漏洞具体情况

**一、漏洞概述**

漏洞公告显示，SMB 3.1.1协议中处理压缩消息时，对其中数据没有经过安全检查，直接使用会引发内存破坏漏洞，可能被攻击者利用远程执行任意代码。攻击者利用该漏洞无须权限即可实现远程代码执行，受黑客攻击的目标系统只需开机在线即可能被入侵。该漏洞的后果十分接近永恒之蓝系列，都利用Windows SMB漏洞远程攻击获取系统最高权限，WannaCry勒索蠕虫就是利用永恒之蓝系列漏洞攻击工具制造的大灾难。除了直接攻击SMB服务端造成RCE外，该漏洞的高危性在于对SMB客户端的攻击，攻击者可以构造特定的网页，压缩包，共享目录，OFFICE文档等多种方式触发漏洞进行攻击。

**二、影响范围**

漏洞不影响win7，漏洞影响Windows 10 1903之后的32位、64位Windows，包括家用版、专业版、企业版、教育版。具体列表如下：
Windows 10 Version 1903 for 32-bit Systems
Windows 10 Version 1903 for x64-based Systems
Windows 10 Version 1903 for ARM64-based Systems
Windows Server, Version 1903 (Server Core installation)
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 1909 for ARM64-based Systems
Windows Server, Version 1909 (Server Core installation)
**三、系统版本检测**

1、点击windows系统左下角徽标键（即“开始”键），打开“Windows系统”下的“命令提示符”窗口。


2、进入命令提示符窗口，输入winver命令，查看系统版本。





**四、漏洞修复**

方法1、下载SMB远程代码执行漏洞修复工具，进行漏洞检测和修复。下载地址：http://dlied6.qq.com/invc/QQPatch/QuickFix\_SMB0796.exe



方法2、直接运行Windows 更新，完成补丁的安装。

操作步骤：设置->更新和安全->Windows更新，点击“检查更新”。

注：补丁安装后，可使用SMB远程代码执行漏洞修复工具进行检测确认，修复成功如下图所示。



相关信息来源：

腾讯御见威胁情报中心