

信息安全漏洞周报

2017 年 06 月 12 日-2017 年 06 月 18 日

2017 年第 25 期

本周漏洞态势研判情况

本周信息安全漏洞威胁整体评价级别为**高**。

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 296 个，其中高危漏洞 104 个、中危漏洞 177 个、低危漏洞 15 个。漏洞平均分为 6.17。本周收录的漏洞中，涉及 0day 漏洞 77 个（占 26%），其中互联网上出现与 Windows 操作系统和 Linux 内核相关的重要安全更新，影响面较广。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 1342 个，与上周（1067）环比增长 26%。

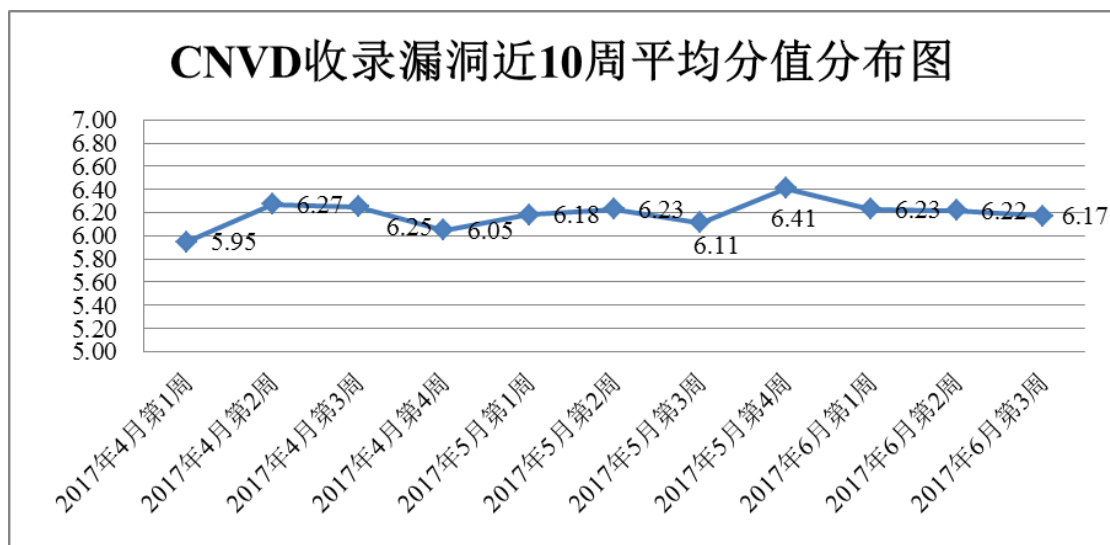


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 21 家成员单位、企业用户及个人用户报送了本周收录的全部 296 个漏洞。报送情况如表 1 所示。其中，启明星辰、恒安嘉新、安天实验室、绿盟科技、天融信等单位报送数量较多。360 网神、漏洞盒子、南京联成科技发展有限公司、广州软云计算机科技有限公司、福建六壬网安股份有限公司、中新网络信息安全股份有限公司、

江苏君立华域安全测评有限公司、广州神月信息技术有限公司、清远职业技术学院、江西安服信息产业有限公司、杭州朔方信息技术有限公司、河北网信智安信息技术有限公司、广州圣辉信息技术有限公司、山石网科通信技术有限公司、安徽新华博信息技术股份有限公司、长沙天融信网络安全技术有限公司、北京安码科技有限公司及其他个人白帽子向 CNVD 提交了 1342 个以事件型漏洞为主的原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
360 网神	375	375
启明星辰	199	15
恒安嘉新	190	0
漏洞盒子	174	174
安天实验室	151	1
天融信	123	0
东软	97	0
H3C	84	0
华为技术有限公司	76	0
中国电信集团系统集成有限责任公司	62	0
绿盟科技	54	0
阿里云计算有限公司	51	0
杭州安恒信息技术有限公司	48	0
厦门服云信息科技有限公司	33	0
深圳市深信服电子科技有限公司	6	6
深圳市腾讯计算机系统有限公司（玄武实验室）	5	5
知道创宇	5	5
北京数字观星科技有限公司	5	0

北京无声信息技术有限公司	5	0
南京铨迅信息技术股份有限公司	1	1
西安四叶草信息技术有限公司	1	1
南京联成科技发展有限公司	48	48
广州软云计算科技有限公司	22	22
福建六壬网安股份有限公司	22	22
中新网络信息安全股份有限公司	19	19
江苏君立华域安全测评有限公司	13	13
广州神月信息安全技术有限公司	5	5
清远职业技术学院	5	5
江西安服信息产业有限公司	4	4
杭州朔方信息技术有限公司	3	3
河北网信智安信息技术有限公司	3	3
广州圣辉信息技术有限公司	3	3
山石网科通信技术有限公司	3	3
安徽新华博信息技术股份有限公司	2	2
长沙天融信网络安全技术有限公司	1	1
北京安码科技有限公司	1	1
CNCERT 山西分中心	25	25
CNCERT 浙江分中心	13	13
CNCERT 宁夏分中心	7	7
CNCERT 广东分中心	3	3

CNCERT 吉林分中心	2	2
个人报送者	555	555
报送总计	2504	1342
录入总计	296（去重）	1342

表 1 漏洞报送情况统计表

本周漏洞按类型和厂商统计

本周，CNVD 收录了 296 个漏洞。其中应用程序漏洞 212 个，web 应用漏洞 34 个，操作系统漏洞 26 个，网络设备漏洞 19 个，安全产品漏洞 5 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	212
web 应用漏洞	34
操作系统漏洞	26
网络设备漏洞	19
安全产品漏洞	5

表 2 漏洞按影响类型统计表

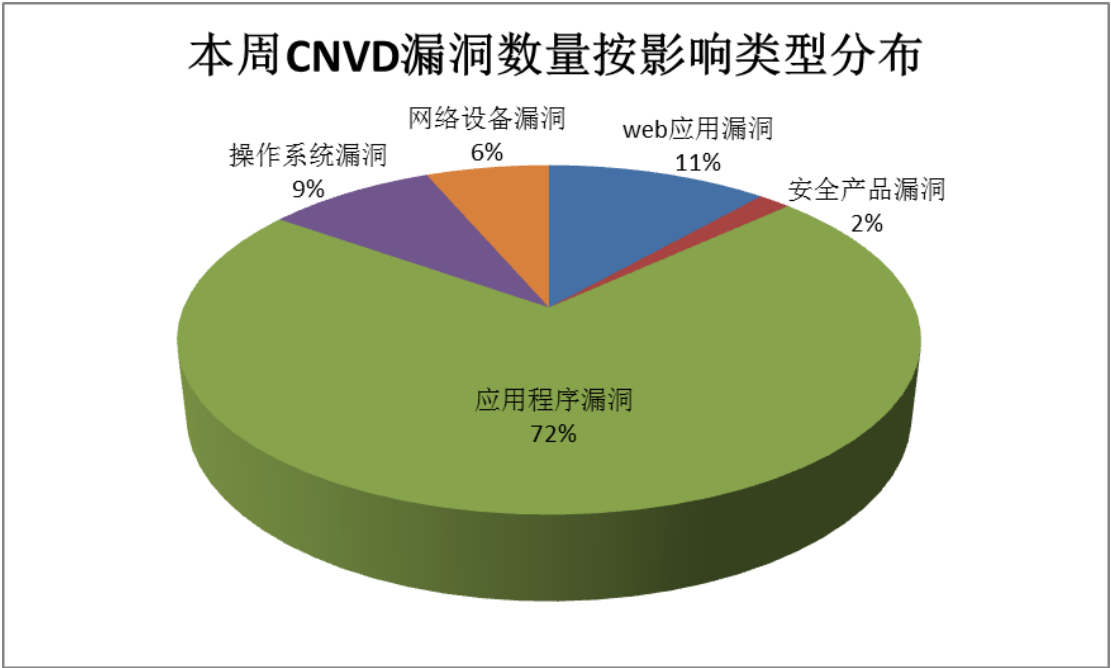


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Schneider Electric、IBM 等多家厂商的产品，部分漏洞数量按厂商统计如表 3 所示。

序号	厂商（产品）	漏洞数量	所占比例
----	--------	------	------

1	Google	41	14%
2	Schneider Electric	23	8%
3	IBM	16	5%
4	Microsoft	11	4%
5	Cisco	8	3%
6	Peplink	7	2%
7	Pivotal	7	2%
8	MarkLogic	6	2%
9	Huawei	5	2%
10	其他	172	58%

表 3 漏洞产品涉及厂商分布统计表

本周行业漏洞收录情况

本周，CNVD 收录了 18 个电信行业漏洞，46 个移动互联网行业漏洞（如下图所示）。其中，“Cisco Prime Data Center Network Manager 默认帐户验证绕过漏洞、多款 Peplink Balance 产品存在目录遍历漏洞、多款 Peplink Balance 产品存在 SQL 注入漏洞、多款 Moxa 产品存在暴力破解漏洞、Open vSwitch 整数溢出漏洞、Google Android Qualcomm TrustZone 安全绕过漏洞、Google Android Qualcomm TrustZone 双重释放漏洞、Google Android Qualcomm TrustZone 竞争条件漏洞”等的综合评级为“高危”。相关厂商已经发布了上述漏洞的修补程序，请参照 CNVD 相关行业漏洞库链接。

电信行业漏洞链接：<http://telecom.cnvd.org.cn/>

移动互联网行业漏洞链接：<http://mi.cnvd.org.cn/>

工控系统行业漏洞链接：<http://ics.cnvd.org.cn/>

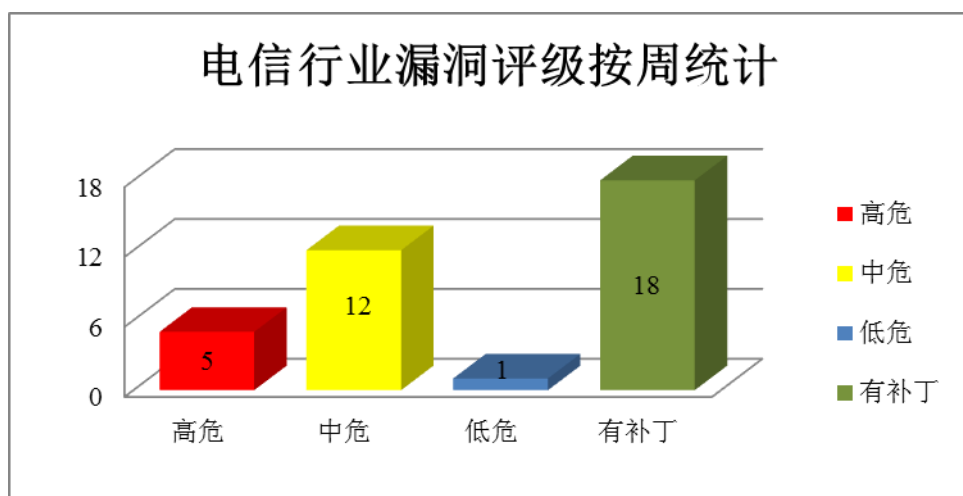


图 3 电信行业漏洞统计

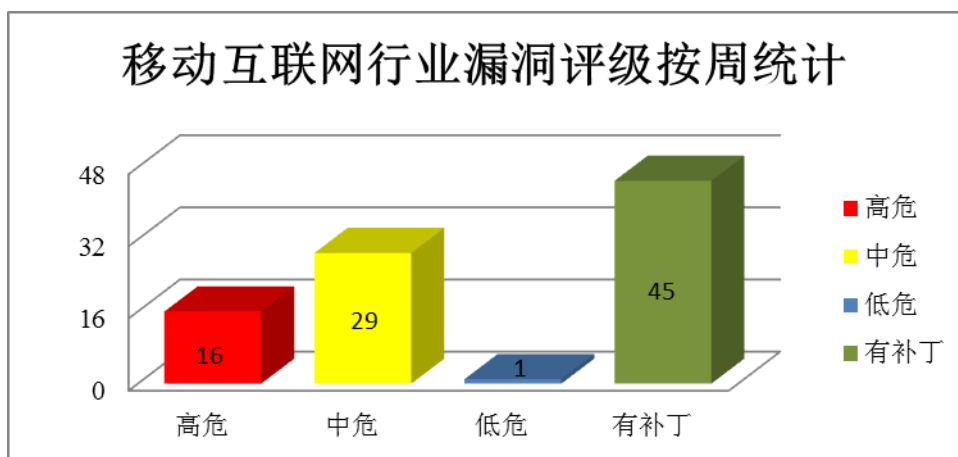


图 4 移动互联网行业漏洞统计

本周重要漏洞安全告警

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、Microsoft 产品安全漏洞

Microsoft Windows 是美国微软（Microsoft）公司发布的一系列操作系统，Microsoft Forefront 是应用在其中的一套面向企业的服务器安全特性解决方案。Microsoft Defender 是一款应用在其中的杀毒软件。Windows Search 服务（WSS）是 windows 的一项默认启用的基本服务。本周，上述产品被披露存在远程代码执行和拒绝服务漏洞，攻击者可利用漏洞执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Microsoft Malware Protection 引擎拒绝服务漏洞（CNVD-2017-09499、CNVD-2017-09500、CNVD-2017-09502）、Microsoft Malware Protection 引擎远程代码执行漏洞（CNVD-2017-09503、CNVD-2017-09504）、Microsoft Windows LNK 文件远程代码执行漏洞、Microsoft Windows OLE 远程代码执行漏洞（CNVD-2017-09716）、Microsoft Windows Search 远程代码执行漏洞。其中，“Microsoft Windows LNK 文件远程代码执行漏洞、Microsoft Windows OLE 远程代码执行漏洞（CNVD-2017-09716）、Microsoft Windows Search 远程代码执行漏洞”的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09499>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09500>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09502>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09503>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09504>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09382>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09716>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09381>

2、Schneider Electric 产品安全漏洞

U.motion Builder 是法国施耐德电气（Schneider Electric）公司的一款生成器产品。本周，该产品被披露存在远程代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Schneider Electric U.motion Builder editobject 远程代码执行漏洞、Schneider Electric U.motion Builder loadtemplate 远程代码执行漏洞、Schneider Electric U.motion Builder nfcserver 远程代码执行漏洞、Schneider Electric U.motion Builder SOAP 远程代码执行漏洞、Schneider Electric U.motion Builder track_getdata 远程代码执行漏洞、Schneider Electric U.motion Builder xmlserver 远程代码执行漏洞、Schneider Electric U.motion Builder 硬编码远程代码执行漏洞、Schneider Electric U.motion Builder 远程代码执行漏洞。上述漏洞的综合评级为“高危”。CNVD 提醒广大用户随时关注厂商主页，以获取最新版本。

参考链接：<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09473>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09463>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09470>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09477>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09471>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09472>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09462>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09469>

3、Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司开发的一款 Web 浏览器。Blink 是一套浏览器排版引擎。print preview 是一个 qrp 文件转换工具。FFmpeg 是一套可录制、转换以及流化音视频的完整解决方案。Android 是一套以 Linux 为基础的开源操作系统。Media 是其中的一个用于多媒体开发框架。本周，上述产品被披露存在远程代码执行和内存错误引用漏洞，攻击者可利用漏洞执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Google Android Media framework 远程代码执行漏洞、Google Android Media framework 远程代码执行漏洞（CNVD-2017-09306、CNVD-2017-09307、CNVD-2017-09308、CNVD-2017-09309、CNVD-2017-09310）、Google Chrome FFmpeg 内存错误引用漏洞、Google Chrome print preview 内存错误引用漏洞。上述漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09311>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09306>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09307>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09308>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09309>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09310>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09218>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09214>

4、Cisco 产品安全漏洞

Cisco Aironet Access Points 是美国思科 (Cisco) 公司的一套无线访问接入点设备。Cisco AnyConnect Secure Mobility Client 是下一代 VPN 客户端。Cisco Prime Collaboration 是综合性视频及声音服务保障及管理系统。Cisco Prime Data Center Network Manager 是网络管理应用。Cisco TelePresence 是思科网真解决方案。Cisco Firepower System Software 是一款下一代防火墙产品 (NGFW)。本周, 上述产品被披露存在多个漏洞, 攻击者可利用漏洞绕过安全限制、提升权限、执行任意命令或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括: Cisco Aironet Access Points 任意代码执行漏洞、Cisco AnyConnect Secure Mobility Client 本地权限提升漏洞、Cisco Elastic Services Controller 默认凭据安全绕过漏洞、Cisco Prime Collaboration Provisioning 目录遍历漏洞 (CNVD-2017-09962)、Cisco Prime Data Center Network Manager 默认帐户验证绕过漏洞、Cisco Prime Data Center Network Manager 远程代码执行漏洞、Cisco TelePresence 端点拒绝服务漏洞、Cisco Firepower System Software 远程安全绕过漏洞。除“Cisco Firepower System Software 远程安全绕过漏洞”外其余漏洞的综合评级为“高危”。CNVD 提醒用户及时下载补丁更新, 避免引发漏洞相关的网络安全事件。

参考链接: <http://www.cnvd.org.cn/flaw/show/CNVD-2017-09957>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09961>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09963>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09962>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09960>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09959>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09958>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-09795>

5、ISC BIND 9 权限提升漏洞

ISC BIND 是美国 Internet Systems Consortium (ISC) 公司所维护的一套实现了 DNS 协议的开源软件。本周, ISC 被披露存在权限提升漏洞, 攻击者可利用漏洞在权限进程的上下文中执行任意代码。目前, 互联网上已经出现了针对该漏洞的攻击代码, 厂商尚未发布漏洞修补程序。CNVD 提醒广大用户随时关注厂商主页, 以获取最新版本。

参考链接: <http://www.cnvd.org.cn/flaw/show/CNVD-2017-09365>

更多高危漏洞如表 4 所示, 详细信息可根据 CNVD 编号, 在 CNVD 官网进行查询。

参考链接:<http://www.cnvd.org.cn/ flaw/ list. html>

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2017-09376	libxml2 不完全修复栈缓冲区溢出漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞: https://bugzilla.redhat.com/show_bug.cgi?id=1408305
CNVD-2017-09525	多款 Peplink Balance 产品存在 SQL 注入漏洞	高	目前厂商已发布升级补丁以修复漏洞, 详情请关注厂商主页: https://www.peplink.com/
CNVD-2017-09520	多款 Peplink Balance 产品存在目录遍历漏洞	高	目前厂商已发布升级补丁以修复漏洞, 详情请关注厂商主页: https://www.peplink.com/
CNVD-2017-09580	Phoenix Contact mGuard 拒绝服务漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞: https://ics-cert.us-cert.gov/advisories/ICS-17-131-01
CNVD-2017-09579	Zimbra Collaboration Suite (ZCS) 目录遍历漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞: https://wiki.zimbra.com/wiki/Security_Center
CNVD-2017-09592	多款 Puppet 产品 YAML 反序列化远程代码执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞: https://bugzilla.redhat.com/show_bug.cgi?id=1452651
CNVD-2017-09862	InvoicePlane 存在多个漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题, 补丁获取链接: https://community.invoiceplane.com/t/topic/4258
CNVD-2017-09871	Oniguruma 'mbc_enc_len()' 函数越边界写入漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题, 补丁获取链接: https://github.com/kkos/oniguruma/issues/55
CNVD-2017-09880	多款 Moxa 产品存在暴力破解漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题, 详情请关注厂商主页: http://www.moxa.com/
CNVD-2017-09893	Bubblewrap 安全绕过漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞: https://bugzilla.redhat.com/show_bug.cgi?id=1411811

表 4 部分重要高危漏洞列表

小结: 本周, Microsoft 被披露存在远程代码执行和拒绝服务漏洞, 攻击者可利用漏

洞执行任意代码或发起拒绝服务攻击。此外，Schneider Electric、Google、Cisco 等多款产品被披露存在多个漏洞，攻击者利用漏洞可绕过安全限制、提升权限、执行任意命令或发起拒绝服务攻击等。另外，ISC 被披露存在权限提升漏洞，攻击者可利用漏洞在权限进程的上下文中执行任意代码。建议相关用户随时关注上述厂商主页，及时获取修复补丁或解决方案。

本周漏洞要闻速递

1. 潜伏长达 11 年之久的 Linux 内核漏洞“Phoenix Talon”曝光

启明星辰 ADLab 提交了四个存在于 Linux 内核的远程漏洞，并命名为“Phoenix Talon”；其中一个漏洞为严重(Critical)级别，另外三个为高危(High)。漏洞可导致远程 DOS，在符合一定利用条件下可导致远程代码执行，包括传输层的 TCP、DCCP、SCTP 以及网络层的 IPv4 和 IPv6 协议均受影响。

参考链接：<http://www.freebuf.com/articles/system/137572.html>

2. Windows 修复两个严重远程代码执行漏洞（CVE-2017-8543/8464）

微软的 Patch Tuesday 更新发布了多达 95 个针对 Windows、Office、Skype、IE 和 Edge 浏览器的补丁。其中，最危险的两个漏洞存在于 Windows Search 功能和处理 LNK 文件的过程中。黑客可以在存在 Windows Search 服务(WSS)的 Windows 系统中执行远程代码。另一个漏洞存在于 LNK 文件中的，攻击者可以生成特制的快捷方式从而执行远程代码执行。

参考链接：<http://www.freebuf.com/articles/system/137283.html>

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

关于 CNCERT

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，为非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心协调机构。

作为国家级应急中心，CNCERT 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82990999