

信息安全漏洞周报

2017 年 09 月 11 日-2017 年 09 月 17 日

2017 年第 38 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 450 个，其中高危漏洞 178 个、中危漏洞 249 个、低危漏洞 23 个。漏洞平均分为 6.42。本周收录的漏洞中，涉及 0day 漏洞 101 个（占 22%），其中互联网上出现“Joomla! Event Registration Pro Calendar 组件 SQL 注入漏洞、Supervisor 远程命令执行漏洞”等零日代码攻击漏洞。此外，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 1029 个，与上周（1326 个）环比减少 22%。

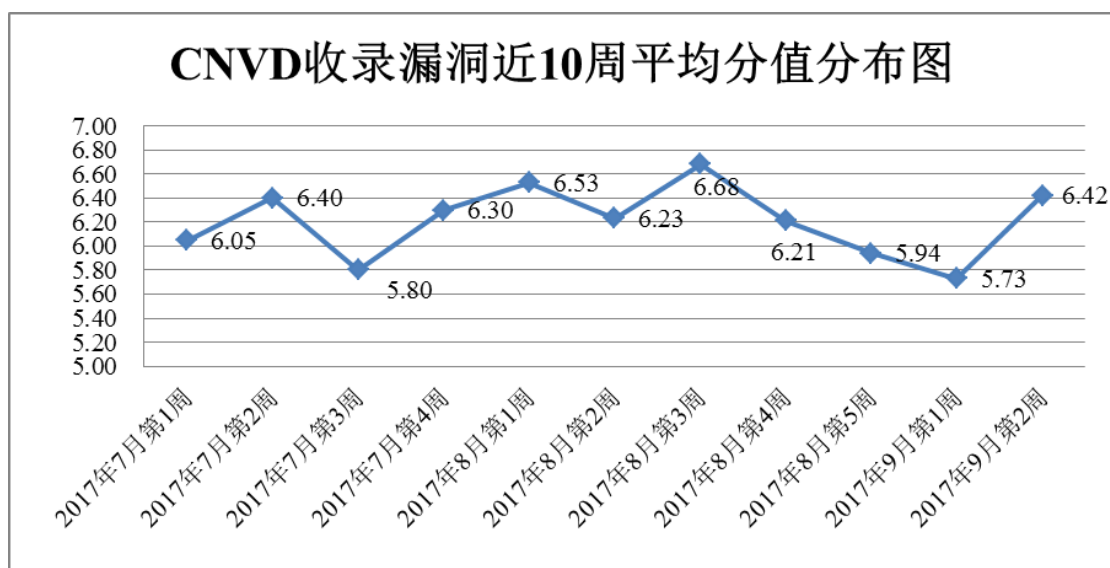


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 15 家成员单位、企业用户及个人用户报送了本周收录的全部 450 个漏洞。报送情况如表 1 所示。其中，恒安嘉新、H3C、安天实验室、华为技术有限公司、天融信等单位报送数量较多。四川虹微技术有限公司（子午攻防实验室）、深圳市鼎安天下

信息科技有限公司、中新网络信息安全股份有限公司、邹平九零冰讯网络科技有限公司、上海犇众信息技术有限公司、广州软云计算机科技有限公司及其他个人白帽子向 CNVD 提交了 1029 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
恒安嘉新	284	0
H3C	234	0
安天实验室	222	0
华为技术有限公司	211	6
网神	195	195
天融信	169	2
漏洞盒子	91	91
启明星辰	83	3
北京数字观星科技有限公司	53	0
绿盟科技	51	0
中国电信集团系统集成有限责任公司	51	11
杭州安恒信息技术有限公司	24	0
东软	5	5
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
四川虹微技术有限公司 (子午攻防实验室)	101	101
深圳市鼎安天下信息科技有限公司	9	9
中新网络信息安全股份有限公司	1	1
邹平九零冰讯网络科技有限公司	1	1
上海犇众信息技术有限公司	1	1

广州软云计算科技有限公司	1	1
CNCERT 广东分中心	3	3
CNCERT 宁夏分中心	1	1
个人	596	596
报送总计	2389	1029
录入总计	450（去重）	1029

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 450 个漏洞。其中应用程序漏洞 236 个，web 应用漏洞 116 个，操作系统漏洞 61 个，网络设备漏洞 22 个，安全产品漏洞 12 个，数据库漏洞 3 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	236
web 应用漏洞	116
操作系统漏洞	61
网络设备漏洞	22
安全产品漏洞	12
数据库漏洞	3

表 2 漏洞按影响类型统计表

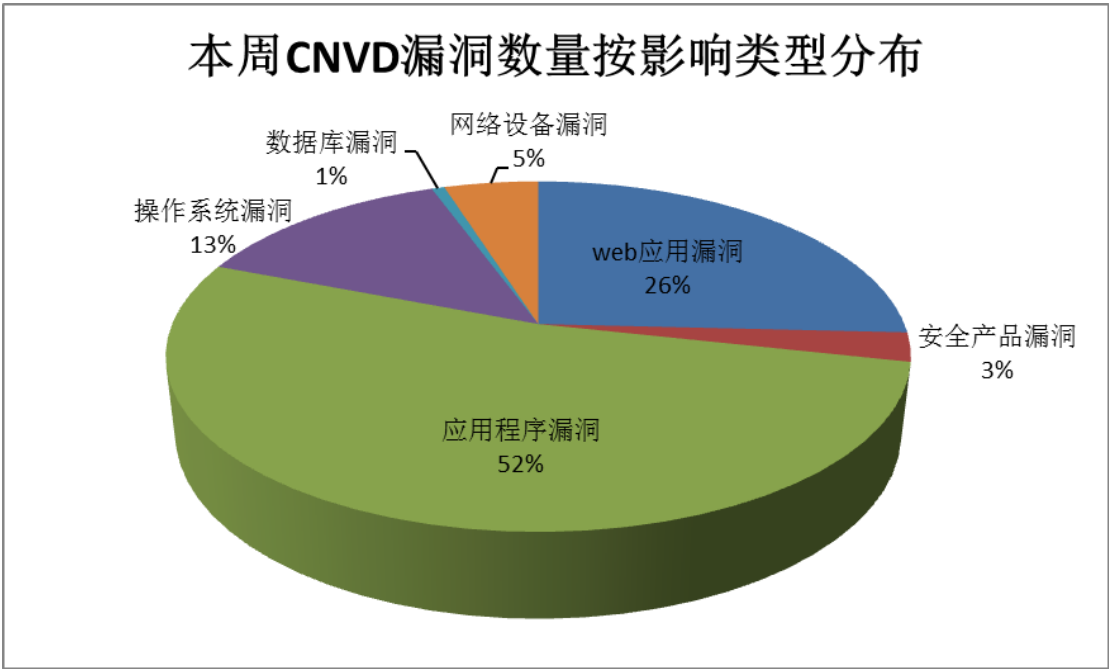


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Oracle、Adobe 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	57	13%
2	Oracle	38	8%
3	Adobe	27	6%
4	Cisco	16	4%
5	WordPress	12	3%
6	IBM	12	3%
7	Joomla!	8	2%
8	NVIDIA	8	2%
9	Aruba Networks	6	1%
10	其他	266	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 15 个电信行业漏洞，105 个移动互联网行业漏洞，4 个工控系统行业漏洞（如下图所示）。其中，“mySCADA myPRO 权限提升漏洞、Google Android Qualcomm 组件缓冲区溢出漏洞（CNVD-2017-26643）、PostgreSQL 安全绕过漏洞（CNVD-2017-26577）、Google Android Qualcomm 组件内存访问漏洞、Android BNEP 远程执行代码漏洞”等漏洞的综合评级为“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/>

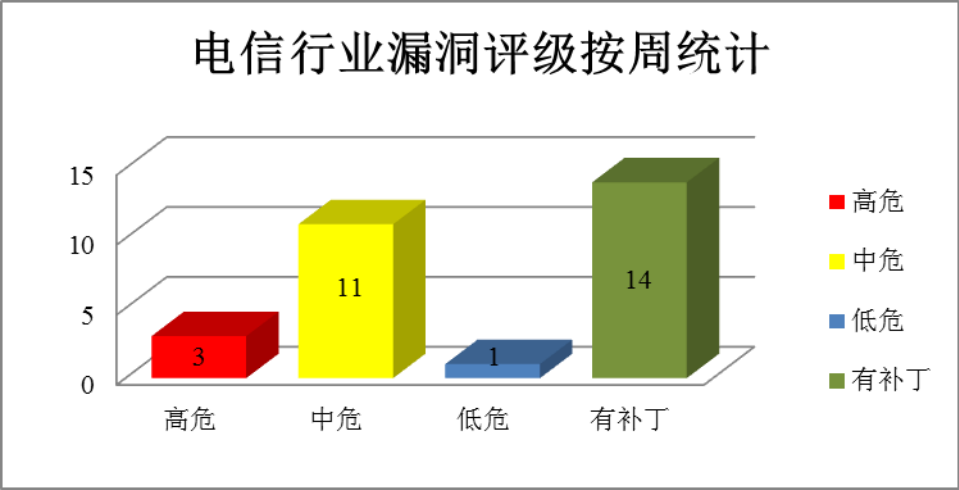


图 3 电信行业漏洞统计

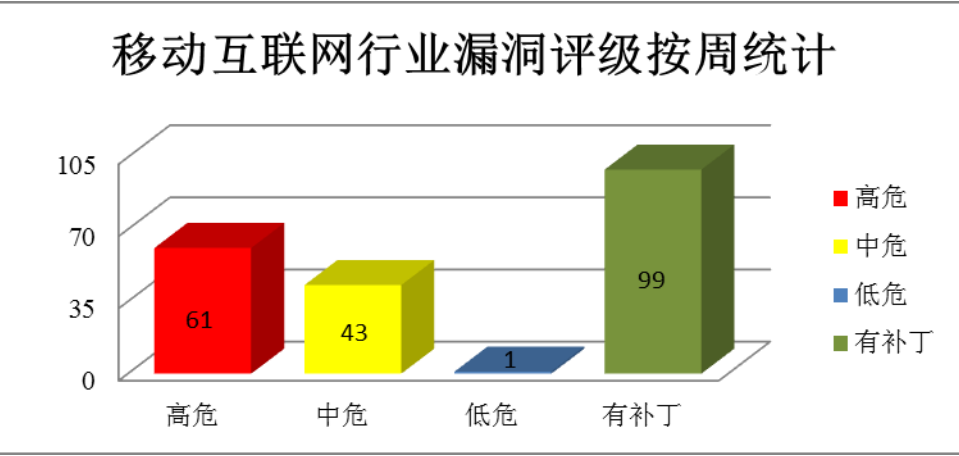


图 4 移动互联网行业漏洞统计

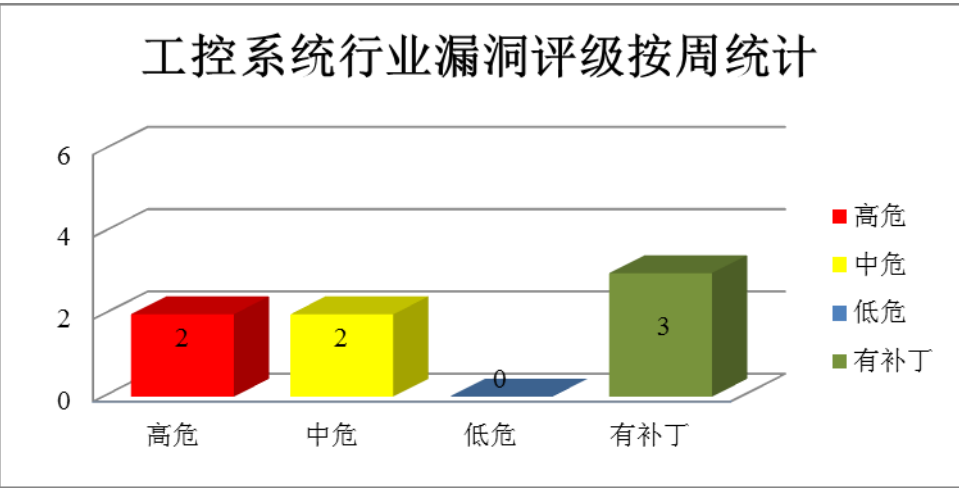


图 5 工控系统行业漏洞统计

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、蓝牙(Bluetooth)协议存在多个漏洞

蓝牙(Bluetooth)协议存在的 8 个安全漏洞。由于漏洞涉及到基础协议，影响到 Android、iOS、Windows 以及 Linux 系统设备甚至使用短距离无线通信技术的物联网设备。攻击者可通过蓝牙(Bluetooth)协议远程不经过任何传统网络介质发起攻击。

CNVD 收录的相关漏洞包括：Android The Bluetooth Pineapple 中间人攻击漏洞、Android BNEP 远程执行代码漏洞、Android PAN 远程执行代码漏洞、Android SDP 服务器信息泄露漏洞、Apple Bluetooth LEAP and Apple TV 堆缓冲区溢出漏洞、Linux BlueZ 缓冲区溢出漏洞、Windows The Bluetooth Pineapple 中间人攻击漏洞、Linux BlueZ SDP 服务器信息泄露漏洞。除“Windows The Bluetooth Pineapple 中间人攻击漏洞、Linux BlueZ SDP 服务器信息泄露漏洞”外，其余漏洞的综合评级为“高危”。目前，厂商已经发布了除“Apple Bluetooth LEAP and Apple TV 堆缓冲区溢出漏洞、Linux BlueZ 缓冲区溢出漏洞”以外漏洞的修补程序。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-2017-26765>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-26762>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-26763>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-26761>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-26764>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-26759>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-26766>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-26760>

2、Google 产品安全漏洞

Android 是美国谷歌公司和开放手持设备联盟共同开发的一套以 Linux 为基础的开源操作系统。Qualcomm closed-source components 是其中的一个美国高通公司开发的闭源组件。本周，上述产品被披露存在缓冲区溢出漏洞，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 Qualcomm 组件缓冲区溢出漏洞（CNVD-2017-26628、CNVD-2017-26629、CNVD-2017-26630、CNVD-2017-26631、CNVD-2017-26632、CNVD-2017-26633、CNVD-2017-26634、CNVD-2017-26639）。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-2017-26628>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-26629>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-26630>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-26631>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-26632>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-26633>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-26634>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-26639>

3、Adobe 产品安全漏洞

Adobe Reader/Acrobat 是一款流行的处理 PDF 文件的应用程序。本周，该产品被披露存在堆缓冲区溢出和远程代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Acrobat/Reader 堆缓冲区溢出漏洞（CNVD-2017-26614、CNVD-2017-26615、CNVD-2017-26616）、Adobe Acrobat 和 Reader 远程代码执行漏洞（CNVD-2017-26553、CNVD-2017-26555、CNVD-2017-26557、CNVD-2017-26558、CNVD-2017-26572）。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-2017-26614>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-26615>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-26616>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-26553>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-26555>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-26557>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-26558>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-26572>

4、NVIDIA 产品安全漏洞

NVIDIA Windows GPU Display Driver 是一套专用于 Windows 的图形处理器(GPU)显卡驱动程序。本周，该产品被披露存在拒绝服务和权限提升漏洞，攻击者可利用漏洞发起拒绝服务攻击或提升权限。

CNVD 收录的相关漏洞包括：NVIDIA Windows GPU Display Driver 拒绝服务漏洞（CNVD-2017-26296、CNVD-2017-26297）、NVIDIA Windows GPU Display Driver 权限提升漏洞（CNVD-2017-26295、CNVD-2017-26298、CNVD-2017-26299、CNVD-2017-26300、CNVD-2017-26301、CNVD-2017-26302）。除“NVIDIA Windows GPU Display Driver 权限提升漏洞（CNVD-2017-26295）”外，其余漏洞的综合评级为“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-2017-26296>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-26297>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-26295>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-26298>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-26299>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-26300>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-26301>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-26302>

5、Siemens 300/400 系列 PLC 远程控制漏洞

可编程控制器(即 PLC)是一款新型工业自动控制装置。Siemens 的中型 PLC S7-300 和大型 PLC S7-400 产品可以组成 MPI、PROFIBUS 和工业以太网等。本周, Siemens 被披露存在远程控制漏洞, 攻击者可以通过 Siemens PLC 通过 102 端口进行 TCP 通信, 该脚本通过向 PLC 的 102 端口发送特定的报文可实现远程控制 PLC 的启停。目前, 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-2017-26804>

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.htm>

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2017-26160	Unit4 Polska TETA Web 会话固定漏洞	高	厂商已发布了漏洞修复程序, 请及时关注更新: http://www.unit4.com/pl
CNVD-2017-26163	Supervisor 远程命令执行漏洞	高	厂商已发布漏洞修复程序, 请及时关注更新: https://github.com/Supervisor/supervisor/issues/964
CNVD-2017-26161	Razer Synapse rzpnk.sys 驱动程序权限提升漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞: https://www.razerzone.com/
CNVD-2017-26273	UltraISO 栈缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序, 请及时关注更新: http://www.ezbsystems.com/ultraiso/history.htm
CNVD-2017-26351	SAP TREX 代码注入漏洞	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.sap.com/index.html
CNVD-2017-26356	Avira Antivirus 远程代码执行漏洞	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.avira.com/
CNVD-2017-26426	mySCADA myPRO 权限提升漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞: https://www.myscada.org/download/
CNVD-2017-26600	CompuLab Intense PC 输入验证漏洞	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: http://www.compulab.com/

CNVD-2017-26767	WebKit 远程代码执行漏洞 (CNVD-2017-26767)	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://webkit.org/
CNVD-2017-26929	CalAmp LMU-3030 Devices 身份验证绕过漏洞	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： http://www.calamp.com/

表 4 部分重要高危漏洞列表

小结：本周，蓝牙(Bluetooth)协议存在的 8 个安全漏洞。漏洞影响到 Android、iOS、Windows 以及 Linux 系统设备甚至使用短距离无线通信技术的物联网设备。攻击者可通过蓝牙(Bluetooth)协议远程不经过任何传统网络介质发起攻击。此外，Adobe、Google、NVIDIA 多款产品被披露存在多个漏洞，攻击者可利用漏洞提升权限、执行任意代码或发起拒绝服务攻击等。另外，Siemens 被披露存在远程控制漏洞，攻击者可以通过 Siemens PLC 通过 102 端口进行 TCP 通信，该脚本通过向 PLC 的 102 端口发送特定的报文可实现远程控制 PLC 的启停。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. 蓝牙(Bluetooth)协议存在多个漏洞

最近研究人员发现蓝牙协议中有 8 个 0-day 漏洞，其中有 3 个被列为严重级别。这些漏洞可能会影响 53 亿智能设备，Android、iOS、Windows、Linux 系统的设备以及 IoT 设备等只要使用了蓝牙技术，就有可能中招。黑客可以利用这些漏洞发起远程攻击，不需要任何用户交互就能接管设备、传播恶意程序甚至进行中间人攻击，接入设备的网络并获取设备的关键数据。

参考链接：<http://www.freebuf.com/news/147577.html>

2. .NET 0day 漏洞被用来传播 FinFisher 病毒

微软在本月安全更新中修补的漏洞之一的一个 0day 漏洞被黑客用来传播 FinFisher 恶意软件，目标针对俄语用户。该漏洞由 FireEye 的研究人员向微软报告，漏洞编号 CVE-2017-8759，它影响的是 .NET 框架中的 SOAP WSDL (Web 服务描述语言) 解析器。攻击者可以利用漏洞远程执行代码，让目标用户打开特制的文档或应用程序。

参考链接：<http://www.freebuf.com/news/147593.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