

|  |  |
| --- | --- |
| 文档编号 | AH-AHXX-0418 |
| 版本编号 | V1.0 |
| 密级 | 受控 |
| 日期 | 2021-04-18 |

|  |
| --- |
| 安恒信息  主机扫描报告 |

|  |
| --- |
| **©2021安恒信息** |
| **版权所有，未经授权，严禁复制、编辑和传播** |

* 适用性声明

本文档仅适用于杭州安恒信息技术股份有限公司（以下简称“安恒信息”）在安恒信息（以下简称“安恒信息”）开展主机扫描时的状况。主机扫描结束之后，因内部环境或不可预知的国内国际政治、经济、法律等社会环境的变化，可能会影响文档的有效性。再者，任何控制系统都存在固有的局限性，错误、违反内部控制的情况仍然有可能发生及不被发现。

* 版权声明

本文中的所有信息均为安恒信息（以下简称“安恒信息”）内部信息，务请妥善保管，未经安恒信息和安恒信息明确作出的书面许可，不得为任何目的、以任何形式或手段（包括电子、机械、复印、录音或其他形式）对本文档的任何部分进行复制、存储、引入检索系统或者传播。

* 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** |
| V0.1 | 2020-04-27 | 张韵 | 创建文档，添加样式库 | 韦国文 |
| V0.2 | 2020-07-30 | 甘雁南、苏启波 | 添加样式库、修改图注 | 韦国文 |
| V0.3 | 2020-09-08 | 甘雁南 | 修改格式和字体 | 韦国文 |
| V0.4 | 2020-10-23 | 王琦 | 修改格式 | 韦国文 |
| V1.0 | 2021-01-25 | 甄杰 | 修改格式和样式库 | 韦国文 |

目录

[一. 概述 3](#_Toc69608613)

[1.1 项目目标 3](#_Toc69608614)

[1.2 测试依据 3](#_Toc69608615)

[1.3 项目收益 3](#_Toc69608616)

[二. 实施范围 4](#_Toc69608617)

[三. 风险规避与处理措施 4](#_Toc69608618)

[3.1 风险规避措施 4](#_Toc69608619)

[3.1.1 系统备份与恢复 4](#_Toc69608620)

[3.1.2 风险与应对 5](#_Toc69608621)

[3.2 风险处理措施 5](#_Toc69608622)

[四. 检测结果与建议 5](#_Toc69608623)

[4.1 【紧急】网站1（192.168.1.1） 6](#_Toc69608624)

[4.1.1 【紧急】MS14-066：Schannel 远程代码执行漏洞 6](#_Toc69608625)

[4.1.2 【紧急】Windows SMB 远程代码执行漏洞 6](#_Toc69608626)

[4.1.3 【紧急】Microsoft Windows SMBv1多个漏洞 6](#_Toc69608627)

[4.1.4 【中危】微软Windows远程桌面协议服务器中间人攻击漏洞 7](#_Toc69608628)

[4.1.5 【中危】SSL证书签名使用弱强度的哈希算法 7](#_Toc69608629)

[4.1.6 【中危】允许SSL采用中强度加密 8](#_Toc69608630)

[4.1.7 【中危】SSL证书不被信任 8](#_Toc69608631)

[4.1.8 【中危】SSL自签名证书 8](#_Toc69608632)

[4.1.9 【中危】SMB数字签名通信禁用 9](#_Toc69608633)

[4.1.10 【中危】终端服务加密级别是中等或低 9](#_Toc69608634)

[4.1.11 【中危】终端服务未使用网络级别身份验证(NLA) 9](#_Toc69608635)

[4.1.12 【中危】远程主机支持SSL RC4加密套件 10](#_Toc69608636)

[4.1.13 【中危】Windows SAM 和 LSAD 降级漏洞 10](#_Toc69608637)

[4.1.14 【低危】终端服务加密级别不符合FIPS-140 11](#_Toc69608638)

[4.2 【紧急】网站2（192.168.1.2） 11](#_Toc69608639)

[4.2.1 【紧急】低版本的Windows系统 11](#_Toc69608640)

[4.2.2 【紧急】Microsoft Remote Desktop Services 输入验证错误漏洞 11](#_Toc69608641)

[4.2.3 【高危】Microsoft Windows SMBv1多个漏洞 12](#_Toc69608642)

[4.2.4 【中危】TLS版本1.0协议检测 13](#_Toc69608643)

1. 概述
   1. 项目目标

根据安恒信息的安全性需求，授权杭州安恒信息技术股份有限公司（以下简称“安恒信息”）对其进行主机扫描测试；并根据本次扫描过程中所发现的系统脆弱点提供改进方案，以指导安恒信息开展安全整改、完善安全策略，降低安全风险，使安恒信息的安全保障能力符合国家的相关政策法规和自身业务的安全需求。

* 1. 测试依据

项目所依据及参考的标准：

《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）

《信息安全技术 信息安全风险评估规范》（GB/T 20984-2007）

《信息技术 安全技术 信息技术安全性评估准则》（GB/T 18336-2015）

《信息系统安全保障评估框架》（GB/T 20274-2006）

《OWASP测试指南V4.0》（2014）

《开源安全测试方法手册（OSSTMM）3》（2010）

《PTES渗透测试执行标准》（2011）

* 1. 项目收益

从攻击者的角度进行测试将有助于发现并识别出一些隐性存在的安全漏洞和风险点。

从客户收益的角度来说，可以对信息系统的安全性得到较深的感性认知，有助于后续的安全建设，对设备的版本、典型的可利用漏洞可以进行全面的排查，同时也可以用于验证经过安全保护后的网络是否真实的达到了预定安全目标、遵循了安全策略。

1. 实施范围

经过与安恒信息协商确定，将主机扫描的时间安排为2021-04-18，主机扫描限定于以下对象：

|  |  |  |
| --- | --- | --- |
| 序号 | IP地址 | 对象名称 |
| 1 | 192.168.1.1 | 网站1 |
| 2 | 192.168.1.2 | 网站2 |
| 3 | 192.168.1.3 | 网站3 |
| 4 | 192.168.1.4 | 网站4 |
| 5 | 192.168.1.5 | 网站5 |
| 6 | 192.168.1.6 | 网站6 |
| 7 | 192.168.1.7 | 网站7 |
| 8 | 192.168.1.8 | 网站8 |
| 9 | 192.168.1.9 | 网站9 |

1. 风险规避与处理措施
   1. 风险规避措施
      1. 系统备份与恢复

为防止在加固过程中出现的异常情况，所有被加固系统均应在被加固之前进行完整的系统备份,以便在系统发生灾难后及时恢复。

操作系统类：对系统的配置、用户目录和重要文件进行备份。例如：注册表、sam文件、/etc中的配置文件。并应该确保备份的自身安全。

数据库系统类：对数据库系统进行数据转储，并妥善保护好备份数据。同时对数据库系统的配置信息和用户信息进行备份。

网络应用系统类：对网络应用服务系统及其配置、用户信息、数据库等进行备份。

网络设备类：对网络设备的配置文件进行备份。

* + 1. 风险与应对

加固时间尽量安排在业务量不大的时段。在加固过程中如果出现被加固系统没有响应的情况，应立即停止加固工作，与配合人员一起分析情况，在确定原因后，并正确恢复系统，采取必要的预防措施后，才可以继续进行。

* 1. 风险处理措施

对信息系统安全加固过程中发现的风险，其处理方式一般有以下处理方式：

* 避免：指通过不继续进行可能产生风险的活动来避免风险。这种方式是最佳的解决方式，但实施的前提是要具有可行性，需要结合具体的实际情况在分析后决定。
* 转移：是指将相关的风险借助合同、保险以及合伙，合资等方式全部或部分转移给第三方，但这种转移一般只能降低部分经济损失或转移部分责任，不能降低安全本身的风险。
* 降低：通过采取相应的风险控制措施、安全机制来切实降低风险，减少发生的机率可能性，这也是采用最多的一种方式之一。
* 接受：在风险降低或转移后，可能还有剩余的风险，完全的零风险最理论和实践中都是不可能的，而且降低风险的成本会随着风险的降低而增大，通常考虑的尺度是让风险的处理成本与该项处理活动保持一种可接受的平衡。

1. 检测结果与建议

经过此次检测，共发现安全漏洞主机2个，其中紧急主机2个、高危主机0个、中危主机0个、低危主机0个。存在的安全隐患主要包括MS14-066：Schannel 远程代码执行漏洞、低版本的Windows系统、Microsoft Remote Desktop Services 输入验证错误漏洞等安全漏洞，可能将导致等严重危害。

* 1. 【紧急】网站1（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. 【紧急】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. 【紧急】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。符合FIPS

* 1. 【紧急】网站2（192.168.1.2）
     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 |
| 192.168.1.2 | 0 |

* 加固建议：

升级操作系统

* + 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。KB4019215-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。