

|  |  |
| --- | --- |
| 文档编号 | Hypdncy-XXKH-1217 |
| 日期 | 2021-12-17 |

|  |
| --- |
| XX客户  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 | Hypdncy |

目录

[一. 懂 3](#_Toc90633601)

[二. 的 3](#_Toc90633602)

[三. 都 3](#_Toc90633603)

[四. 懂 3](#_Toc90633604)

[4.1 【紧急】192.168.1.1 3](#_Toc90633605)

[4.1.1 【紧急】MS14-066：Schannel 远程代码执行漏洞 3](#_Toc90633606)

[4.1.2 【高危】Windows SMB 远程代码执行漏洞 4](#_Toc90633607)

[4.1.3 【高危】Microsoft Windows SMBv1多个漏洞 4](#_Toc90633608)

[4.1.4 【中危】微软Windows远程桌面协议服务器中间人攻击漏洞 5](#_Toc90633609)

[4.1.5 【中危】SSL证书签名使用弱强度的哈希算法 5](#_Toc90633610)

[4.1.6 【中危】允许SSL采用中强度加密 5](#_Toc90633611)

[4.1.7 【中危】SSL证书不被信任 6](#_Toc90633612)

[4.1.8 【中危】SSL自签名证书 6](#_Toc90633613)

[4.1.9 【中危】SMB数字签名通信禁用 6](#_Toc90633614)

[4.1.10 【中危】终端服务加密级别是中等或低 7](#_Toc90633615)

[4.1.11 【中危】终端服务未使用网络级别身份验证(NLA) 7](#_Toc90633616)

[4.1.12 【中危】远程主机支持SSL RC4加密套件 8](#_Toc90633617)

[4.1.13 【中危】Windows SAM 和 LSAD 降级漏洞 8](#_Toc90633618)

[4.1.14 【低危】终端服务加密级别不符合FIPS-140 8](#_Toc90633619)

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 | 192.168.1.1 | - |

1. 都
2. 懂

经过此次检测，共发现安全漏洞种类14个，其中紧急漏洞1个、高危漏洞2个、中危漏洞10个、低危漏洞1个。存在的安全隐患主要包括MS14-066：Schannel 远程代码执行漏洞、Windows SMB 远程代码执行漏洞、Microsoft Windows SMBv1多个漏洞等安全漏洞，可能将导致等严重危害。

* 1. 【紧急】192.168.1.1
     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 |
| 192.168.1.1 | 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. 【高危】Windows SMB 远程代码执行漏洞
* 漏洞描述：

当 Microsoft 服务器消息块 1.0 (SMBv1) 服务器处理某些请求时，存在多个远程执行代码漏洞。成功利用这些漏洞的攻击者可以获取在目标系统上执行代码的能力。 为了利用此漏洞，在多数情况下，未经身份验证的攻击者可能向目标 SMBv1 服务器发送经特殊设计的数据包

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.1.1 | 445 |

* 加固建议：

微软已发布官方补丁，具体参考： https://technet.microsoft.com/zh-cn/library/security/MS17-010

* + 1. 【高危】Microsoft Windows SMBv1多个漏洞
* 漏洞描述：

Microsoft Windows SMB中存在安全更新。如果攻击者将特制数 据包发送到Microsoft Server Message Block 1.0（SMBv1）服务 器，则最严重的漏洞可能允许远程执行代码。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.1.1 | 445 |

* 加固建议：

厂商已发布升级程序修复该漏洞，请及时下载更新： https://support.microsoft.com/zh-cn/help/4025687/microsoft-security-advisory-4025685-guidance-for-older-platforms

* + 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 |
| 192.168.1.1 | 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 |
| 192.168.1.1 | 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 |
| 192.168.1.1 | 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 |
| 192.168.1.1 | 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 |
| 192.168.1.1 | 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 |
| 192.168.1.1 | 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】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 |
| 192.168.1.1 | 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 |
| 192.168.1.1 | 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】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 |
| 192.168.1.1 | 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 |
| 192.168.1.1 | 49155 |

* 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. 【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 |
| 192.168.1.1 | 3389 |

* 加固建议：

将RDP加密级别更改为：4.FIPS兼容