

# “震网三代”及其他高危漏洞

## 安全预警通告

第 2 次更新



360安全监测与响应中心

2017年06月14日

## 目录

<b>第 1 章 安全通告</b> .....	<b>3</b>
<b>第 2 章 漏洞信息</b> .....	<b>5</b>
2.1 漏洞描述.....	5
“震网三代”LNK 文件远程代码执行漏洞（cve-2017-8464） .....	5
Windows 搜索远程命令执行漏洞（cve-2017-8543） .....	5
2.2 风险等级.....	6
<b>第 3 章 处置建议</b> .....	<b>7</b>
3.1 确认影响范围 .....	7
“震网三代”LNK 文件远程代码执行漏洞（cve-2017-8464） .....	7
Windows 搜索远程命令执行漏洞（cve-2017-8543） .....	7
3.2 缓解措施.....	8
“震网三代”LNK 文件远程代码执行漏洞（cve-2017-8464） .....	8
Windows 搜索远程命令执行漏洞（cve-2017-8543） .....	9
3.3 根治手段.....	9
360 企业安全发布“震网三代”一键式漏洞修复工具 .....	9
“震网三代”LNK 文件远程代码执行漏洞（cve-2017-8464） .....	9
Windows 搜索远程命令执行漏洞（cve-2017-8543） .....	9
<b>第 4 章 参考文档</b> .....	<b>10</b>

# 第1章 安全通告

尊敬的客户：

本月的微软补丁今天发布，经过 360 安全专家研判确认以下两个漏洞需要紧急处置：“震网三代”LNK 文件远程代码执行漏洞（cve-2017-8464）和 Windows 搜索远程命令执行漏洞（cve-2017-8543）。

“震网三代”LNK 文件远程代码执行漏洞（cve-2017-8464）可以用于穿透物理隔离网络。微软 14 日凌晨发布的安全公告，称 CVE-2017-8464 被国家背景的网络攻击所使用，实施攻击。

该漏洞的原理同 2010 年破坏伊朗核设施的震网行动中所使用的、用于穿透核设施中隔离网络的 Windows 安全漏洞 CVE-2010-2568 非常相似。它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。该漏洞也可能藉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。

另一个漏洞，Windows 搜索远程代码执行漏洞的补丁，解决了在 Windows 操作系统中发现的 Windows 搜索服务（Windows Search Service）的一个远程代码执行漏洞（WSS：Windows 中允许用户跨多个 Windows 服务和客户机搜索的功能）

微软在同一天发布了 Windows XP 和 Windows Server 2003 等 Windows 不继续支持的版本的补丁，这个修改是为了避免上月发生的 WannaCry 蠕虫勒索事件的重现。

Window XP 的补丁更新可以在微软下载中心找到，但不会自动通过 Windows 推送。

360 安全监测与响应中心也将持续关注该事件进展，并第一时间为您更新该漏洞信息。

关于本次事件的进展，可以访问以下地址获取最新信息：

[http://b.360.cn/about/shownews/57?type=about\\_news](http://b.360.cn/about/shownews/57?type=about_news)

## 第2章 漏洞信息

### 2.1 漏洞描述

#### “震网三代” LNK 文件远程代码执行漏洞（cve-2017-8464）

一个常见的攻击场景是：物理隔离的基础设施、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的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。

在 2010 年，伊朗生产浓缩铀的核工厂的技术人员，将含有类似漏洞的 U 盘插入了控制核工厂工业控制系统的电脑，感染后的电脑继续攻击了离心机设备，导致核原料提炼失败，伊朗的核计划最终失败并可能造成了一定规模的核泄漏事件。

本次的漏洞 CVE-2017-8464 和 2010 年的漏洞的原理和能力几乎完全一致。据微软官方发布的消息，该漏洞已经被攻击者利用在真实世界的攻击中。但是此次微软并没有公开是哪个组织或公司向其报告的攻击事件，这一反常的行为很可能是由于攻击方来自具有国家背景的黑客组织，或者被攻击方是具有国家背景的组织或机构。

#### Windows 搜索远程命令执行漏洞（cve-2017-8543）

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

## 2.2 风险等级

360 安全监测与响应中心风险评级为：**危急**

## 第3章 处置建议

### 3.1 确认影响范围

#### “震网三代”LNK 文件远程代码执行漏洞（cve-2017-8464）

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 2016
- Windows Vista

#### Windows 搜索远程命令执行漏洞（cve-2017-8543）

具体受影响的操作系统列表如下：

- Windows Server 2016 (Server Core installation)
- Windows Server 2016
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 (Server Core installation)
- Windows Server 2012
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
- Windows Server 2008 R2 for x64-based Systems Service Pack 1

Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1

Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)

Windows Server 2008 for x64-based Systems Service Pack 2

Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)

Windows Server 2008 for 32-bit Systems Service Pack 2

Windows RT 8.1

Windows 8.1 for x64-based systems

Windows 8.1 for 32-bit systems

Windows 7 for x64-based Systems Service Pack 1

Windows 7 for 32-bit Systems Service Pack 1

Windows 10 Version 1703 for x64-based Systems

Windows 10 Version 1703 for 32-bit Systems

Windows 10 Version 1607 for x64-based Systems

Windows 10 Version 1607 for 32-bit Systems

Windows 10 Version 1511 for x64-based Systems

Windows 10 Version 1511 for 32-bit Systems

Windows 10 for x64-based Systems

Windows 10 for 32-bit Systems

Windows XP

Windows 2003

Windows Vista

## 3.2 缓解措施

对于无法及时更新补丁的主机，我们建议采用如下的方式进行缓解：

### “震网三代”LNK 文件远程代码执行漏洞（cve-2017-8464）

建议在服务器环境执行以下缓解措施：

禁用 U 盘、网络共享及关闭 Webclient service

请管理员关注是否有业务与上述服务相关并做好恢复准备。



## Windows 搜索远程命令执行漏洞（cve-2017-8543）

关闭 Windows Search 服务

### 3.3 根治手段

#### 360 企业安全发布“震网三代”一键式漏洞修复工具

360 企业安全集团天擎团队发布的“震网三代”漏洞补丁修复工具支持对 LNK 文件远程代码执行漏洞（CVE-2017-8464）和 Windows 搜索远程命令执行漏洞（CVE-2017-8543）进行一键式检测与修复。

下载地址：<http://b.360.cn/other/stuxnet3fixtool>

#### “震网三代”LNK 文件远程代码执行漏洞（cve-2017-8464）

目前微软已经针对除了 Windows 8 系统外的操作系统提供了官方补丁。

微软官方补丁下载地址：

<https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8464>

<https://support.microsoft.com/en-us/help/4025687/microsoft-security-advisory-4025685-guidance-for-older-platforms>

#### Windows 搜索远程命令执行漏洞（cve-2017-8543）

目前微软已经提供了官方补丁。

微软官方补丁下载地址：

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8543>

3

<https://support.microsoft.com/en-us/help/4025687/microsoft-security-advisory-4025685-guidance-for-older-platforms>

使用 360 天擎的用户，请稍后更新天擎补丁库，天擎将针对全网推送补丁。

## 第4章 参考文档

<https://threatpost.com/microsoft-patches-two-critical-vulnerabilities-under-attack/126239/>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8543>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8464>