 | 3389 |

* 加固建议：

组策略--计算机配置--管理模板--远程桌面服务--设置客户端连接加密级别： 修改RDP加密级别为“高”或者“FIPS兼容”

* + 1. 【中危】终端服务未使用网络级别身份验证(NLA)
* 漏洞描述：

远程终端服务未配置采用网络级别身份验证(NLA)。NLA使用凭据安全支持提供者(CredSSP)协议通过TLS/ SSL或Kerberos机制来执行强大的服务器身份验证，这能有效防止中间人攻击。除了优化认证,NLA也有助于防止恶意用户在一个完整的RDP连接建立之前，完成用户身份验证。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.62 | 3389 |

* 加固建议：

在“系统”设置的“远程”选项卡-- 启用网络级身份验证(NLA) 注意：如果客户端不支持“网络级身份验证”，将无法连接服务器远程管理服务。远程管理客户端版本需大于等于6.0

* + 1. 【中危】TLS版本1.0协议检测
* 漏洞描述：

远程服务接受使用TLS 1.0加密的连接。TLS 1.0有许多密码设计缺陷。TLS 1.0的现代实现减轻了这些问题，但是像1.2和1.3这样的TLS的新版本是针对这些缺陷而设计的，应该尽可能使用。截至2020年3月31日，为TLS 1.2及更高版本启用的终结点将不再与主要web浏览器和主要供应商正常工作。PCI DSS v3.2要求在2018年6月30日之前完全禁用TLS 1.0，但POS POI终端（及其连接的SSL/TLS终端点）除外，这些终端可以被验证为不易受任何已知漏洞攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.62 | 3389 |

* 加固建议：

启用对TLS 1.2和1.3的支持，并禁用对TLS 1.0的支持。

* + 1. 【低危】终端服务加密级别不符合FIPS-140
* 漏洞描述：

远程终端服务使用的加密设置不符合FIPS-140。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.62 | 3389 |

* 加固建议：

将RDP加密级别更改为：4.FIPS兼容

* 1. 【中危】康软体检，LIS服务器（10.10.14.65）
     1. 【中危】SSL证书不被信任
* 漏洞描述：

此项服务的SSL证书不被信任。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.65 | 3389 |

* 加固建议：

为此项服务购买或生成合适的证书

* + 1. 【中危】SSL自签名证书
* 漏洞描述：

服务器所使用的X.509签署的证书链不是权威的证书颁发机构所颁发的。这削弱了使用SSL的效果，因为任何人都可以建立一个中间人攻击远程主机。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.65 | 3389 |

* 加固建议：

购买或者生成被认可的证书

* + 1. 【中危】TLS版本1.0协议检测
* 漏洞描述：

远程服务接受使用TLS 1.0加密的连接。TLS 1.0有许多密码设计缺陷。TLS 1.0的现代实现减轻了这些问题，但是像1.2和1.3这样的TLS的新版本是针对这些缺陷而设计的，应该尽可能使用。截至2020年3月31日，为TLS 1.2及更高版本启用的终结点将不再与主要web浏览器和主要供应商正常工作。PCI DSS v3.2要求在2018年6月30日之前完全禁用TLS 1.0，但POS POI终端（及其连接的SSL/TLS终端点）除外，这些终端可以被验证为不易受任何已知漏洞攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.65 | 3389 |

* 加固建议：

启用对TLS 1.2和1.3的支持，并禁用对TLS 1.0的支持。

* 1. 【中危】电子病历363视图服务器（10.10.14.86）
     1. 【中危】允许SSL采用中强度加密
* 漏洞描述：

远程主机支持SSL使用的密码采用中强度解密，即使用的KEY解密长度至少64位，但少于112位。注意：如果攻击者在同一个物理网段，密码很容易暴露。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.86 | 6443 |

* 加固建议：

重新设置受影响的应用程序，可能的话，避免使用中强度加密，改为强度较高的加密算法。

* + 1. 【中危】SSL证书不被信任
* 漏洞描述：

此项服务的SSL证书不被信任。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.86 | 6443 |

* 加固建议：

为此项服务购买或生成合适的证书

* + 1. 【低危】SSH服务器CBC模式密码已启用
* 漏洞描述：

SSH服务器配置为支持密码块链接（CBC）加密。这可能允许攻击者从密文中恢复明文消息。注意，这个插件只检查SSH服务器的选项，不检查易受攻击的软件版本。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.86 | 22 |

* 加固建议：

联系供应商或查阅产品文档以禁用CBC模式密码加密，并启用CTR或GCM密码模式加密。

* 1. 【中危】电子病历365视图服务器（10.10.14.88）
     1. 【中危】MongoDB没有认证检测服务
* 漏洞描述：

MongoDB,面向文档的数据库系统,是侦听的远程端口，它被配置为允许没有任何的联系身份验证。远程攻击可以连接到数据库系统,以创建、读取、更新和删除 文档、集合和数据库。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.88 | 27017 |

* 加固建议：

启用身份验证或限制访问到MongoDB服务

* + 1. 【低危】SSH服务器CBC模式密码已启用
* 漏洞描述：

SSH服务器配置为支持密码块链接（CBC）加密。这可能允许攻击者从密文中恢复明文消息。注意，这个插件只检查SSH服务器的选项，不检查易受攻击的软件版本。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.88 | 22 |

* 加固建议：

联系供应商或查阅产品文档以禁用CBC模式密码加密，并启用CTR或GCM密码模式加密。

* 1. 【中危】电子病历应用服务器（10.10.14.94）
     1. 【中危】微软Windows远程桌面协议服务器中间人攻击漏洞
* 漏洞描述：

Microsoft Windows远程桌面协议的实现在处理密钥的交换时存在漏洞，远程攻击者可能利用此漏洞窃取服务器的加密密钥。 起因是尽管通过网络传输的信息已经过加密，但在建立会话的加密密钥时没有核实服务器的身份，导致攻击者可以获得密钥，计算出有效的签名，然后发动中间人攻击。成功利用这个漏洞的攻击者可以完全控制连接在服务器上的客户端。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.94 | 3389 |

* 加固建议：

[1]如果支持的话，RDP使用SSL作为传输层 [2]“只允许使用网络级身份验证的电脑运行远程桌面建立连接”设置为启用

* + 1. 【中危】终端服务加密级别是中等或低
* 漏洞描述：

远程终端服务加密级别不够强，会降低攻击者窃听通信（包含获取截图和键盘记录）的难度。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.94 | 3389 |

* 加固建议：

组策略--计算机配置--管理模板--远程桌面服务--设置客户端连接加密级别： 修改RDP加密级别为“高”或者“FIPS兼容”

* + 1. 【中危】终端服务未使用网络级别身份验证(NLA)
* 漏洞描述：

远程终端服务未配置采用网络级别身份验证(NLA)。NLA使用凭据安全支持提供者(CredSSP)协议通过TLS/ SSL或Kerberos机制来执行强大的服务器身份验证，这能有效防止中间人攻击。除了优化认证,NLA也有助于防止恶意用户在一个完整的RDP连接建立之前，完成用户身份验证。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.94 | 3389 |

* 加固建议：

在“系统”设置的“远程”选项卡-- 启用网络级身份验证(NLA) 注意：如果客户端不支持“网络级身份验证”，将无法连接服务器远程管理服务。远程管理客户端版本需大于等于6.0

* + 1. 【低危】终端服务加密级别不符合FIPS-140
* 漏洞描述：

远程终端服务使用的加密设置不符合FIPS-140。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.94 | 3389 |

* 加固建议：

将RDP加密级别更改为：4.FIPS兼容

* 1. 【中危】电子病历应用服务器（10.10.14.95）
     1. 【中危】微软Windows远程桌面协议服务器中间人攻击漏洞
* 漏洞描述：

Microsoft Windows远程桌面协议的实现在处理密钥的交换时存在漏洞，远程攻击者可能利用此漏洞窃取服务器的加密密钥。 起因是尽管通过网络传输的信息已经过加密，但在建立会话的加密密钥时没有核实服务器的身份，导致攻击者可以获得密钥，计算出有效的签名，然后发动中间人攻击。成功利用这个漏洞的攻击者可以完全控制连接在服务器上的客户端。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.95 | 3389 |

* 加固建议：

[1]如果支持的话，RDP使用SSL作为传输层 [2]“只允许使用网络级身份验证的电脑运行远程桌面建立连接”设置为启用

* + 1. 【中危】终端服务加密级别是中等或低
* 漏洞描述：

远程终端服务加密级别不够强，会降低攻击者窃听通信（包含获取截图和键盘记录）的难度。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.95 | 3389 |

* 加固建议：

组策略--计算机配置--管理模板--远程桌面服务--设置客户端连接加密级别： 修改RDP加密级别为“高”或者“FIPS兼容”

* + 1. 【中危】终端服务未使用网络级别身份验证(NLA)
* 漏洞描述：

远程终端服务未配置采用网络级别身份验证(NLA)。NLA使用凭据安全支持提供者(CredSSP)协议通过TLS/ SSL或Kerberos机制来执行强大的服务器身份验证，这能有效防止中间人攻击。除了优化认证,NLA也有助于防止恶意用户在一个完整的RDP连接建立之前，完成用户身份验证。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.95 | 3389 |

* 加固建议：

在“系统”设置的“远程”选项卡-- 启用网络级身份验证(NLA) 注意：如果客户端不支持“网络级身份验证”，将无法连接服务器远程管理服务。远程管理客户端版本需大于等于6.0

* + 1. 【低危】终端服务加密级别不符合FIPS-140
* 漏洞描述：

远程终端服务使用的加密设置不符合FIPS-140。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.95 | 3389 |

* 加固建议：

将RDP加密级别更改为：4.FIPS兼容

* 1. 【中危】PACS系统（222.222.100.6）
     1. 【中危】SSL证书签名使用弱强度的哈希算法
* 漏洞描述：

远程服务器的SSL证书签名使用弱强度的哈希加密算法，例如MD2、MD4或者MD5。这些签名算法显示容易遭到破解。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.100.6 | 3389 |

* 加固建议：

联系证书认证机构发布新的证书。 如果服务器使用自签名证书，则可自己

* + 1. 【中危】SSL证书不被信任
* 漏洞描述：

此项服务的SSL证书不被信任。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.100.6 | 3389 |

* 加固建议：

为此项服务购买或生成合适的证书

* + 1. 【中危】SSL自签名证书
* 漏洞描述：

服务器所使用的X.509签署的证书链不是权威的证书颁发机构所颁发的。这削弱了使用SSL的效果，因为任何人都可以建立一个中间人攻击远程主机。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.100.6 | 3389 |

* 加固建议：

购买或者生成被认可的证书

* + 1. 【中危】TLS版本1.0协议检测
* 漏洞描述：

远程服务接受使用TLS 1.0加密的连接。TLS 1.0有许多密码设计缺陷。TLS 1.0的现代实现减轻了这些问题，但是像1.2和1.3这样的TLS的新版本是针对这些缺陷而设计的，应该尽可能使用。截至2020年3月31日，为TLS 1.2及更高版本启用的终结点将不再与主要web浏览器和主要供应商正常工作。PCI DSS v3.2要求在2018年6月30日之前完全禁用TLS 1.0，但POS POI终端（及其连接的SSL/TLS终端点）除外，这些终端可以被验证为不易受任何已知漏洞攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.100.6 | 3389 |

* 加固建议：

启用对TLS 1.2和1.3的支持，并禁用对TLS 1.0的支持。

* + 1. 【中危】JQuery 1.2<3.5.0多个XSS
* 漏洞描述：

根据脚本中自我报告的版本，远程web服务器上托管的JQuery版本大于或等于1.2且早于3.5.0。因此，它受到多个跨站点脚本漏洞的影响。注意，此插件中引用的漏洞对PAN-OS没有安全影响，并且/或者运行PAN-OS版本的设备上不存在成功利用漏洞所需的场景。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.100.6 | 81 |

* 加固建议：

升级到JQuery 3.5.0或更高版本。

* 1. 【中危】OA系统（222.222.222.50）
     1. 【中危】SSL证书不被信任
* 漏洞描述：

此项服务的SSL证书不被信任。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.50 | 3389 |

* 加固建议：

为此项服务购买或生成合适的证书

* + 1. 【中危】SSL自签名证书
* 漏洞描述：

服务器所使用的X.509签署的证书链不是权威的证书颁发机构所颁发的。这削弱了使用SSL的效果，因为任何人都可以建立一个中间人攻击远程主机。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.50 | 3389 |

* 加固建议：

购买或者生成被认可的证书

* + 1. 【中危】SMB数字签名通信禁用
* 漏洞描述：

SMB 协议为 Microsoft 文件和打印共享以及许多其他网络操作（例如远程 Windows 管理）提供基础。为了防止在传输过程中修改 SMB 数据包的拦截攻击，SMB 协议支持对 SMB 数据包的数字签名。 主机禁用了SMB数字签名通信，这可能导致潜在攻击者针对SMB通信服务进行中间人攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.50 | 445 |

* 加固建议：

在本地策略中--安全选项设置如下： Microsoft 网络客户端：对通信进行数字签名（若服务器同意）（启用） Microsoft 网络服务器：对通信进行数字签名（若客户同意）（启用）

* + 1. 【中危】TLS版本1.0协议检测
* 漏洞描述：

远程服务接受使用TLS 1.0加密的连接。TLS 1.0有许多密码设计缺陷。TLS 1.0的现代实现减轻了这些问题，但是像1.2和1.3这样的TLS的新版本是针对这些缺陷而设计的，应该尽可能使用。截至2020年3月31日，为TLS 1.2及更高版本启用的终结点将不再与主要web浏览器和主要供应商正常工作。PCI DSS v3.2要求在2018年6月30日之前完全禁用TLS 1.0，但POS POI终端（及其连接的SSL/TLS终端点）除外，这些终端可以被验证为不易受任何已知漏洞攻击。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 222.222.222.50 | 3389 |

* 加固建议：

启用对TLS 1.2和1.3的支持，并禁用对TLS 1.0的支持。

* 1. 【低危】电子病历360视图服务器（10.10.14.83）
     1. 【低危】SSH服务器CBC模式密码已启用
* 漏洞描述：

SSH服务器配置为支持密码块链接（CBC）加密。这可能允许攻击者从密文中恢复明文消息。注意，这个插件只检查SSH服务器的选项，不检查易受攻击的软件版本。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.83 | 22 |

* 加固建议：

联系供应商或查阅产品文档以禁用CBC模式密码加密，并启用CTR或GCM密码模式加密。

* 1. 【低危】电子病历361视图服务器（10.10.14.84）
     1. 【低危】SSH服务器CBC模式密码已启用
* 漏洞描述：

SSH服务器配置为支持密码块链接（CBC）加密。这可能允许攻击者从密文中恢复明文消息。注意，这个插件只检查SSH服务器的选项，不检查易受攻击的软件版本。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.84 | 22 |

* 加固建议：

联系供应商或查阅产品文档以禁用CBC模式密码加密，并启用CTR或GCM密码模式加密。

* 1. 【低危】电子病历362视图服务器（10.10.14.85）
     1. 【低危】SSH服务器CBC模式密码已启用
* 漏洞描述：

SSH服务器配置为支持密码块链接（CBC）加密。这可能允许攻击者从密文中恢复明文消息。注意，这个插件只检查SSH服务器的选项，不检查易受攻击的软件版本。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 10.10.14.85 | 22 |

* 加固建议：

联系供应商或查阅产品文档以禁用CBC模式密码加密，并启用CTR或GCM密码模式加密。