预警编号：YJ-2017013

恒安嘉新

关于 Windows Search 远程代码执行漏洞

安全预警通告

恒安嘉新（北京）科技股份公司

信息安全处

2017 年 06 月 14 日

1. 简介

Windows 搜索服务（WSS）是 windows 的一项默认启用的基本服务。允许用户在多个 Windows 服务和客户端之间进行搜索。当 Windows 搜索处理内存中的对象时，存在远程执行代码漏洞(CVE-2017-8543)。成功利用此漏洞的攻击者可以控制受影响的系统。

2. 利用原理

攻击者向 Windows Search 服务发送精心构造的 SMB 消息。从而利用此漏洞提升权限并控制计算机。此外，在企业场景中，未经身份验证的攻击者可以通过 SMB 服务连接远程触发漏洞，然后控制目标计算机。

3. 影响范围

桌面系统：Windows 10, 7, 8, 8.1, Vista, Xp 和 Windows RT 8.1

服务器系统：Windows Server 2016，2012，2008，2003

4. 修复建议

桌面系统 Windows 10, 7, 8.1 和 Windows RT 8.1；服务器系统：Windows Server 2016，2012，2008，可以通过 Windows Update 自动更新微软补丁的方式进行修复。

Windows 8, Vista, Xp 和 Windows Server 2003 可以通过选择对应版本然后手动更新补丁的方式进行更新。

（补丁下载地址参考）

https://support.microsoft.com/zh-cn/help/4025687/microsoft-security-advisory-4025685-guidance-for-older-platforms