关于加强防范“震网三代”及其他高危漏洞的情况通报

各单位：

近日，据技术支持单位通报，“震网三代”LNK 文件远程代码执行漏洞和 Windows 搜索远程命令执行漏洞需要紧急处置，对我国互联网安全构成一定的威胁。目前该漏洞可以用于穿透物理隔离网络，可以很容易地被黑客利用并组装成用于攻击基础设施、存放关键资料的核心隔离系统等的网络武器。该漏洞是一个微软 Windows 系统处理 LNK 文件过程中发生的远程代码执行漏洞。当存在漏洞的电脑被插上存在漏洞文件的 U 盘时，不需要任何额外操作，漏洞攻击程序就可以借此完全控制用户的电脑系统。该漏洞也可能籍由用户访问网络共享、从互联网下载、拷贝文件等操作被触发和利用攻击。为此，请各单位立即开展安全防范工作，具体情况通报如下：

一、“震网三代”及其他高危漏洞的基本情况

1.“震网三代”LNK 文件远程代码执行漏洞（文件远程代码执行漏洞）描述

物理隔离基础设施、核心网络通常需要使用 U 盘、移动硬盘等移动存储设备进行数据交换，当有权限物理接触被隔离系统的人员有意或无意（已经被入侵的情况下），将存在漏洞攻击文件设备插入被隔离系统，就会使得恶意程序感染并控制被隔离系统。

2.Windows 搜索远程命令执行漏洞（搜索远程命令执行漏洞）描述

当 Windows 搜索处理内存中的对象时，存在远程代码执行漏洞。成功利用此漏洞的攻击者可以控制受影响的系统。攻击者可以安装、查看、更改或删除数据，或者创建具有完全用户权限的新帐户。

为了利用该漏洞，攻击者向 Windows 搜索服务发送特定 SMB 消息。访问目标计算机的攻击者可以利用此漏洞提升权限并控制计算机。在企业场景中，一个未经身份验证的远程攻击者可以远程触发漏洞，通过 SMB 连接然后控制目标计算机。

二、漏洞影响范围

1.“震网三代”LNK 文件远程代码执行漏洞

该漏洞影响从 Win7 到最新的 Windows 10 操作系统，漏洞同样影响操作系统，但不影响 XP\2003 系统。具体受影响的操作系统列表如下：

Windows 7 (32/64 位)

Windows 8 (32/64 位)

Windows 8.1(32/64 位)

Windows 10 (32/64 位， RTM/TH2/RS1/RS2)

Windows Server 2008 (32/64/IA64)

Windows Server 2008 R2 (64/IA64)

Windows Server 2012

Windows Server 2012 R2

Windows Server 2016W

Windows Vista

2.Windows 搜索远程命令执行漏洞（搜索远程命令执行漏洞）

具体受影响的操作系统列表如下：

Windows Server 2016 (Core installation)

Windows Server 2016

Windows Server 2012 R2(Server Core installation)

Windows Server 2012 R2

Windows Server 2012 (Core installation)

Windows Server 2012

Windows Server 2008 R2 for x64-based Systems Service Pack 1

Windows 8.1

Windows 7

Windows 10

三、漏洞排查和防范措施建议

1.目前微软公司已经针对除了 Windows 8 系统外的操作提供了官方补丁，请到微软官方网站下载补丁并进行一键式修复。

2.对于目前无法及时更新补丁的主机，建议采用如下方式进行缓解:禁用 U 盘、网络共享及关闭 Webclient service、请管理员关注是否做好恢复准备、关闭 Windows Search 服务。

3.定期在不同的存储介质上备份信息系统业务和个人数据。

4.下载主流杀毒软件进行检测和查杀。

针对“震网三代”及其他高危漏洞，请各单位立即开展立即排查,安装杀毒软件，突出情况及时上报.

2017年6月14日