安天CVE-2017-11780漏洞免疫工具使用说明

# 一 概述

本工具为安天CERT响应CVE-2017-11780SMB远程代码执行漏洞(CNVD-2017-29681)紧急发布，提供禁用系统服务、设置ipsec本地组策略等功能，提供通过阻断SMB连接使CVE-2017-11780漏洞(CNVD-2017-29681)无法触发的临时缓解方案。

注意，请优先选择及时更新补丁并安装防护软件保证系统安全！安装补丁后即可无需免疫处理。

工具会阻断部分端口的连接，请在使用前确认是否会影响其他应用。

# 二 功能介绍

## 2.2设置组策略免疫

### 2.2.1常规型组策略设置

* 功能介绍  
  该策略适用于Windows Vista及之后系统，仅阻止445端口的连接，推荐Windows Vista及之后系统的用户优先使用。
* 使用说明  
  点击“设置免疫”，工具会自动关闭445端口，重启后设置生效。  
  点击“取消设置”，会重新开启445端口。

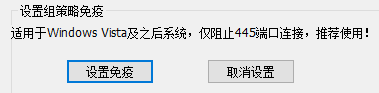


图2-1常规型策略界面

### 2.2.2增强型组策略设置

* 功能介绍  
  该策略为增强型策略，可以关闭135/137/138/139/445端口。
* 使用说明  
  点击“设置增强免疫”，工具会自动关闭135/137/138/139/445端口，重启后设置生效。  
  点击“取消设置”，会重新开启135/137/138/139/445端口。

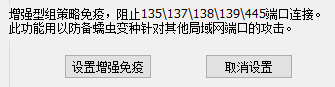


图2-2 增强型组策略免疫界面

### 2.2.3禁用服务免疫

* 功能介绍  
  适用于Windows XP系统，设置后会关闭部分系统服务，有可能影响其他系统功能。
* 使用说明  
  点击“设置免疫”，工具会自动关闭部分系统服务，重启后设置生效。  
  点击“取消设置”，会重新开启部分服务。

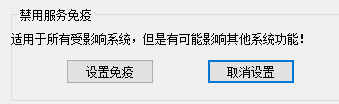


图2-3 禁用服务免疫功能截图

### 2.2.4官方补丁下载

* 功能介绍  
  可以链接到微软官网下载漏洞补丁。
* 使用说明  
  点击“官方补丁下载”，将会启动浏览器并访问微软官方网站，用户点击接受EULA后，即可通过网站下载适配的补丁程序。

**03.CVE-2017-11780.Windows.SMB.Remote.Code.Execution.Vulnerability-Microsoft.pdf文档中包含本漏洞升级补丁的下载地址。**  
注：漏洞补丁由微软官方提供，与工具无关。