

|  |  |
| --- | --- |
| 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](#_Toc90633607)

[二. 的 3](#_Toc90633608)

[三. 都 3](#_Toc90633609)

[四. 懂 3](#_Toc90633610)

[4.1 【紧急】192.168.1.2 3](#_Toc90633611)

[4.1.1 【紧急】Microsoft Remote Desktop Services 输入验证错误漏洞 3](#_Toc90633612)

[4.1.2 【高危】Microsoft Windows SMBv1多个漏洞 4](#_Toc90633613)

[4.1.3 【中危】TLS版本1.0协议检测 5](#_Toc90633614)

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 | 192.168.1.2 | - |

1. 都
2. 懂

经过此次检测，共发现安全漏洞种类3个，其中紧急漏洞1个、高危漏洞1个、中危漏洞1个、低危漏洞0个。存在的安全隐患主要包括Microsoft Remote Desktop Services 输入验证错误漏洞、Microsoft Windows SMBv1多个漏洞、TLS版本1.0协议检测等安全漏洞，可能将导致等严重危害。

* 1. 【紧急】192.168.1.2
     1. 【紧急】Microsoft Remote Desktop Services 输入验证错误漏洞
* 漏洞描述：

Windows系列服务器于2019年5月15号，被爆出高危漏洞，该漏洞影响范围较广，windows2003、windows2008、windows2008 R2、windows xp \* 系统都会遭到攻击，该服务器漏洞利用方式是通过远程桌面端口3389，RDP协议进行攻击的 。CVE-2019-0708漏洞是通过检查用户的身份认证，导致可以绕过认证，不用任何的交互，直接通过rdp协议进行连接发送恶意代码执行命令到服务器中去。这个漏洞是今年来说危害严重性最大的漏洞，换句话说，该漏洞是“可传播的”，这意味着任何利用该漏洞的恶意软件都可能从受影响的计算机传播到受影响的计算机，就像2017年WannaCry恶意软件在全球蔓延一样，跟之前的勒索，永恒之蓝病毒差不多。 \*备注：微软不在对 windows-Xp 和windows 2003 提供安全更新（对windows10和8无影响）

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.1.2 | 3389 |

* 加固建议：

目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0708

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

远程Windows主机已启用Microsoft Server Message Block 1.0（SMBv1）。因此，它受到多个漏洞的影响：-由于不正确处理SMBv1数据包，Microsoft Server Message Block 1.0（SMBv1）中存在多个信息泄漏漏洞。未经验证的远程攻击者可以通过巧尽心思构建的SMBv1数据包利用这些漏洞来泄露敏感信息(CVE-2017-0267、CVE-2017-0268、CVE-2017-0270、CVE-2017-0271、CVE-2017-0274、CVE-2017-0275、CVE-2017-0276）-由于请求处理不当，Microsoft Server Message Block 1.0（SMBv1）中存在多个拒绝服务漏洞。未经验证的远程攻击者可以通过巧尽心思构建的SMB请求利用这些漏洞，使系统停止响应(CVE-2017-0269、CVE-2017-0273、CVE-2017-0280）-由于不正确处理SMBv1数据包，Microsoft Server Message Block 1.0（SMBv1）中存在多个远程代码执行漏洞。未经验证的远程攻击者可以通过巧尽心思构建的SMBv1数据包利用这些漏洞执行任意代码(CVE-2017-0272、CVE-2017-0277、CVE-2017-0278、CVE-2017-0279）根据主机的安全策略配置，如果主机运行的是更高版本的Windows（即Windows 8.1、10、2012、2012 R2，特别是允许远程匿名访问命名管道和共享。Tenable不建议使用此配置，应在本地检查主机是否有以下插件之一的修补程序，具体取决于Windows版本：100054、100055、100057、100059、100060或100061。

* 受影响主机：

|  |  |
| --- | --- |
| 主机 | 端口 |
| 192.168.1.2 | 445 |

* 加固建议：

为您的Windows版本应用适用的安全更新：-Windows Server 2008:KB4018466-Windows 7:KB4019264-Windows Server 2008 R2:KB4019264-Windows Server 2012:KB4019216-Windows 8.1/RT 8.1.：KB4019264KB4019215-Windows Server 2012 R2:KB4019215-Windows 10:KB4019474-Windows 10版本1511:KB4019473-Windows 10版本1607:KB4019472-Windows 10版本1703:KB4016871-Windows Server 2016:KB4019472

* + 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 |
| 192.168.1.2 | 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。