安天应对微软 SMB 漏洞（CVE-2017-11780）响应手册

安天安全研究与应急处理中心（安天 CERT）

一、 概述

近日，国家信息安全漏洞共享平台（CNVD）收录了 Microsoft Windows SMB Server 远程代码执行漏洞（CNVD-2017-29681，对应 CVE-2017-11780）。远程攻击者成功利用漏洞可允许在目标系统上执行任意代码，如果利用失败将导致拒绝服务。CNVD 对该漏洞的综合评级为“高危”。综合业内各方研判情况，该漏洞影响版本范围跨度大，一旦漏洞细节披露，将造成极为广泛的攻击威胁，或可诱发 APT 攻击，安天提醒用户警惕出现“WannaCry”蠕虫翻版，建议根据本手册中“受影响系统版本”和“微软官方补丁编号”及时做好漏洞排查和处置工作。

二、 受影响系统版本

微软产品系列	具体版本
Microsoft Windows 7	x32-bit Systems SP1 x64-bit Systems SP1
Microsoft Windows 8.1	x32-bit Systems x64-bit Systems
Microsoft Windows RT 8.1	
Microsoft Windows 10	for x32-bit Systems for x64-bit Systems Version 1511 for x32-bit Systems Version 1511 for x64-bit Systems Version 1607 for x32-bit Systems Version 1607 for x64-bit Systems Version 1703 for x32-bit Systems Version 1703 for x64-bit Systems
Microsoft Windows Server 2008	R2 for Itanium-based Systems SP1 R2 for x64-bit Systems SP1 x32-bit Systems SP2 x64-bit Systems SP2 Itanium-based Systems SP2
Microsoft Windows Windows Server 2012 **Microsoft Windows Server 2012 R2**	
Microsoft Windows Server 2016	

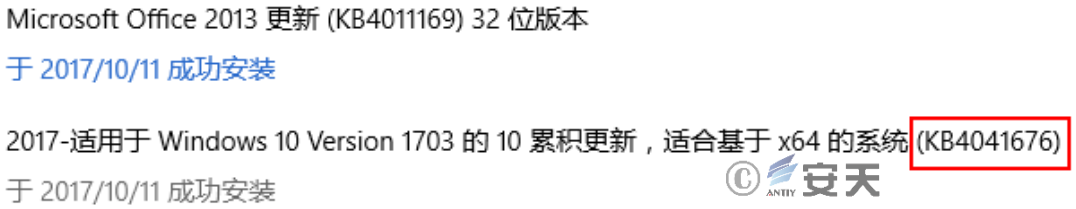
三、 防护解决方案

3.1 安装微软官方补丁

用户可根据系统安装补丁编号排查是否已经安装官方补丁。

Win7 系统操作如下：开始—>控制面板—>Windows Update—>查看更新历史记录。

Win10 系统操作如下：Windows 设置—>更新和安全—>历史更新记录（如下图）。



不同系统版本微软官方补丁编号、参考链接如下表（安全更新是本次漏洞单独补丁、月度累积更新是补丁集合含本次漏洞补丁）：

微软产系统版本	补丁编号（KB***）和链接
Windows 10 for 32-bit Systems	https://www.catalog.update.microsoft.com/Search.aspx?q=KB4042895（安全更新）
Windows 10 for x64-based Systems	
Windows 10 Version 1511 for 32-bit Systems	https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041689（安全更新）
Windows 10 Version 1511 for x64-based Systems	
Windows 10 Version 1607 for 32-bit Systems	https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041691（安全更新）
Windows 10 Version 1607 for x64-based Systems	
Windows 10 Version 1703 for 32-bit Systems	https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041676（安全更新）
Windows 10 Version 1703 for x64-based Systems	
Windows 7 for 32-bit Systems Service Pack 1	https://www.catalog.update.microsoft.com/Search.aspx?q=KB4041681（月度累积更新）
Windows 7 for x64-based Systems Service Pack 1	https://www.catalog.update.microsoft.com/Search.aspx?q=KB4041678（安全更新）
Windows 8.1 for 32-bit systems	https://www.catalog.update.microsoft.com/Search.aspx?q=KB4041693（月度累积更新）
Windows 8.1 for x64-based systems	https://www.catalog.update.microsoft.com/Search.aspx?q=KB4041687（安全更新）
Windows RT 8.1	https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041693（月度累积更新）
Windows Server 2008 for 32-bit Systems Service Pack 2	https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041995（安全更新）
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	
Windows Server 2008 for Itanium-Based Systems Service Pack 2	
Windows Server 2008 for x64-based Systems Service Pack 2	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041681（月度累积更新） https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041678（安全更新）
Windows Server 2008 R2 for x64-based Systems	

Service Pack 1	
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	
Windows Server 2012	https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041690（月度累积更新）
Windows Server 2012 (Server Core installation)	https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041679（安全更新）
Windows Server 2012 R2	https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041693（月度累积更新）
Windows Server 2012 R2 (Server Core installation)	https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041687（安全更新）
Windows Server 2016	https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4041691（安全更新）
Windows Server 2016 (Server Core installation)	

3.2 临时防护步骤

3.3 由于相关原因不能及时安装补丁的详细防护步骤如下：

- 关闭网络，开启系统防火墙；
- 利用系统防火墙高级设置阻止向 445 端口进行连接（该操作会影响使用 445 端口的服务）及网络共享；
- 打开网络，开启系统自动更新，并检测更新进行安装；

3.3.1 Win7 系统的处理流程举例：

1) 关闭网络

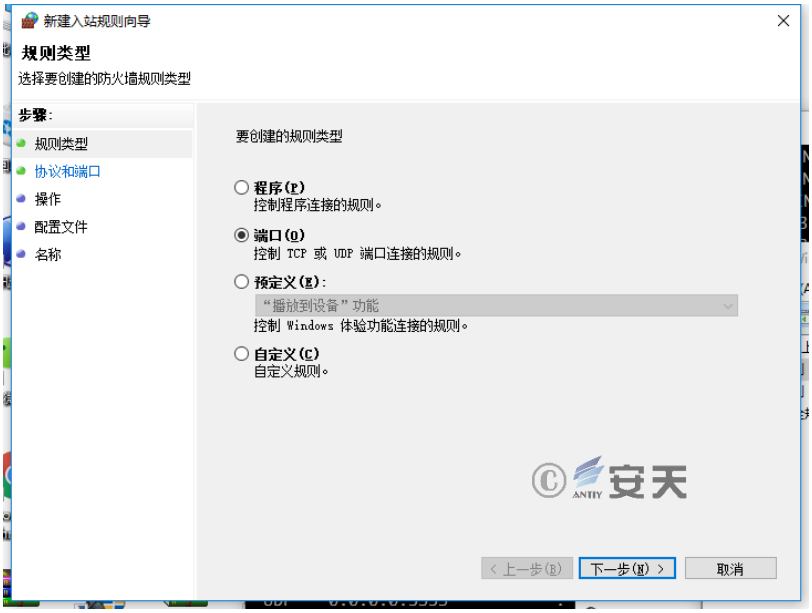
2) 打开控制面板-系统与安全-Windows 防火墙，点击左侧启动或关闭 Windows 防火墙

3) 选择启动防火墙，并点击确定

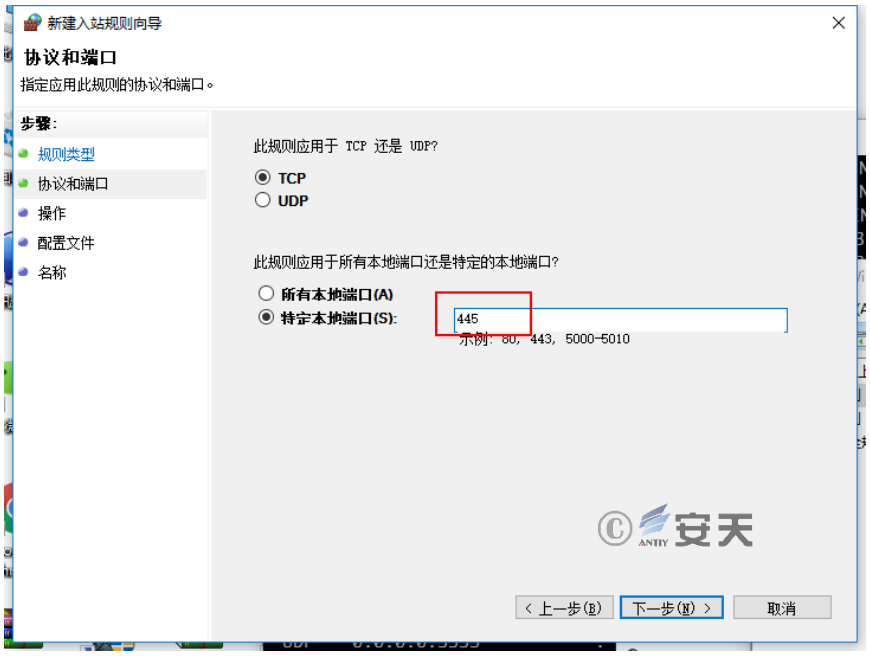
4) 点击高级设置

5) 点击入站规则，新建规则，以 445 端口为例

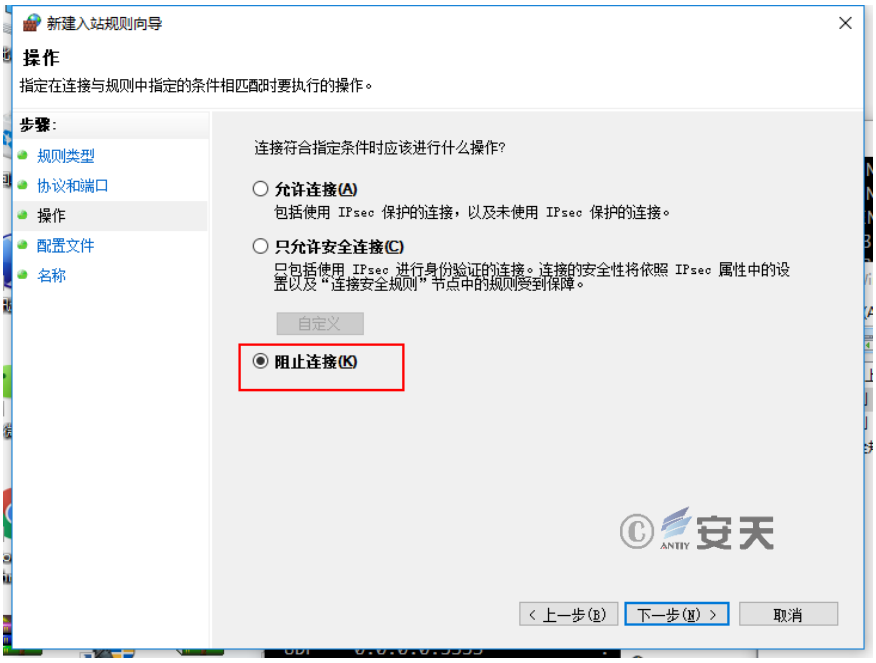
6) 选择端口、下一步



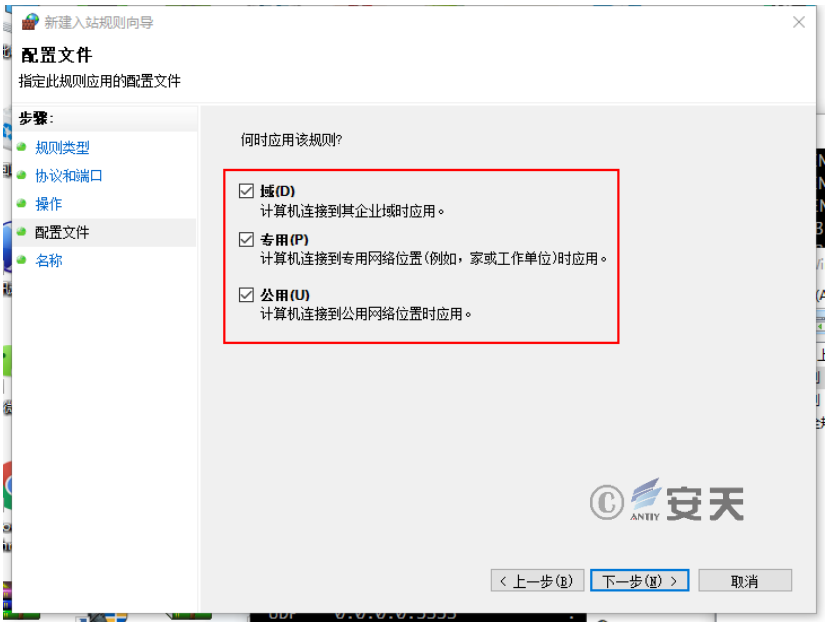
7) 选择特定本地端口，输入 445，下一步



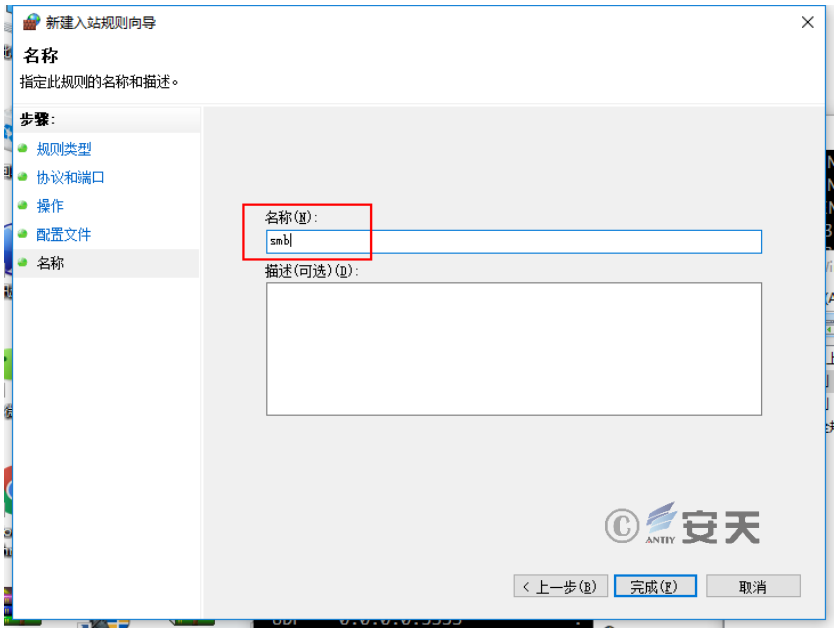
8) 选择阻止连接，下一步



9) 配置文件，全选，下一步

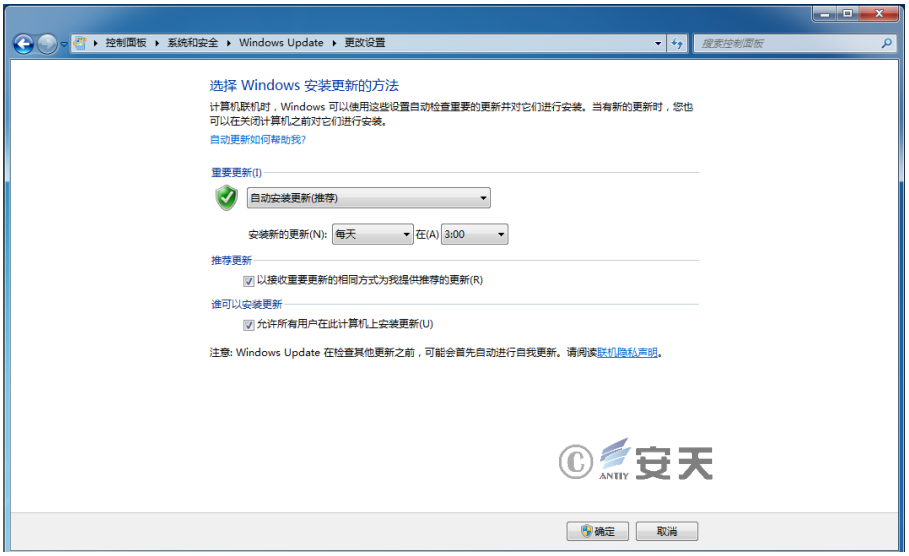


10) 名称，可以任意输入，完成即可。



11) 恢复网络

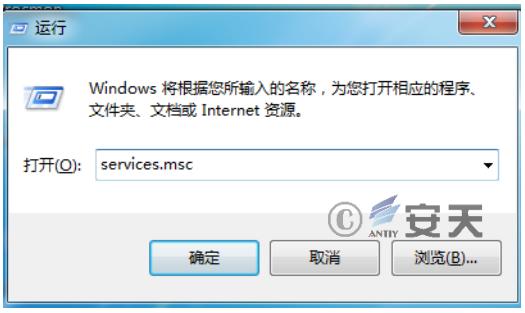
12) 开启系统自动更新，并检测更新进行安装



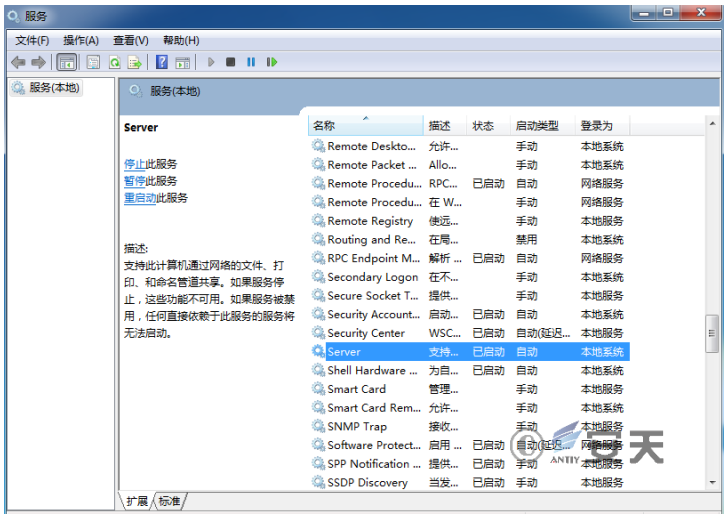
13) Win7 系统需要关闭 Server 服务才能够禁用 445 端口的连接。

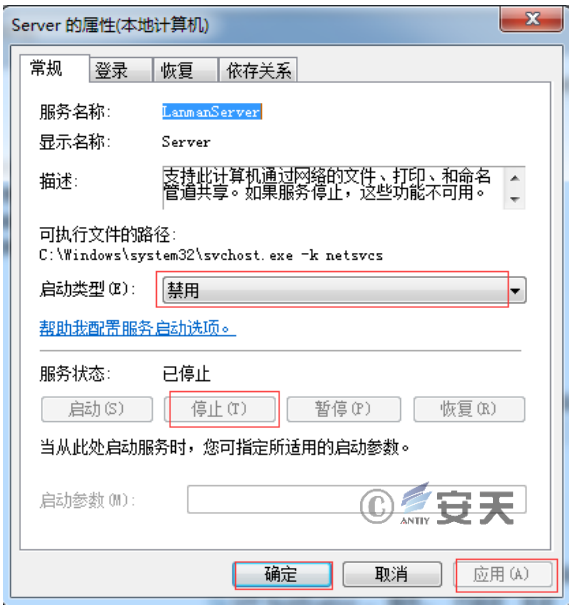
需要操作系统的 server 服务关闭，依次点击“开始”，“运行”，输入 services.msc，进入服务

管理控制台。

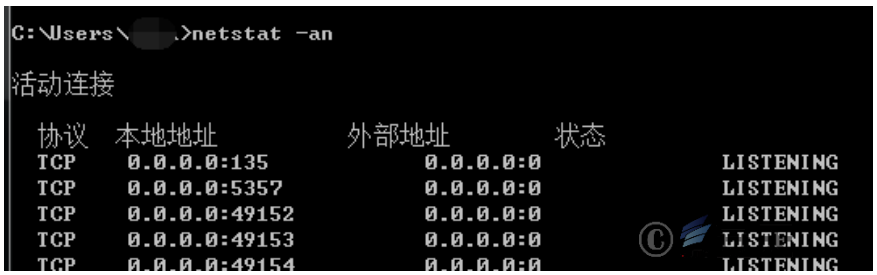


双击 Server，先停用，再选择禁用。

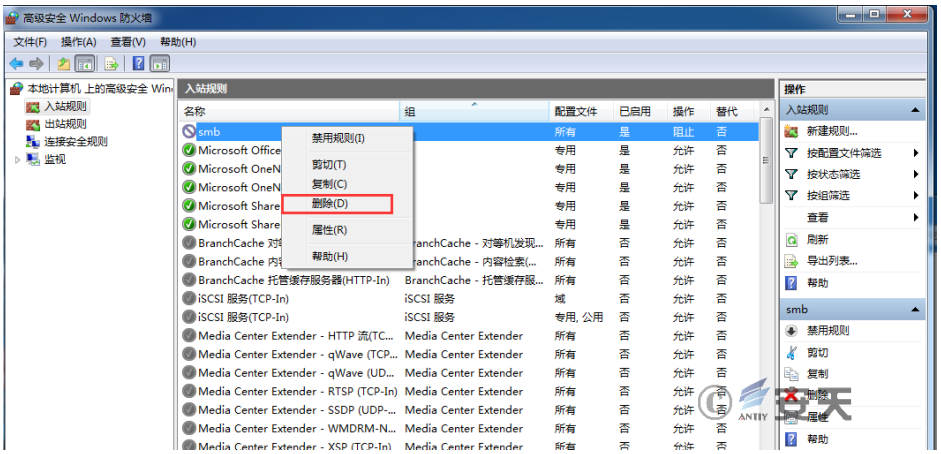




最后重启 win7。使用 netstat –an 查看 445 端口不存在了。



注：在系统更新完成后，如果业务需要使用 SMB 服务，将上面设置的防火墙入站规则删除即可。



附录一：关于安天

安天是专注于威胁检测防御技术的领导厂商。安天以提升用户应对网络空间威胁的核心能力、改善用户对威胁的认知为企业使命，依托自主先进的威胁检测引擎等系列核心技术和专家团队，为用户提供端点防护、流量监测、深度分析、威胁情报和态势感知等相关产品、解决方案与服务。

安天的监控预警能力覆盖全国、产品与服务辐射多个国家。安天将大数据分析、安全可视化等方面的技术与产品体系有效结合，以海量样本自动化分析平台延展分析师团队作业能力、缩短产品响应周期。安天结合多年积累的海量安全威胁知识库，综合应用大数据分析、安全可视化等方面经验，推出了可抵御各类已知和未知威胁的多样化解决方案。

全球超过一百家以上的著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的威胁检测引擎目前已为全球近十万台网络设备和网络安全设备、超过八亿部移动终端设备提供安全防护，其中安天移动检测引擎是全球首个获得 AV-TEST 年度奖项的中国产品，并在国际权威认证机构 AV-C 的 2015 年度移动安全产品测评中，成为全球唯一两次检出率均为 100%的产品。

安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续五届蝉联国家级网络安全应急服务支撑单位资质，亦是中国国家信息安全漏洞库六家首批一级支撑单位之一。

安天是中国应急响应体系中重要的企业节点，在红色代码 II、口令蠕虫、震网、破壳、沙虫、方程式、白象、魔窟等重大安全事件中，安天提供了先发预警、深度分析或系统的解决方案。

安天实验室更多信息请访问：	*http://www.antiy.com（中文）* *http://www.antiy.net（英文）*
安天企业安全公司更多信息请访问：	*http://www.antiy.cn*
安天移动安全公司（AVL TEAM）更多信息请访问：	*http://www.avlsec.com*