Windows 系统高危漏洞

修复方案

广州华南信息安全测评中心

2017 年 04 月 16 日

1、 漏洞名称

Windows 系统高危漏洞

2、 漏洞说明

2017 年 4 月 15 日，国外黑客组织 Shadow Brokers 泄露出了一份机密文档，其中包含了多个 Windows 远程漏洞利用工具，外部攻击者利用此工具可远程攻击并获取服务器控制权限，该漏洞影响极大。

3、 漏洞风险

黑客可以通过发布的工具远程攻击服务器。

4、 受影响的版本

受影响版本:Windows NT、Windows 2000、Windows 2003、Windows 2008、Windows 2008 R2、Windows Server 2012 SP0、Windows XP、Windows Vista、Windows 7、Windows 8

5、 影响服务

主要影响 SMB 和 RDP 服务。

6、 风险级别

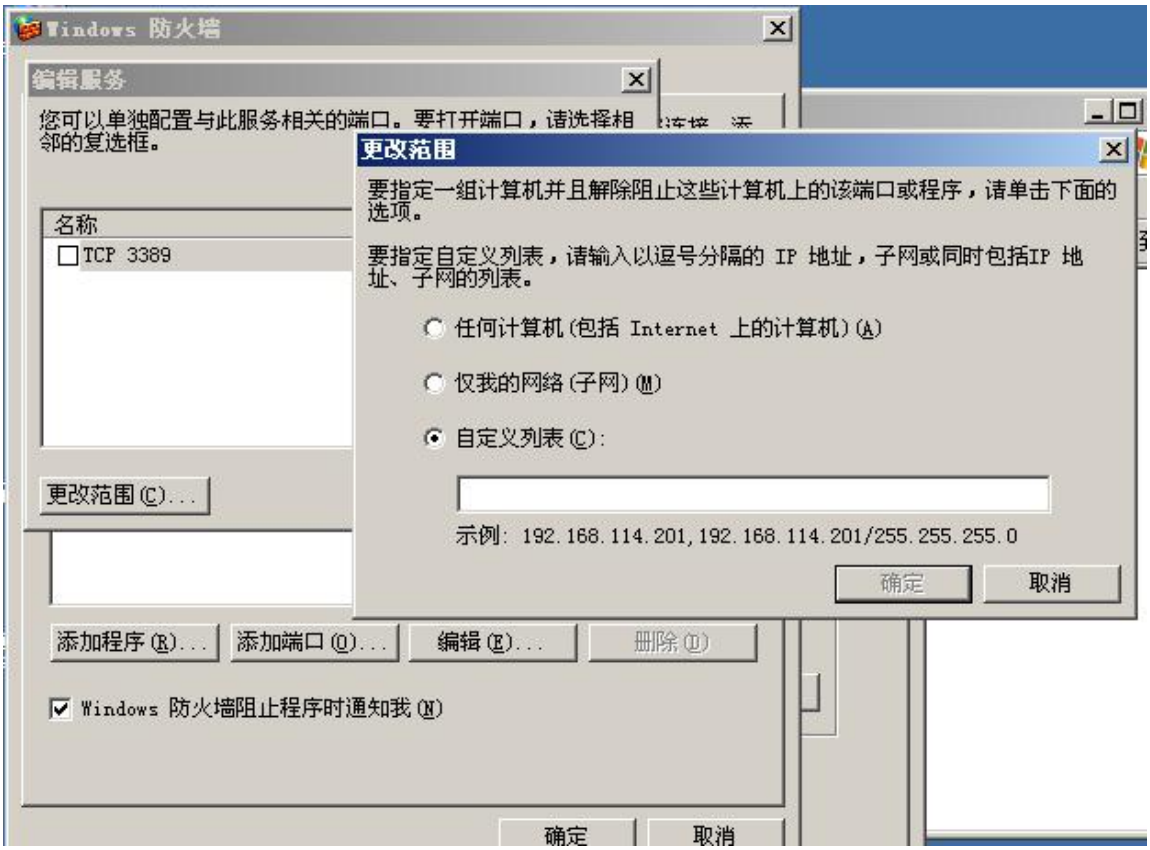
风险级别：高

7、 漏洞修复建议

7.1 应急解决方案

1)、使用系统自带的防火墙设置访问规则

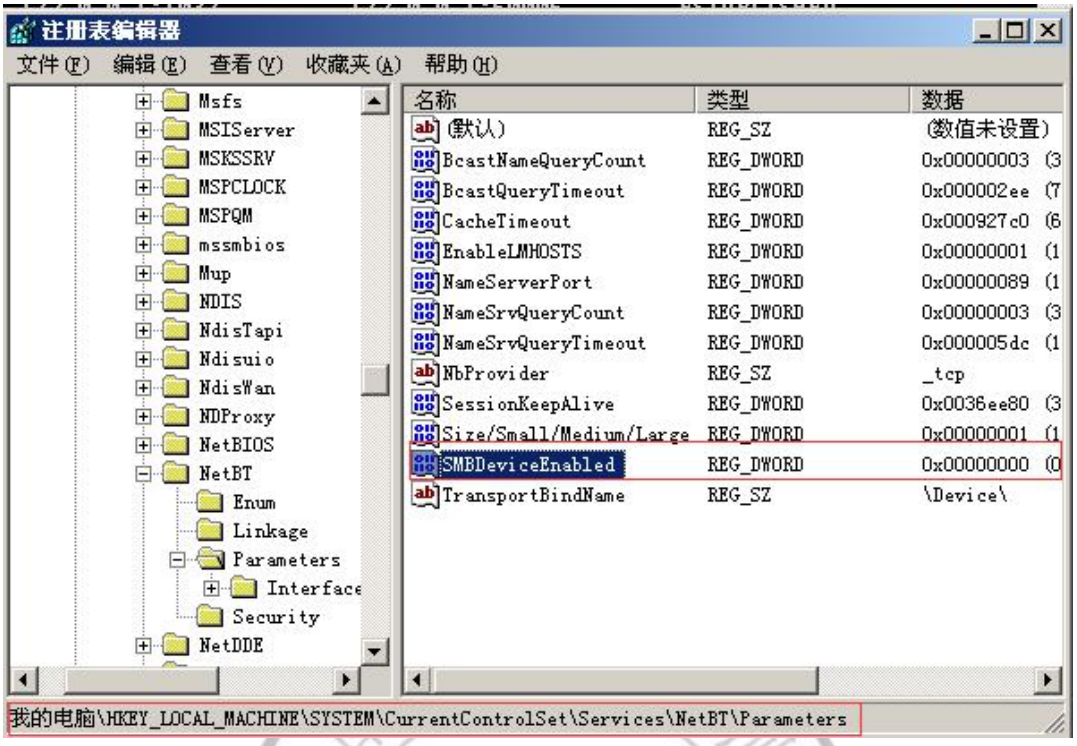
使用系统自带的防护墙，设置远程访问端口 137、139、445、3389 的源 IP。



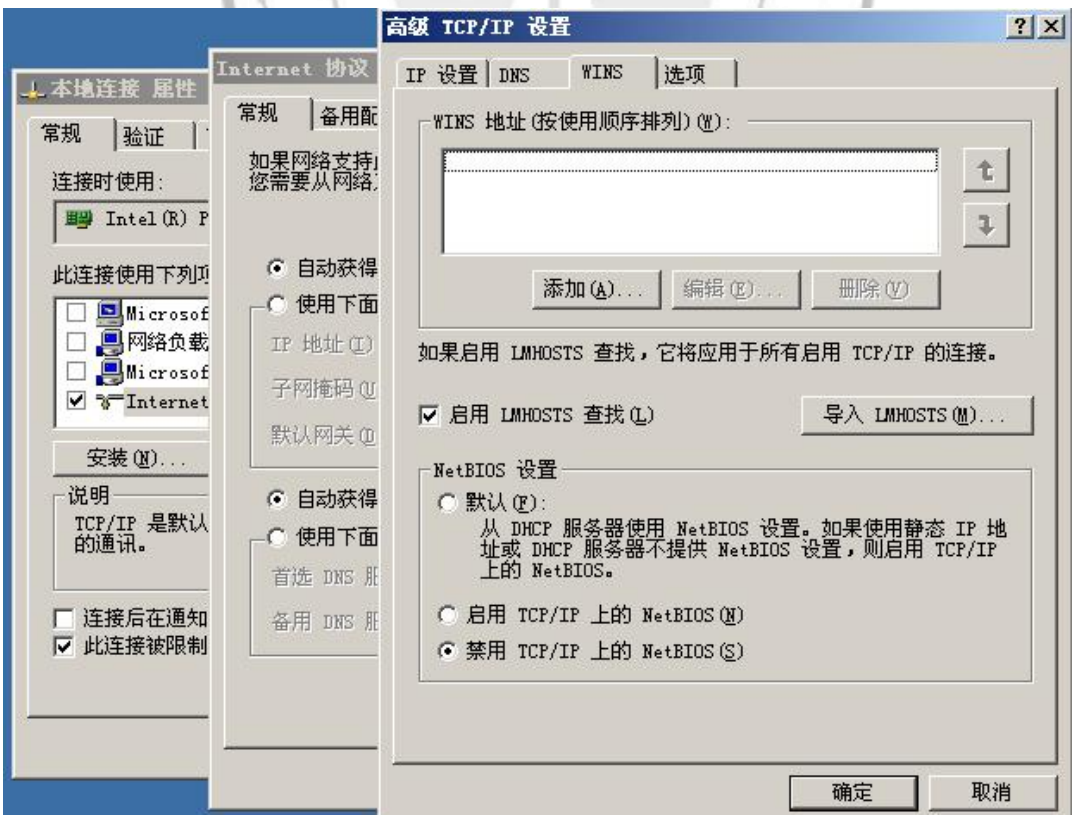
2)、Windows 临时关闭相应端口：

- 关闭 445 端口

修改注册表，添加一个键值（HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NetBT\Parameters）在右面的窗口建立一个 SMBDeviceEnabled 为 DWORD 类型键值为 0。

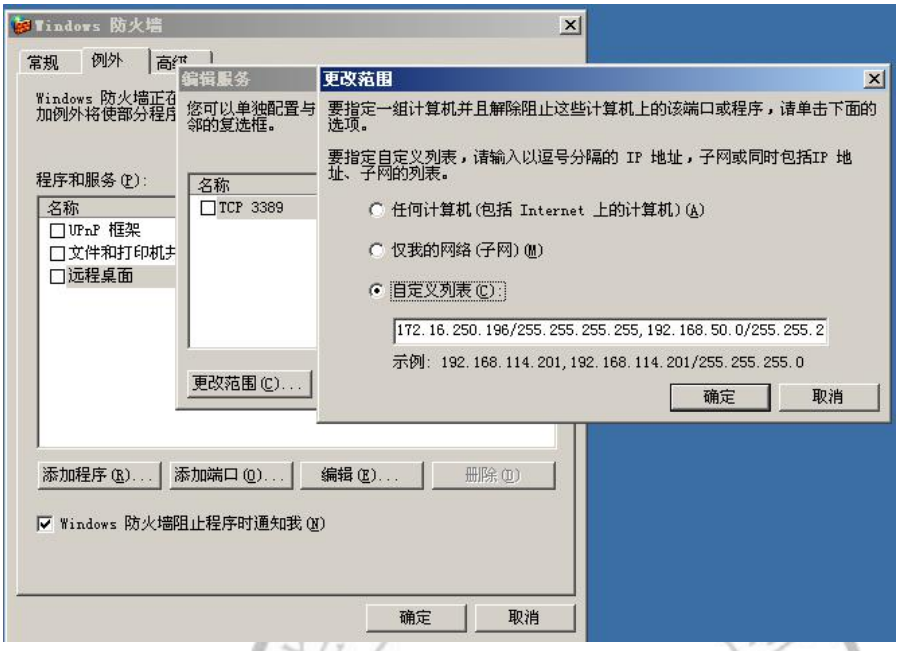

注册表编辑器
文件(F) 编辑(E) 查看(V) 收藏夹(A) 帮助(H)
Msfs
MSIServer
MSKSSRV
MSPCLOCK
MSPQM
mssmbios
Mup
NDIS
NdisTapi
Ndisuio
NdisWan
NDProxy
NetBIOS
NetBT
Enum
Linkage
Parameters
Interface
Security
NetDDE
名称 类型 数据
(默认) REG_SZ (数值未设置)
BcastNameQueryCount REG_DWORD 0x00000003 (3
BcastQueryTimeout REG_DWORD 0x000002ee (7
CacheTimeout REG_DWORD 0x000927c0 (6
EnableLMHOSTS REG_DWORD 0x00000001 (1
NameServerPort REG_DWORD 0x00000089 (1
NameSrvQueryCount REG_DWORD 0x00000003 (3
NameSrvQueryTimeout REG_DWORD 0x000005dc (1
NbProvider REG_SZ _tcp
SessionKeepAlive REG_DWORD 0x0036ee80 (3
Size/Small/Medium/Large REG_DWORD 0x00000001 (1
SMBDeviceEnabled REG_DWORD 0x00000000 (0
TransportBindName REG_SZ \Device\
我的电脑\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters

❖ 关闭 137、139 端口：


本地连接 属性
常规 验证
连接时使用:
Intel(R) P
此连接使用下列项
Microsof
网络负载
Microsof
Internet
安装(N)...
说明
TCP/IP 是默认
的通讯。
连接后在通知
此连接被限制
Internet 协议
常规 备用配
如果网络支持
您需要从网络
自动获得
使用下面
IP 地址(I)
子网掩码(U)
默认网关(D)
自动获得
使用下面
首选 DNS 服
备用 DNS 服
高级 TCP/IP 设置
IP 设置 DNS WINS 选项
WINS 地址(按使用顺序排列)(W):
添加(A)... 编辑(E)... 删除(V)
如果启用 LMHOSTS 查找，它将应用于所有启用 TCP/IP 的连接。
启用 LMHOSTS 查找(L)
导入 LMHOSTS(M)...
NetBIOS 设置
默认(F):
从 DHCP 服务器使用 NetBIOS 设置。如果使用静态 IP 地址或 DHCP 服务器不提供 NetBIOS 设置，则启用 TCP/IP 上的 NetBIOS。
启用 TCP/IP 上的 NetBIOS(N)
禁用 TCP/IP 上的 NetBIOS(S)
确定
取消

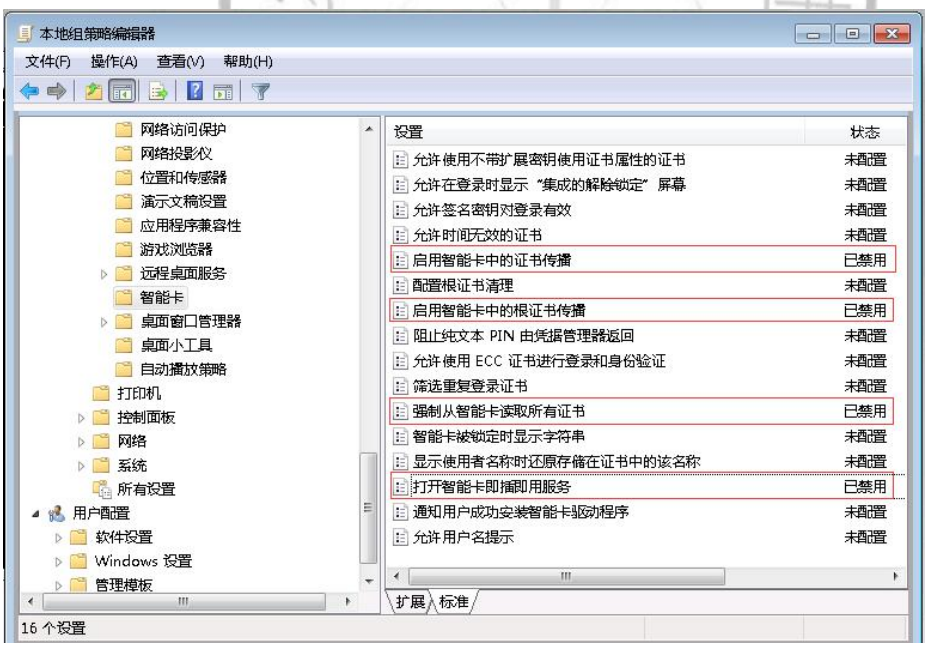
❖ 3389 端口：

Windows 2003：通过防火墙策略限制访问源 IP。



Windows 2008：在组策略中关闭智能卡登录功能。

组策略(gpedit.msc)-->管理模板-->Windows 组件-->智能卡



7.2 更新官方补丁方案：

截至目前，大部分漏洞官方均已发布相关补丁，建议您更新相关补丁。对应的补丁列表：MS17-010、MS10-061、MS14-068、MS17-010、MS09-050、MS17-010、MS08-067