预警编号：YJ-2017014

恒安嘉新

关于 LNK 文件（快捷方式）远程代码漏洞

安全预警通告

恒安嘉新（北京）科技股份公司

2017 年 06 月 14 日

1. 简介

lnk 文件是用于指向其他文件的一种文件。 这些文件通常称为快捷方式文件，通常它以快捷方式放在硬盘上，以方便使用者快速的调用。如果用户打开攻击者精心构造的恶意 LNK 文件，则会造成远程代码执行(CVE-2017-8464)。成功利用此漏洞的攻击者可以获得与本地用户相同的用户权限。

2. 利用原理

攻击者可以通过可移动驱动器（U 盘）或远程共享等方式将包含恶意 LNK 文件和与之相关的恶意二进制文件传播给用户。当用户通过 Windows 资源管理器或任何能够解析 LNK 文件的程序打开恶意的 LNK 文件时，与之关联的恶意二进制代码将在目标系统上执行

3. 影响范围

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

服务器系统：Windows Server 2016，2012，2008

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 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