TC260-PG-2022XX

网络安全标准实践指南

—Windows 7 操作系统安全加固指引

（征求意见稿 V1.0-202204）

全国信息安全标准化技术委员会秘书处

2022 年 4 月

本文档可从以下网址获得：
www.tc260.org.cn

全国信息安全标准化技术委员会
NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

前　言

《网络安全标准实践指南》（以下简称《实践指南》）是全国信息安全标准化技术委员会（以下简称“信安标委”）秘书处组织制定和发布的标准相关技术文件，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。

声　明

本《实践指南》版权属于信安标委秘书处，未经秘书处书面授权，不得以任何方式抄袭、翻译《实践指南》的任何部分。凡转载或引用本《实践指南》的观点、数据，请注明“来源：全国信息安全标准化技术委员会秘书处”。

技术支持单位

本《实践指南》得到安天科技集团股份有限公司、杭州安恒信息技术股份有限公司、中国电子技术标准化研究院、深信服科技股份有限公司、杭州迪普科技股份有限公司、三六零数字安全科技集团有限公司、天融信网络安全技术有限公司、北京山石网科信息技术有限公司等单位的技术支持。

引 言

2020年1月，微软停止了对Windows 7操作系统的补丁升级（以下简称“WIN7停服”），除付费用户或针对一些影响极大的高危漏洞，微软将不会为停服系统提供补丁更新服务，继续使用Windows 7操作系统的用户将更容易受到恶意软件和黑客的攻击，面临较大的安全风险。

为获得更高的安全保障，首选建议相关用户尽快更新迭代到更加安全的操作系统；对于受业务所限确实无法更新迭代的操作系统，建议相关用户在保障业务连续性和系统安全性之间做出适合自身业务目标的选择，但业务目标缺乏网络安全保障是很难持续并达成的。

本实践指南主要考虑当前一些无法进行更新迭代、不得不继续使用Windows 7操作系统的场景，从WIN7停服带来的安全风险分析出发，以操作系统加固体系为基础，参考国内外的相关技术指导文件，并重点结合多家网络安全厂商和用户在实际运维中的最佳实践，从安全防护加固和安全配置加固两方面提出了对Windows 7操作系统安全加固的实践建议。

此外，建议用户持续关注新出现的系统漏洞，依靠相关主管单位、研究机构、网络安全厂商等，对新出现的漏洞加强跟踪分析和研究，并有针对性的采取相关漏洞的补救措施。

特别需要注意的是，即使全面采用了本实践指南推荐的这些加固措施，Windows 7 操作系统底层固有的一些漏洞和

风险依然存在，并不能保障该系统环境以及其上运行的应用程序免受最新威胁的攻击。用户应尽快升级到适用的、正在服务的操作系统产品。

目　录

1 范围

本实践指南针对Windows 7操作系统停服后仍必须使用的应用场景，从安全防护加固和安全配置加固两个方面，给出了Windows 7操作系统本地防护和安全策略以及网络安全策略配置建议。

本实践指南适用于Windows 7操作系统以及兼容操作系统平台的安全加固，Windows 7以上的操作系统安全加固也可参考使用。

2 术语定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

2.1 身份 identity

与某一实体相关的一组属性。

注1：一个实体能有多个身份。

注2：几个实体能有同一的身份。

2.2 鉴别 authentication

验证某一实体所声称身份的过程。

2.3 访问控制 access control

一种确保数据处理系统的资源只能由经授权实体以授权方式进行访问的手段。

2.4 安全审计 security audit

对信息系统记录与活动的独立评审和考察，以测试系统控制的充分程度，确保对于既定安全策略和运行规程的符合性，发现安全违规，并在控制、安全策略和过程三方面提出改进建议。

2.5 入侵 intrusion

对网络或联网系统的未授权访问，即对信息系统进行有意或无意的未授权访问，包括针对信息系统的恶意活动或对信息系统内资源的未授权使用。

2.6 入侵防御 intrusion prevention

积极应对以防止入侵的正规过程。

2.7 加固优先级 reinforcement priority

加固项优先级，分重要和一般两个级别。

3 缩略语

下列缩略语适用于本文件。

DEP：数据执行保护（Data Execution Protection）

DPAPI：数据保护API（Data Protection API）

DS：目录服务（Directory Service）

FTP：文件传输协议（File Transfer Protocol）

MPSSVC：防火墙服务（Windows Defender Firewall service）

RDS：远程桌面服务（Remote Desktop Services）

RPC：远程过程调用（Remote procedure call）

SAM：安全账户管理（Security Account Manager）

SYN：同步序列编号（Synchronize Sequence Numbers）

TCP：传输控制协议（Transmit Control Protocol）

UAC：用户账户控制（User Account Control）

4 概述

本实践指南从安全防护加固和安全配置加固两个方面给出了加固建议。每个加固项使用了“要求、加固建议、加固优先级、实施/操作指南”四项要素，具体说明了加固方法，便于指导操作。附录中列出了建议安装的系统补丁、常见高危漏洞、建议关闭的服务以及建议关闭的端口列表，用户可根据实际使用场景参考使用。

5 安全防护加固

安全防护加固从三个方面考虑。首先，微软官方已经发布的针对Windows 7系统漏洞的补丁（见附录A和附录B）的安装，防止恶意攻击利用已知漏洞的攻击；其次，针对一些新出现的漏洞且没有官方补丁的情况，可以采用第三方网络安全厂商提供的热补丁、系统加固方案等作为缓解措施，但第三方补丁的有效性以及与用户业务系统的兼容性等需要用户根据自身的实际情况进行验证、修补；最后，可以利用系统本身的安全配置以及安装第三方网络安全厂商提供的恶意代码防范软件，以达到安全加固的目的。

5.1 系统补丁

及时安装系统补丁，可以很大程度避免被恶意入侵和利用，让系统和软件运行更稳定。建议安装的系统补丁见附录A。

5.1.1 已知高危害漏洞修复

要求

已知高危害系统漏洞进行补丁修复。

加固建议

针对已知高危害漏洞，充分评估后进行修复。

加固优先级

重要

实施/操作指南

针对已知高危害漏洞查找并安装对应补丁或使用安全软件进行漏洞修复。常见的高危害漏洞详见附录B。

5.1.2 Windows Update 系统升级进程

要求

禁止Windows Update系统升级进程访问互联网，防止可能通过本升级进程收集信息，增加安全风险。

加固建议

禁止Windows Update系统升级进程访问互联网。

加固优先级

一般

实施/操作指南

利用操作系统自身的功能设置或采用第三方联网检查工具实现阻止外联Windows 7升级服务器。

5.2 第三方安全防护

采用网络安全厂商等第三方安全防护软件，可针对没有微软补丁的操作系统漏洞进行主动防御，对攻击行为进行拦截，包括但不限于以下技术方式。

5.2.1 停服后的漏洞修复

要求

修复Windows 7停服后高危操作系统漏洞。

加固建议

针对Windows 7停服后无法提供实体补丁的高危操作系统漏洞，采用第三方安全厂商提供的相应补丁解决方案进行漏洞修复。

加固优先级

重要

实施/操作指南

部署具备相关补丁漏洞免疫功能的终端安全防护软件，并开启针对Windows 7操作系统适配的系统补丁，下发至Windows 7操作系统终端并开启防护。

5.2.2 热补丁

要求

使用第三方安全厂商提供的热补丁技术，通过内存检测、内核加固、网络流量检测等方式进行漏洞修复或攻击拦截。

加固建议

安装并开启第三方安全厂商提供的热补丁功能，进行动态检测防护加固。

加固优先级

重要

实施/操作指南

部署具备热补丁功能的终端安全防护软件，并开启针对Windows 7操作系统的热补丁能力。

5.2.3 系统加固

要求

使用包括但不限于主动防御、内存修补等技术措施，以清除由于系统漏洞带来的安全隐患。

加固建议

安装并开启第三方安全厂商提供的系统加固功能。

加固优先级

重要

实施/操作指南

部署具备系统加固能力的终端安全防护软件，并开启系统加固功能。

5.3 恶意代码防范

本节主要针对恶意代码可能的入侵点提供安全加固建议。

5.3.1 UAC 验证

要求

启用用户账户控制（UAC）功能。

加固建议

启用用户账户控制（UAC）功能。

加固优先级

重要

实施/操作指南

在运行窗口输入“gpedit.msc”打开本地组策略。配置计算机配置 -> Windows设置 ->安全设置 ->本地策略的策略值 ->安全选项 ->“用户账户控制：以管理员批准模式运行所有管理员”为“已启用”。

5.3.2 自动播放

要求

关闭自动播放功能。

加固建议

关闭自动播放功能。

加固优先级

重要

实施/操作指南

在运行窗口输入“gpedit.msc”打开本地组策略。将计算机配置 -> 管理模板 -> Windows组件 ->自动播放策略 ->“自动运行的默认行为”的策略值配置为“已启用：不执行任何自动运行命令”。

5.3.3 数据执行保护

要求

启用数据执行保护（DEP）。

加固建议

打开数据执行保护（DEP）功能。

加固优先级

重要

实施/操作指南

进入“控制面板->系统”；选择“高级系统设置->高级->性能->设置->数据执行保护”选项卡，勾选“仅为基本 Windows 操作系统程序和服务启用DEP”。

5.3.4 恶意代码防范软件

要求

安装恶意代码防范软件并及时更新特征库。

加固建议

开启实时防护功能并定期扫描，及时升级软件、更新特征库。

加固优先级

重要

实施/操作指南

选用符合国家标准的恶意代码防范软件。

6 安全配置加固

安全配置加固主要依靠Windows 7操作系统本身提供的各种配置进行加固，包括但不限于身份鉴别、访问控制、安全审计、入侵防范等。部分配置项在默认情况下未启用，启用这些配置项可以预防某些特定的网络威胁攻击，增强Windows 7系统安全。

本实践指南所列的配置加固项未穷尽，用户可以根据自身业务需求以及网络威胁的发展变化态势，进行动态调整，以增强系统的安全性。

用户在参考本章中的安全配置加固项进行加固工作时，除了手动加固，还可采用满足本实践指南要求的自动化工具开展安全策略检查并实施加固操作。

6.1 身份鉴别

身份鉴别主要是对登录用户数字身份进行合法性校验，保证以数字身份进行操作的操作者就是这个数字身份合法拥有者，通过对身份鉴别相关安全策略的加固，可以提高账号安全性。本节主要针对口令复杂度、使用期限、登录失败处理、屏幕保护等与身份鉴别等有关策略提供安全加固建议。

6.1.1 口令复杂度

要求

口令策略启用口令符合复杂性要求。

加固建议

满足口令复杂度要求：至少包含大小写字母、数字和特殊符号3种或者3种以上组合。

加固优先级

重要

实施/操作指南

运行窗口输入“gpedit.msc”打开本地组策略。配置计算机配置 -> Windows设置 ->安全设置 -> 账户策略 ->密码策略”：“密码必须符合复杂性要求”选择“已启动”。

6.1.2 口令长度

要求

口令要有最小长度限制。

加固建议

配置口令策略限制口令的长度必须至少为8个字符。

加固优先级

重要

实施/操作指南

在运行窗口输入“gpedit.msc”打开本地组策略。配置计算机配置 -> Windows设置 ->安全设置 ->账户策略->密码策略->密码长度最小值大于等于8个字符。

6.1.3 口令最长使用期限

要求

口令要有最长使用期限限制。

加固建议

配置口令最长使用时间，设置口令为30天至90天后过期。

加固优先级

重要

实施/操作指南

在运行窗口输入“gpedit.msc”打开本地组策略。配置计算机配置 -> Windows设置 ->安全设置 ->账户策略->密码策略->密码最长使用期限的策略值为30-90之间数值。

6.1.4 错误登录尝试

要求

错误登录尝试次数要有最多次数限制。

加固建议

配置错误登录尝试次数，设置为不超过5次。

加固优先级

重要

实施/操作指南

在运行窗口输入“gpedit.msc”打开本地组策略。配置计算机配置 -> Windows设置 ->安全设置 ->账户策略->账户锁定策略->账户锁定阈值的策略值为“5”。

6.1.5 锁定持续时间

要求

锁定持续时间要有最短时间限制。

加固建议

配置锁定持续时间，设置至少为15分钟。

加固优先级

重要

实施/操作指南

在运行窗口输入“gpedit.msc”打开本地组策略。配置计算机配置 -> Windows设置 ->安全设置 ->账户策略->账户锁定策略->账户锁定时间的策略值大于等于15。

6.1.6 登录计数器

要求

重置登录计数器要有最短时间限制。

加固建议

配置重置登录计数器之前的时间，设置至少为15分钟。

加固优先级

重要

实施/操作指南

在运行窗口输入“gpedit.msc”打开本地组策略。配置计算机配置 -> Windows设置 ->安全设置 ->账户策略->账户锁定策略->重置账户锁定计数器的策略值大于等于15。

6.1.7 口令使用历史

要求

用户不能重复使用最近已使用的口令。

加固建议

配置强制口令历史，设置至少为10个。

加固优先级

重要

实施/操作指南

在运行窗口输入“gpedit.msc”打开本地组策略。配置计算机配置 -> Windows设置 ->安全设置 ->账户策略->密码策略->强制密码历史的策略值大于等于10。

6.1.8 空闲会话时间

要求

对于远程登录的账号，要设置强制终结空闲会话的时间。

加固建议

设置该空闲时间不超过15分钟。

加固优先级

重要

实施/操作指南

控制面板->管理工具->本地安全策略->本地策略->安全选项。打开选项“Microsoft 网络服务器：暂停会话前所需的空闲时间数量”的属性页。设置“中断连接如果空闲时间超过”小于等于15分钟。

6.1.9 屏幕保护

要求

设置带口令的屏幕保护，并设定进入屏幕保护的空闲时间。

加固建议

设置带口令的屏幕保护，并将时间设定为至少5分钟。

加固优先级

重要

实施/操作指南

进入“控制面板->显示->屏幕保护程序”。启用屏幕保护程序，设置等待时间为大于等于5分钟，启用“在恢复时使用密码保护”。

6.2 访问控制

通过访问控制管理可以减少主机被非法远程登录，以及减少通过共享等方式使计算机感染恶意代码的可能性。本节主要针对账户管理、账户使用、权限管理等与访问控制等有关策略提供安全加固建议。

6.2.1 管理员账号

要求

禁用或更改Administrator管理员账户。

加固建议

禁用Administrator账户或把Administrator更改成其他名称。

加固优先级

重要

实施/操作指南

进入“控制面板→管理工具→计算机管理”，在“系统工具→本地用户和组→用户”：

Administrator→属性→重命名或设置“账户已禁用”；

或Administrator→重命名→修改为其他名称。

6.2.2 Guest 账户

要求

禁用Guest来宾账户。

加固建议

禁用Guest来宾账户。

加固优先级

重要

实施/操作指南

进入“控制面板->系统和安全->管理工具->计算机管理”，在“系统工具->本地账号和组”，查看Administrator、Guest及其他账号状态，选择Guest账号，右击属性，勾选“账户已禁用”。

6.2.3 多余或者过期账户

要求

删除多余或者过期的账户。

加固建议

删除多余或者过期的账户。

加固优先级

重要

实施/操作指南

进入“控制面板->系统和安全->管理工具->计算机管理”，在“系统工具->本地账号和组”，查看多余或者过期的账号状态，选择该账号，进行删除。

6.2.4 用户自动登录

要求

禁止用户开机自动登录。

加固建议

禁止用户开机自动登录。

加固优先级

重要

实施/操作指南

在“开始->运行->键入 regedit”

设置注册表项：

HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\AutoAdminLogon (REG_DWORD)，值为0。

6.2.5 远程强制关机

要求

限定拥有“从远程系统强制关机”权限的用户。

加固建议

只允许Administrators或改名的管理员具备远程关机权限。

加固优先级

重要

实施/操作指南

在运行窗口输入“gpedit.msc”打开本地组策略。配置计算机配置 -> Windows设置 ->安全设置 ->本地策略 ->用户权限分配 ->“从远程系统强制关机”的策略值。

6.2.6 共享文件夹访问

要求

只将共享文件夹权限授予指定账户。

加固建议

共享文件夹不能有everyone的权限，只允许授权的账户拥有权限共享此文件夹。

加固优先级

重要

实施/操作指南

进入“控制面板->管理工具->计算机管理”，进入“系统工具—>共享文件”；修改对应共享文件夹的共享权限。

6.2.7 匿名访问命名

要求

禁用匿名访问命名管道和共享。

加固建议

禁用匿名访问命名管道和共享。

加固优先级

重要

实施/操作指南

“控制面板->管理工具->本地安全策略”，在“本地策略->安全选项”：网络访问：可匿名访问的共享设置为全部删除。

“控制面板->管理工具->本地安全策略”，在“本地策略->安全选项”：网络访问：可匿名访问的命名管道设置为全部删除。

6.2.8 共享账户

要求

应按照不同的用户分配不同的账号，避免不同用户间共享账号。避免用户账号和设备间通信使用的账号共享。

加固建议

为不同的用户分配不同的账户。

加固优先级

一般

实施/操作指南

进入“控制面板->管理工具->计算机管理”，在“系统工具->本地用户和组”：根据系统的要求，设定不同的账户和账户组。

6.2.9 远程访问

要求

禁止未经授权的远程访问注册表路径。

加固建议

“远程访问的注册表路径和子路径”的配置已全部删除或仅配置需要远程访问的注册表路径。

加固优先级

一般

实施/操作指南

配置计算机配置 -> Windows设置 ->安全设置 ->本地策略 ->安全选项 ->“网络访问：可远程访问的注册表路径”的策略值为“System\CurrentControlSet\Control\ProductOptions

System\CurrentControlSet\Control\Server Applications

Software\Microsoft\Windows NT\CurrentVersion”。

6.2.10 域控环境

6.2.10.1 拒绝从网络访问计算机

要求

配置“拒绝从网络访问这台计算机”的用户权限。

加固建议

“拒绝从网络访问这台计算机”的策略值仅包含Enterprise Admins组、Domain Admins组、本地账户、Guests组。

加固优先级

一般

实施/操作指南

在运行窗口输入“gpedit.msc”打开本地组策略。配置计算机配置 -> Windows设置 ->安全设置 ->本地策略 ->用户权限分配 ->“拒绝从网络访问这台计算机”配置相应值。

6.2.10.2 拒绝批处理作业登录

要求

配置 “拒绝作为批处理作业登录”的用户权限。

加固建议

“拒绝作为批处理作业登录”的策略值仅包含Enterprise Admins组、Domain Admins组、Guests组。

加固优先级

一般

实施/操作指南

在运行窗口输入“gpedit.msc”打开本地组策略。配置计算机配置 -> Windows设置 ->安全设置 ->本地策略 ->用户权限分配 ->“拒绝作为批处理作业登录”配置相应值。

6.2.10.3 拒绝服务登录

要求

配置“拒绝作为服务登录”的用户权限。

加固建议

“拒绝作为服务登录”的策略值仅包含Enterprise Admins组、Domain Admins组。

加固优先级

一般

实施/操作指南

在运行窗口输入“gpedit.msc”打开本地组策略。配置计算机配置 -> Windows设置 ->安全设置 ->本地策略 ->用户权限分配 ->“拒绝作为服务登录”配置相应值。

6.2.10.4 拒绝本地登录

要求

配置“拒绝本地登录”的用户权限。

加固建议

“拒绝本地登录”的策略值仅包含Enterprise Admins组、Domain Admins组、Guests组。

加固优先级

一般

实施/操作指南

在运行窗口输入“gpedit.msc”打开本地组策略。配置计算机配置 -> Windows设置 ->安全设置 ->本地策略 ->用户权限分配 ->“拒绝本地登录”配置相应值。

6.2.10.5 拒绝远程桌面服务登录

要求

配置“拒绝通过远程桌面服务登录”的用户权限。

加固建议

“拒绝通过远程桌面服务登录”的策略值仅包含以下内容：

如果组织未使用远程桌面服务，请将Everyone组分配为此权限以阻止所有访问；

如果组织使用RDS，仅包含Enterprise Admins组、Domain Admins组、本地账户、Guests组。

加固优先级

一般

实施/操作指南

在运行窗口输入“gpedit.msc”打开本地组策略。配置计算机配置 -> Windows设置 ->安全设置 ->本地策略 ->用户权限分配 ->“拒绝通过远程桌面服务登录”配置相应值。

6.3 安全审计

通过系统的安全审计相关功能可以对主机内重要事件进行记录，为调查取证提供依据。本节主要针对安全主体、行为、日志等与安全审计等有关策略提供安全加固建议。

6.3.1 账户登录审计

要求

对用户登录进行审计。

加固建议

开启“审核登录事件”策略，当有非法账号登录后，可以对登录终端的账号或注销的账号进行记录（记录信息主要包含源IP、端口、登录方式等）。

加固优先级

重要

实施/操作指南

在运行窗口输入“gpedit.msc”打开本地组策略。配置计算机配置 -> Windows设置 ->安全设置 ->高级审核策略配置 ->系统审核策略-本地组策略对象 ->账户登录 ->“审核凭证验证”、“审核Kerberos身份验证服务”、“审核Kerberos服务票证操作”以及“审核其他账户登录事件”的策略值，并勾选“配置以下审核事件”的“成功”复选框，以及“失败”复选框。

6.3.2 账户管理审计

要求

对计算机上的每个账户管理进行审计。

加固建议

开启“账户管理”策略，对计算机账户管理相关活动进行记录。

加固优先级

重要

实施/操作指南

在运行窗口输入“gpedit.msc”打开本地组策略。配置计算机配置 -> Windows设置 ->安全设置 ->高级审核策略配置 ->系统审核策略-本地组策略对象 ->账户管理 ->“审核计算机账户管理”、“审核通讯组管理”、“审核其他账户管理事件”、“审核安全组管理”以及“审核用户账户管理”的策略值，并勾选“配置以下审核事件”的“成功”复选框，以及“失败”复选框。

6.3.3 进程详细跟踪审计

要求

对计算机程序进程活动详情进行审计。

加固建议

开启“详细跟踪”策略，可以对计算机程序进程活动详情进行记录。

加固优先级

一般

实施/操作指南

在运行窗口输入“gpedit.msc”打开本地组策略。配置计算机配置 -> Windows设置 ->安全设置 ->高级审核策略配置 ->系统审核策略-本地组策略对象 ->详细跟踪 ->“审核DPAPI活动”、“审核进程创建”、

“进程终止”以及“审核RPC事件”的策略值，并勾选“配置以下审核事件”的“成功”复选框，以及“失败”复选框。

6.3.4 目录服务访问审计

要求

对计算机的目录服务访问进行审计。

加固建议

开启“审核DS访问”策略，可以对访问计算机目录进行记录。

加固优先级

一般

实施/操作指南

在运行窗口输入“gpedit.msc”打开本地组策略。配置计算机配置 -> Windows设置 ->安全设置 ->高级审核策略配置 ->系统审核策略-本地组策略对象 ->DS访问 ->“审核详细的目录服务复制”、“审核目录服务访问”、“审核目录服务更改”、“审核目录服务复制”的策略值，并勾选“配置以下审核事件”的“成功”复选框，以及“失败”复选框。

6.3.5 计算机登录事件审计

要求

对计算机登录/注销相关事件进行审计。

加固建议

开启“审核登录/注销”策略，可以对计算机登录/注销事件进行记录。

加固优先级

一般

实施/操作指南

在运行窗口输入“gpedit.msc”打开本地组策略。配置计算机配置 -> Windows设置 ->安全设置 ->高级审核策略配置 ->系统审核策略-本地组策略对象 ->登录/注销 ->“审核账户锁定”、“审核IPsec扩展模式”、“审核IPsec主模式”、“审核IPsec快速模式”、“审核注销”、“审核登录”、“审核网络策略服务器”、“审核其他登录/注销事件”以及“审核特殊登录”，并勾选“配置以下审核事件”的“成功”复选框，以及“失败”复选框。

6.3.6 对象访问审计

要求

对对象访问进行审计。

加固建议

开启“审核对象访问”策略，可以对对象访问进行记录。

加固优先级

一般

实施/操作指南

在运行窗口输入“gpedit.msc”打开本地组策略。配置计算机配置 -> Windows设置 ->安全设置 ->高级审核策略配置 ->系统审核策略-本地组策略对象 ->对象访问 ->“审核已生成应用程序”、“审核证书服务”、“审核详细的文件共享”、“审核文件共享”、“审核文件系统”、“审核筛选平台连接”、“审核筛选平台数据包丢弃”、“审核句柄操作”、“审

核内核对象”、“审核其他对象访问事件”、“审核注册表”以及“审核SAM”的策略值，并勾选“配置以下审核事件”的“成功”复选框，以及“失败”复选框。

6.3.7 策略更改审计

要求

对用户进行本地安全策略变更时进行审计。

加固建议

开启“审核策略变更”策略，当有攻击者进行本地安全策略变更时，可以对尝试更改终端账号权限分配策略、审核策略、账号策略或信任策略的每一个事件进行记录。

加固优先级

重要

实施/操作指南

在运行窗口输入“gpedit.msc”打开本地组策略。配置计算机配置 -> Windows设置 ->安全设置 ->高级审核策略配置 ->系统审核策略-本地组策略对象 ->策略更改 ->“审核审核策略更改”、“审核身份验证策略更改”、“审核授权策略更改”、“审核筛选平台”以及“审核MPSSVC规则级别策略更改”以及“审核其他策略更改事件”的策略值，并勾选“配置以下审核事件”的“成功”复选框，以及“失败”复选框。

6.3.8 特权使用审计

要求

对特权使用进行审计。

加固建议

开启“审核特权使用”策略，可以记录特权使用记录。

加固优先级

重要

实施/操作指南

在运行窗口输入“gpedit.msc”打开本地组策略。配置计算机配置 -> Windows设置 ->安全设置 ->高级审核策略配置 ->系统审核策略-本地组策略对象 ->特权使用 ->“审核非敏感权限使用”、“审核其他权限使用事件”以及“审核敏感权限使用”的策略值，并勾选“配置以下审核事件”的“成功”复选框，以及“失败”复选框。

6.3.9 系统事件审计

要求

对系统相关事件进行审计。

加固建议

开启“审核系统事件”策略，可以对系统相关事件进行记录。

加固优先级

一般

实施/操作指南

在运行窗口输入“gpedit.msc”打开本地组策略。配置计算机配置 -> Windows设置 ->安全设置 ->高级审核策略配置 ->系统审核策略-本地组策略对象 ->系统 ->“审核IPsec驱动程序”、“审核其他系统事件”、“审核安全状态更改”、“审核安全系统扩展”以及“审核系统完整

性”的策略值，并勾选“配置以下审核事件”的“成功”复选框，以及“失败”复选框。

6.3.10 全局对象访问审计

要求

对文件系统和注册表全局对象访问进行审计。

加固建议

开启“审核全局对象访问”策略，可以对文件系统和注册表全局对象访问进行记录。

加固优先级

一般

实施/操作指南

在运行窗口输入“gpedit.msc”打开本地组策略。配置计算机配置 -> Windows设置 ->安全设置 ->高级审核策略配置 ->系统审核策略-本地组策略对象 ->全局对象访问审计 ->“文件系统”和“注册表”的策略值，并勾选“配置以下审核事件”的“成功”复选框，以及“失败”复选框。

6.3.11 日志配额

要求

系统日志额度要有最小值要求。

加固建议

设置日志容量，可以在恶意用户在攻击系统时记录攻击日志，保证日志存储能够进行溯源。

加固优先级

一般

实施/操作指南

在运行窗口输入“gpedit.msc”打开本地组策略。将计算机配置 -> 管理模板 -> Windows组件 ->事件日志服务 ->系统 ->“最大日志大小（KB）”的策略值配置为“已启用：最大日志大小（KB）为‘32768’（经验值，可满足《中华人民共和国网络安全法》最低保存日志时间180天的存储要求）或更高”。

注：如果系统配置为将审计记录直接发送到审计服务器，则该组策略不适用。

6.4 入侵防范

通过入侵防范相关功能可以减少主机被远程攻击的可能性，缩小主机暴露面。本节主要针对系统服务、共享、端口的使用等与入侵防范等方面提供安全加固建议。

6.4.1 系统服务

要求

关闭非必要的系统服务。

加固建议

停止并禁用非必要的系统服务，建议关闭的服务见附录C。

加固优先级

一般

实施/操作指南

在运行窗口输入“Services.msc”打开服务控制面板，将Shared Information（信息共享）、Dynamic Data Exchange（动态数据交换）、

FTP、Telnet、Remote Desktop Services（远程桌面连接）、Remote Registry（远程注册表）等系统服务设置为禁用。

6.4.2 默认共享

要求

关闭默认共享。

加固建议

将默认共享关闭。

加固优先级

重要

实施/操作指南

在运行窗口输入“Regedit”，进入注册表编辑器，新增注册表键值，具体注册表路径HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\ 值名称：AutoShareServer，值名称：AutoShareWKS，值类型：REG_DWORD值：0。

6.4.3 系统防火墙

要求

启用系统防火墙。

加固建议

启用系统防火墙。

加固优先级

重要

实施/操作指南

进入“控制面板—>系统和安全—>Windows防火墙—>打开或关闭Windows防火墙”，选择“启用Windows防火墙”。

6.4.4 SYN 攻击保护

要求

启用SYN攻击保护。

加固建议

启用SYN攻击保护功能并设置TCP连接数的阈值。

加固优先级

一般

实施/操作指南

在“开始->运行->键入 regedit”,查看注册表项，进入HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters；新建以下字符串值并设置相应数据：

SynAttackProtect，设为2；

TcpMaxportsExhausted，设为5；

TcpMaxHalfOpen，设为500；

TcpMaxHalfOpenRetried，设为400。

6.4.5 高危端口

要求

关闭高危端口。

加固建议

使用系统防火墙或其他安全软件禁用非必要的高危端口，建议关闭的端口见附录D。

加固优先级

重要

实施/操作指南

使用系统防火墙或其他安全软件禁用高危端口。如：135、137、138、139、445、593、1025、2745、3127、3389、6129。

附录A 建议安装的系统补丁

一些重点高危漏洞可以通过安全系统补丁进行修复。建议在条件允许情况下，确保以下补丁已被安装。建议安装的系统补丁见表A.1。

表 A.1 建议安装的系统补丁列表

序号	漏洞描述	补丁
1	Microsoft 辅助功能驱动程序特权提升漏洞	KB2961072
2	HTTP.sys 中的漏洞可能允许远程执行代码	KB3042553
3	Microsoft Windows SMB 输入验证错误漏洞	KB4012212
4	Microsoft Office 内存损坏漏洞	KB3162047
5	Microsoft Remote Desktop Services 资源管理错误漏洞	KB4499164
6	Microsoft Internet Explorer 脚本引擎内存损坏漏洞	KB4537820
7	Windows cng.sys提权漏洞	KB5008244
8	Microsoft Windows TCP/IP 拒绝服务漏洞	KB4601347

附录B 常见的高危漏洞

对于一些具有高危害、易操作、权限高的漏洞，建议进行修复。常见高危漏洞参见表B.1。

表 B.1 常见的高危漏洞列表

序号	漏洞描述	漏洞编号
1	Microsoft 辅助功能驱动程序特权提升漏洞	CVE-2014-1767
2	HTTP.sys 中的漏洞可能允许远程执行代码	CVE-2015-1635
3	Microsoft Windows SMB 输入验证错误漏洞	CVE-2017-0143
4	Microsoft Windows SMB 输入验证错误漏洞	CVE-2017-0144
5	Microsoft Office 内存损坏漏洞	CVE-2017-11882
6	Microsoft Remote Desktop Services 资源管理错误漏洞	CVE-2019-0708
7	Internet连接共享服务远程代码执行漏洞	CVE-2020-0662
8	Microsoft Internet Explorer 脚本引擎内存损坏漏洞	CVE-2020-0674
9	Microsoft Graphics 远程代码执行漏洞	CVE-2020-0687
10	远程桌面客户端远程代码执行漏洞	CVE-2020-0734
11	Media Foundation 内存损坏漏洞	CVE-2020-0738
12	GDI+ 远程代码执行漏洞	CVE-2020-0881
13	GDI+ 远程代码执行漏洞	CVE-2020-0883
14	Jet 数据库引擎远程代码执行漏洞	CVE-2020-0889
15	Microsoft 图形组件远程代码执行漏洞	CVE-2020-0907
16	Microsoft COM for Windows 远程执行代码漏洞	CVE-2020-0922
17	GDI+ 远程代码执行漏洞	CVE-2020-0964
18	Jet 数据库引擎远程代码执行漏洞	CVE-2020-0992
19	组策略特权提升漏洞	CVE-2020-1013
20	Windows权限提升漏洞	CVE-2020-1015
21	Microsoft 脚本运行时远程执行代码漏洞	CVE-2020-1061
22	Internet Explorer 内存损坏漏洞	CVE-2020-1062
23	Windows 远程代码执行漏洞	CVE-2020-1067
24	Windows 后台智能传输服务提权漏洞	CVE-2020-1112
25	Windows 任务计划程序安全功能绕过漏洞	CVE-2020-1113
26	Microsoft 图形组件远程代码执行漏洞	CVE-2020-1153
27	GDI+ 远程代码执行漏洞	CVE-2020-1285
28	LNK 远程代码执行漏洞	CVE-2020-1299
29	Windows SMB 已验证远程执行代码漏洞	CVE-2020-1301
30	组策略特权提升漏洞	CVE-2020-1317
31	Windows Media 远程代码执行漏洞	CVE-2020-1339

表 B.1 常见的高危漏洞列表（续）

序号	漏洞描述	漏洞编号
32	Microsoft Graphics 远程代码执行漏洞	CVE-2020-1408
33	DirectWrite 远程代码执行漏洞	CVE-2020-1409
34	Microsoft 图形组件远程代码执行漏洞	CVE-2020-1412
35	Visual Studio 和 Visual Studio Code 特权提升漏洞	CVE-2020-1416
36	GDI+ 远程代码执行漏洞	CVE-2020-1435
37	Windows Media 音频解码器远程代码执行漏洞	CVE-2020-1508
38	Microsoft 图形组件远程代码执行漏洞	CVE-2020-1562
39	GDI+ 远程代码执行漏洞	CVE-2020-16911
40	Windows Print Spooler 远程代码执行漏洞	CVE-2020-17042
41	Windows cng.sys提权漏洞	CVE-2020-17087
42	Windows SMB信息泄露漏洞	CVE-2020-17140
43	远程过程调用运行时远程代码执行漏洞	CVE-2021-1667
44	Microsoft DTV-DVD 视频解码器远程代码执行漏洞	CVE-2021-1668
45	Windows 打印后台处理程序远程执行代码漏洞	CVE-2021-1675
46	远程过程调用运行时远程代码执行漏洞	CVE-2021-1700
47	远程过程调用运行时远程代码执行漏洞	CVE-2021-1701
48	Windows LUAFV 特权提升漏洞	CVE-2021-1706
49	Windows Installer 特权提升漏洞	CVE-2021-1727
50	Microsoft Windows TCP/IP 拒绝服务漏洞	CVE-2021-24086
51	Internet Explorer 内存损坏漏洞	CVE-2021-26411
52	Windows Installer 特权提升漏洞	CVE-2021-26415
53	脚本引擎内存损坏漏洞	CVE-2021-26419
54	Windows NTFS 特权提升漏洞	CVE-2021-31956
55	脚本引擎内存损坏漏洞	CVE-2021-31959
56	Windows MSHTML 平台远程代码执行漏洞	CVE-2021-33742
57	脚本引擎内存损坏漏洞	CVE-2021-34448
58	Windows 打印后台处理程序远程执行代码漏洞	CVE-2021-34527
59	Windows 远程桌面客户端远程代码执行漏洞	CVE-2021-34535
60	Windows 打印后台处理程序远程执行代码漏洞	CVE-2021-36958
61	Windows 远程桌面客户端远程代码执行漏洞	CVE-2021-38666
62	Microsoft MSHTML远程代码执行漏洞	CVE-2021-40444

附录C 建议关闭的服务

远程控制终端的服务，具有外连功能，使得Windows 7操作系统易成为攻击目标，建议非必要情况下关闭这些服务。建议关闭的相关服务见表C.1。

表 C.1 建议关闭的服务列表

序号	服务名称	建议操作
1	DHCP Client	如果不使用动态IP地址，建议禁用
2	Background Intelligent Transfer Service	如果不启用自动更新，建议禁用
3	Computer Browser	局域网里用来自动搜索网上邻居的一个服务项，建议禁用
4	Diagnostic Policy Service	诊断策略服务启用了 Windows 组件的问题检测、疑难解答和解决方案,建议禁用
5	IP Helper	该服务用于转换IPv6 to IPv4，建议禁用
6	Print Spooler	如果不需要打印，建议禁用
7	Remote Registry	主要用于远程管理注册表，建议禁用
8	Server	禁用本服务将关闭默认共享,如ipc$、admin$和C$等，如果不使用文件共享，建议禁用
9	TCP/IP NetBIOS Helper	提供NetBIOS名称解析支持，允许客户端共享文件、打印机和登录到网络中，若你的计算机没有连接到工作组网络的话，建议禁用
10	Windows Remote Management (WS-Management)	远程管理（WinRM）服务，建议禁用
11	Windows Font Cache Service	用于缓存常用字体数据，建议禁用
12	Telnet	远程终端，如果不使用，建议禁用
13	FTP	用于文件传输，如果不使用，建议禁用
14	Simple Mail Transfer Protocol(SMTP)	用于邮件传输，如果不使用，建议禁用
15	Windows Error Reporting Service	报告错误并提供现有解决方案，建议禁用
16	Terminal Service	允许多位用户连接并控制一台机器，建议禁用
17	Task Scheduler	任务计划，建议禁用
18	Simple Network Management Protocol(SNMP) Service	SNMP允许远程管理设备，如不使用，建议禁用

附录D 建议关闭的端口

端口提供了远程接入主机的主要通道，攻击者可能利用这些端口对主机发起攻击，建议对非必要端口进行关闭。建议关闭的端口见表D.1。

表 D.1 建议关闭的端口列表

序号	端口	端口描述
1	TCP 20,21	FTP（文件传输协议）。FTP服务器漏洞较多，比如匿名身份验证、目录浏览、跨站脚本，同时明文传输密码
2	TCP 23	Telnet（远程终端协议）。攻击者可以监听Telnet报文，查找登录凭证信息，通过中间人攻击注入指令最终执行远程代码
3	TCP 25	SMTP（简单邮件传输协议）。邮件伪造，vrfy/expn查询邮件用户信息
4	TCP/UDP 42	Nameserver（WINS主机名服务）
5	TCP/UDP 53	Domain（DNS域名服务）。通常被用来执行区域传送、DNS劫持、缓存投毒、欺骗以及各种用于DNS隧道的远程控制
6	TCP 110	POP3（邮局协议版本3）。可尝试爆破，嗅探
7	TCP/UDP 135	RPC（远程过程调用）服务。使用RPC协议并提供DCOM服务，攻击者可以利用此端口远程打开对方的telnet服务，用于启动与远程计算机的RPC连接，通过RPC可以执行远程计算机上的代码
8	UDP 137,138,139	netbios-ns（NetBIOS 名称解析）。可尝试爆破以及smb自身的各种远程执行类漏洞利用，如MS08-067，MS17-010嗅探等
9	UDP 138	netbios-dgm（NetBIOS 数据报服务）
10	TCP139	netbios-ssn（NetBIOS 会话服务）
11	UDP 161	SNMP（简单网络管理协议）。SNMP允许远程管理设备，通过SNMP可获得管理设备的配置和运行信息。爆破攻击常用方式，搜集目标内网信息
12	TCP/UDP 445	Microsoft-ds（SMB 服务器 Windows文件和打印机共享）。黑客一般使用工具‘MS06-040’或‘MS08-067’ 。可使用专用的445端口扫描器进行扫描
13	TCP 593	DCOM（Distributed Component Object Model，分布式组件对象模型）协议。它允许C/S结构的应用通过DCOM使用RPC over HTTP service
14	TCP 1025	Windows动态分配的监听端口。匿名接入该端口后，就可获取Windows网络的服务器信息与用户信息等
15	TCP 1080	Socks代理服务。常被攻击者用来执行恶意软件，蠕虫病毒Mydoom和Bugbear就一直用1080端口进行攻击

表 D.1 建议关闭的端口列表（续）

序号	端口	端口描述
16	UDP 1645,1646	RADIUS（旧式 RADIUS Internet 身份验证服务）
17	UDP 1812	RADIUS（身份验证 Internet 身份验证服务）
18	UDP 1813	Radacct（计账 Internet 身份验证服务）
19	TCP 3389	Windows RDP（桌面协议）。攻击者可以利用这个端口，远程控制服务器，控制后可以进行一些系统操作比如文件的导入导出
20	TCP 2745,2773,3127,3128 ,3198,3332,6129	流行病毒的后门端口： 2745=Worm.BBeagle.k 2773=Backdoor,SubSeven 3127=Worm.Novarg 3128=RingZero,Worm.Novarg.B 3198=Worm.Novarg 3332=Worm.Cycle.a 6129=Dameware Nt Utilities服务器

参考文献

[1] GB/T 30278-2013 信息安全技术 政务计算机终端核心配置规范

[2] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

[3] GB/T 22081-2016 信息技术 安全技术 信息安全控制实践指南

[4] GB/T 20984 信息安全技术 信息安全风险评估方法

[5] CIS 2020《CIS Microsoft Windows 7 Workstation Benchmark》