国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2016 年 04 月 18 日-2016 年 04 月 24 日　　2016 年第 17 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**中**。

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 193 个，其中高危漏洞 61 个、中危漏洞 119 个、低危漏洞 13 个。漏洞平均分值为 5.94 分。本周收录的漏洞中，涉及 0day 漏洞 25 个（占 21%）。其中互联网上出现“iScriptsEasyCreate 远程代码执行漏洞、WordPress WP User Frontend 插件无限制文件上传漏洞”等零日代码攻击漏洞，请使用相关产品的用户注意加强防范。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 869 个，与上周（758 个）环比增长 15%。

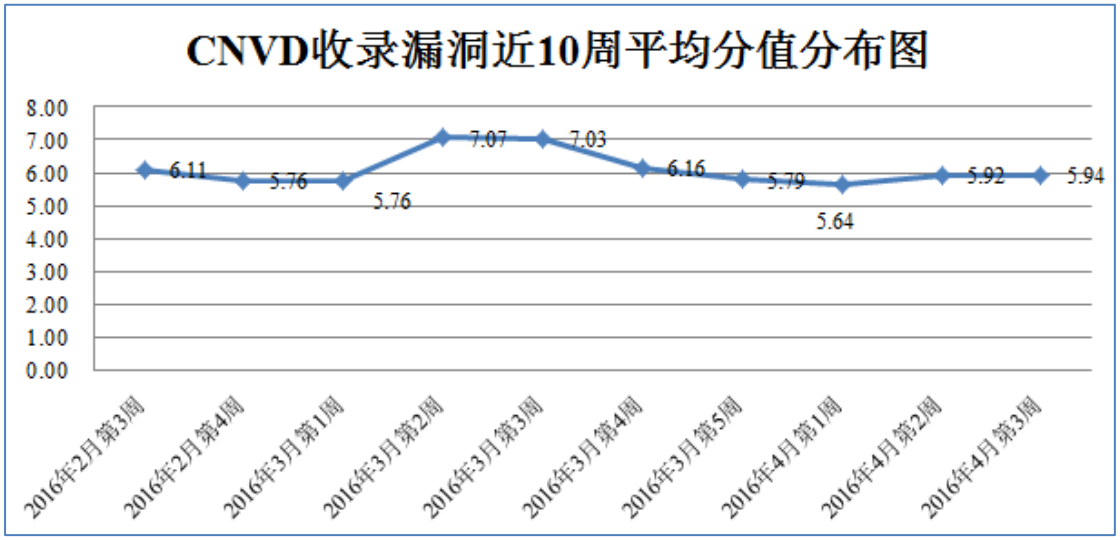

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 8 家成员单位、合作伙伴及个人报送了本周收录的全部 193 个漏洞。报送情况如表 1 所示。其中，安天实验室、启明星辰、天融信等单位报送数量较多。补天平

台、乌云、漏洞盒子、腾讯电脑管家、北京匡恩网络科技有限责任公司、High-Tech Bridge Security Research Lab 及白帽子向 CNVD 提交了 869 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
奇虎(补天平台)	249	249
安天实验室	203	0
启明星辰	202	1
天融信	160	0
杭州安恒信息技术有限公司	111	0
恒安嘉新	48	3
H3C	6	0
东软	4	0
乌云	471	471
漏洞盒子	95	95
腾讯电脑管家	8	8
北京匡恩网络科技有限责任公司	1	1
High-Tech Bridge Security Research Lab	1	1
CNCERT 福建分中心	3	3
CNCERT 陕西分中心	3	3
CNCERT 江西分中心	2	2
CNCERT 上海分中心	1	1
CNCERT 甘肃分中心	1	1
个人	30	30
报送总计	1599	869
录入总计	193（去重）	869

表 1 成员单位上报漏洞统计表

本周漏洞按类型和厂商统计

本周，CNVD 收录了 193 个漏洞。其中应用程序漏洞 114 个，Web 应用漏洞 14 个，操作系统漏洞 12 个，网络设备漏洞 11 个，安全产品漏洞 9 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	144
web 应用漏洞	14
操作系统漏洞	12
网络设备漏洞	11
数据库漏洞	9
安全产品漏洞	3

表 2 漏洞按影响类型统计表

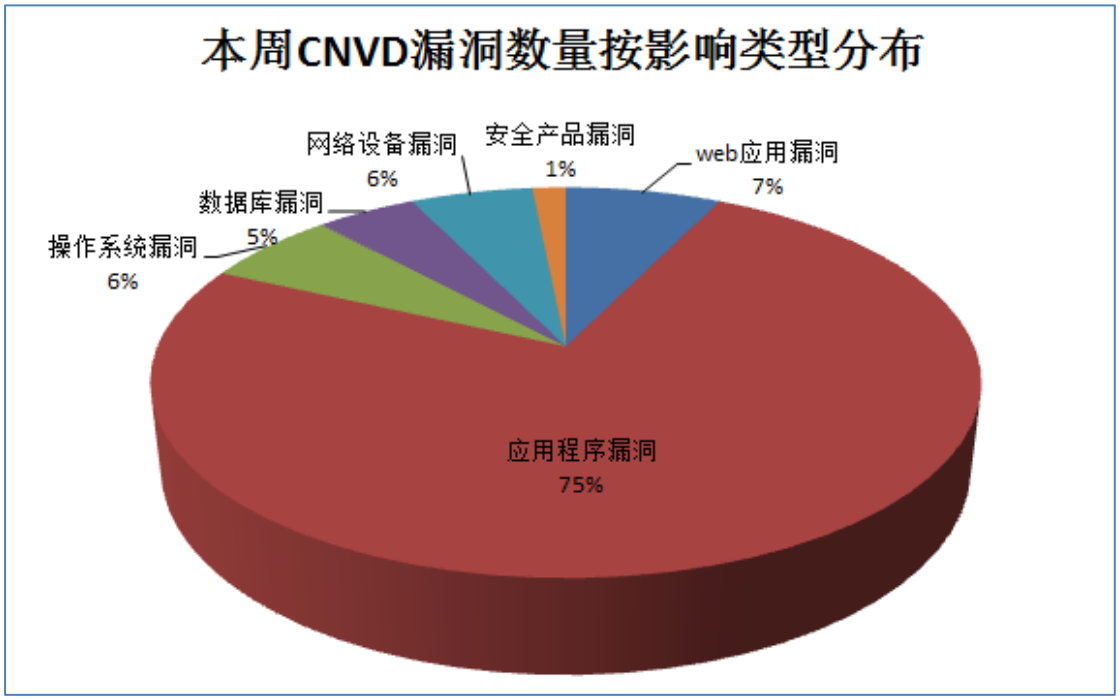

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、Microsoft、Juniper Networks 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	Oracle	23	12%
2	Microsoft	10	5%
3	Juniper Networks	10	5%
4	Google	9	5%

5	IBM	8	4%
6	Cisco	7	4%
7	Samba	7	4%
8	Silicon Graphics, Inc.	7	4%
9	WordPress	6	3%
10	其他	106	54%

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 14 个电信行业漏洞、6 个移动互联网漏洞、9 个工控系统行业漏洞（如下图所示）。其中，“Juniper Networks ScreenOS 安全绕过漏洞、Samsung KNOX 存在未明漏洞、EcavaIntegraXor 信息泄露漏洞（CNVD-2016-02341）、多款 Honeywell Uniformance Process History Database 产品缓冲区溢出漏洞、EcavaIntegraXor 远程代码执行漏洞”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/

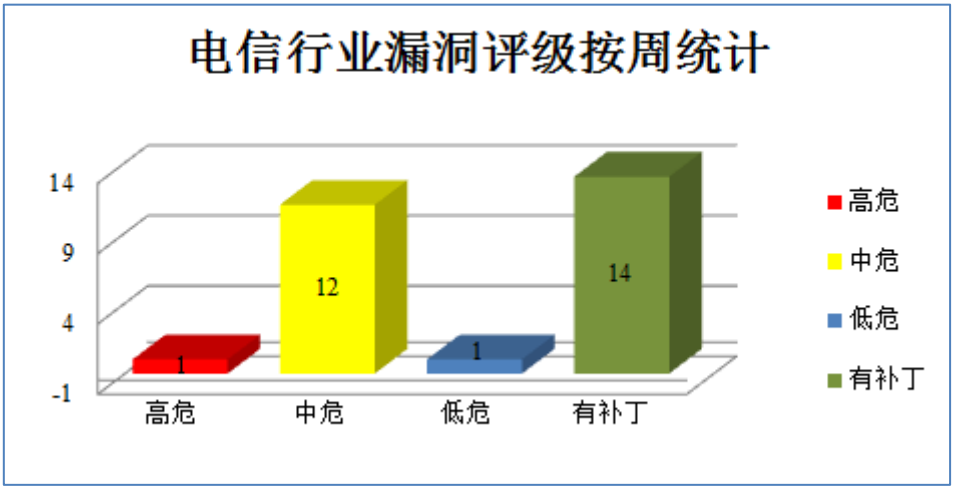

图 3 电信行业漏洞统计

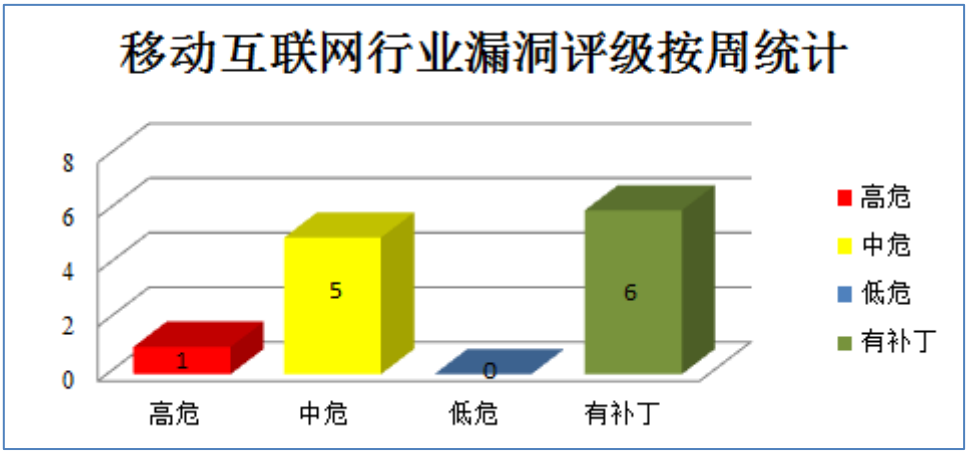

图 4 移动互联网行业漏洞统计

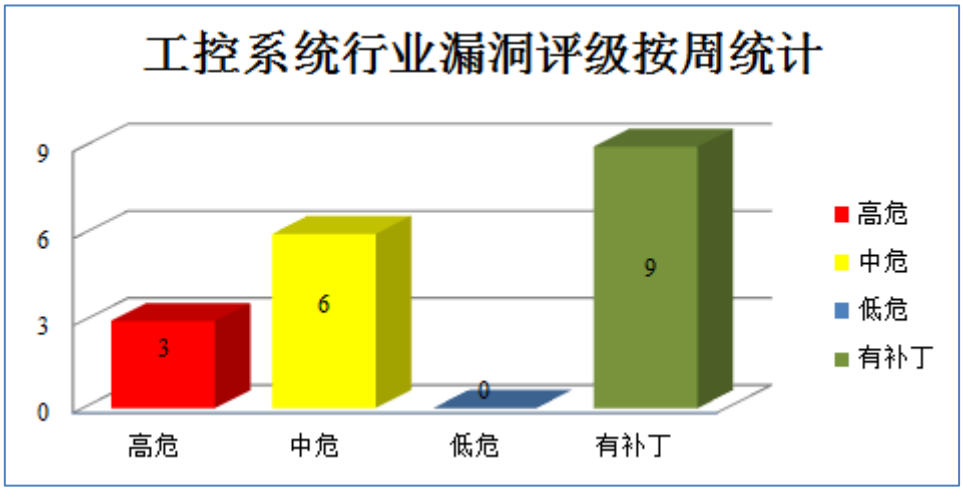

图 5 工控系统行业漏洞统计

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、 Oracle 产品安全漏洞

4 月 19 日，Oracle 发布了 2016 年 4 月份的安全更新，修复了其多款产品存在的 136 个安全漏洞。受影响的产品包括 Oracle 数据库（5 个）、中间件产品 Fusion Middleware（22 个）；供应链套装软件 Oracle Supply Chain Products Suite（6 个）电子商务套装软件 OracleE-Business Suite（7 个）、企业管理器网格控制产品 Oracle Enterprise Manager Grid Control（2 个）、OracleSiebel 托管型 CRM 软件（2 个）；PeopleSoft 产品（15 个）、Berkeley DB（5 个）、Virtualization（4 个）、Financial Services Software（4 个）、Retail Applications（3 个）、Communications Applications（1 个）、Health Sciences Applications（1 个）、JDEdwards 产品（1 个）；Java SE（9 个）、Oracle Sun 系统产品（18 个）和 MySQL 数据库（31 个）。本次安全更新提供了针对 44 个高危漏洞的补丁，有 9

0 个漏洞可被远程利用。

CNVD 收录的相关漏洞包括：Oracle Java SE 2D 子组件存在未明漏洞、Oracle Java SE 和 Java SE Embedded Serialization 子组件存在未明漏洞、Oracle Berkeley DB DataStore 组件存在未明漏洞、Oracle Java SE Deployment 子组件存在未明漏洞（CNVD-2016-02423、CNVD-2016-02435、CNVD-2016-02436、CNVD-2016-02437、CNVD-2016-02438）等。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/webinfo/show/3833

2、 Google 产品安全漏洞

Google Chrome 是由 Google 开发的一款 Web 浏览工具。本周，该产品被披露存在多个安全漏洞，允许攻击者利用该漏洞获取敏感信息、执行任意代码和发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Google Chrome download 操作绕过安全限制漏洞、Google Chrome media 拒绝服务漏洞、Google Chrome V8 LoadBuffer 拒绝服务漏洞、Google Chrome Pdfium JPEG2000 信息泄露漏洞、Google Chrome Extensions 子系统绕过安全限制漏洞、Google Chrome 跨站脚本漏洞（CNVD-2016-02450）、Google Chrome 任意代码执行漏洞（CNVD-2016-02445）、Google Chrome 内存错误引用漏洞（CNVD-2016-02446）等。其中，“Google Chrome 任意代码执行漏洞（CNVD-2016-02445）、Google Chrome 内存错误引用漏洞（CNVD-2016-02446）”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-2016-02452

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02448

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02449

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02451

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02444

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02450

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02445

http://www.cnvd.org.cn/flaw/show/CNVD-2016-02446

3、 IBM 产品安全漏洞

IBM Bluemix Liberty for Java 是美国 IBM 公司的一套基于 IBM Bluemix（平台即服务，PaaS）产品的动态应用程序服务器运行时环境。IBM Tivoli Directory Server 是一套使用了轻量级目录访问协议（LDAP）的企业身份管理软件。IBM Financial Transaction Managerfor Corporate Payment Services 是一款金融事务管理器产品，它主要用于监控、跟踪和报告金融支付和交易。本周，上述产品被披露存在多个安全漏洞，允许攻

击者利用漏洞获取敏感信息、进行跨站脚本攻击或执行任意代码等。

CNVD 收录的相关漏洞包括：IBM Bluemix Liberty for Java 安全绕过漏洞、IBM Tivoli Directory Server 和 Security Directory Server 命令执行漏洞、IBM Financial Transaction Manager for Corporate Payment Services 跨站脚本漏洞、IBM Financial Transaction Manager for Corporate Payment Services 信息泄露漏洞、IBM Financial Transaction Manager for Corporate Payment Services 跨站请求伪造漏洞、IBM Financial Transaction Manager for Corporate Payment Services 点击劫持漏洞、IBM Financial Transaction Manager for Corporate Payment Services 本地信息泄露漏洞、IBM Financial Transaction Manager for Corporate Payment Services 任意代码执行漏洞。其中，“IBM Financial Transaction Manager for Corporate Payment Services 任意代码执行漏洞”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-2016-02372
http://www.cnvd.org.cn/flaw/show/CNVD-2016-02324
http://www.cnvd.org.cn/flaw/show/CNVD-2016-02269
http://www.cnvd.org.cn/flaw/show/CNVD-2016-02270
http://www.cnvd.org.cn/flaw/show/CNVD-2016-02271
http://www.cnvd.org.cn/flaw/show/CNVD-2016-02272
http://www.cnvd.org.cn/flaw/show/CNVD-2016-02273
http://www.cnvd.org.cn/flaw/show/CNVD-2016-02274

4、HP 产品安全漏洞

HP Data Protector 是美国惠普（HP）公司的一套统一数据保护解决方案。该方案通过利用智能数据管理方法，保护跨所有物理和虚拟环境的数据，提供三方（应用源、备用服务器和目标设备）重复数据删除功能。本周，该产品被披露存在远程代码执行漏洞，允许攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：HP Data Protector 远程代码执行漏洞（CNVD-2016-02364、CNVD-2016-02365、CNVD-2016-02366、CNVD-2016-02367、CNVD-2016-02368）。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-2016-02364
http://www.cnvd.org.cn/flaw/show/CNVD-2016-02365
http://www.cnvd.org.cn/flaw/show/CNVD-2016-02366
http://www.cnvd.org.cn/flaw/show/CNVD-2016-02367
http://www.cnvd.org.cn/flaw/show/CNVD-2016-02368

5、Silicon Graphics LibTifftiffcp 工具拒绝服务漏洞

Silicon Graphics LibTiff 是一个读写 TIFF 文件的库。该库包含一些处理 TIFF 文件的命令行工具。tiffcrop tool 是一套用于转换 TIFF 文件的工具。本周，Silicon Graphics LibTiff 被披露存在拒绝服务漏洞，允许攻击者利用漏洞发起拒绝服务攻击或执行任意命令。目前，厂商尚未发布该漏洞的修补程序。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-2016-02267

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-2016-02255	ESET NOD32 Archive support 模块堆缓冲区溢出漏洞	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.eset.com/
CNVD-2016-02249	多款 Honeywell Uniformance Process History Database 产品缓冲区溢出漏洞	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：https://www.honeywellprocess.com
CNVD-2016-02277	Micro Focus Service Desk HQL 注入漏洞	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://www.novell.com/support/kb/doc.php?id=7017430
CNVD-2016-02284	Microsoft Internet Explorer 内存破坏漏洞（CNVD-2016-02284）	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：http://technet.microsoft.com/security/bulletin/MS16-037
CNVD-2016-02282	Microsoft Internet Explorer 内存破坏漏洞（CNVD-2016-02282）	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：http://technet.microsoft.com/security/bulletin/MS16-037
CNVD-2016-02281	Microsoft Windows Win32k 权限提升漏洞（CNVD-2016-02281）	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：http://technet.microsoft.com/security/bulletin/MS16-039
CNVD-2016-02280	Microsoft Internet Explorer 内存破坏漏洞（CNVD-2016-02280）	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：http://technet.microsoft.com/security/bulletin/MS16-037
CNVD-2016-02279	Microsoft Windows Win32k 权限提升漏洞（CNVD-2016-02279）	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：http://technet.microsoft.com/security/bulletin/MS16-039
CNVD-201	EcavaIntegraXor 远程代码执行漏	高	目前厂商已经发布了升级补丁以修

6-02275	洞		复此安全问题，补丁获取链接：http://www.integraxor.com/download/beta.msi?5.0.4522.2
CNVD-2016-02278	Micro Focus Service Desk 路径遍历漏洞	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://www.novell.com/support/kb/doc.php?id=7017428

表 4 部分重要高危漏洞列表

小结：4 月 19 日，Oracle 发布了 2016 年 4 月份的安全更新，修复了其多款产品存在的 136 个安全漏洞。本次安全更新提供了针对 44 个高危漏洞的补丁，有 90 个漏洞可被远程利用。此外，Google、IBM、HP 等多款产品被披露存在多个安全漏洞，攻击者利用漏洞可执行任意代码、获取敏感信息、进行跨站脚本攻击或发起拒绝服务攻击等。另外，Silicon Graphics LibTiff 被披露存在一个高危漏洞，允许攻击者利用漏洞发起拒绝服务攻击或执行任意命令。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. 新型跨平台的键盘记录恶意软件 PWOBot 曝光

最近，安全研究人员发现了一款具有潜在威胁的跨平台恶意软件家族—PWOBot。该恶意软件自身可以实现非常丰富的功能，包括下载和运行文件，执行 Python 代码，记录按键信息，再生一个 HTTP 服务器以及通过受害人的 CPU 和 GPU 挖掘比特币等。且 PWOBot 可以攻击多种平台，包括 Windows，Linux，以及 OS X 等。该恶意软件是基于 Python 编辑的，根据 Palo Alto Networks 的研究表明，截至目前，该恶意软件正大规模在波兰的整个 Windows 操作系统蔓延。然而，利用平台间的切换能力，该恶意软件很有可能实现在全球范围内的蔓延、运行。

参考链接：http://www.freebuf.com/news/102450.html

2. 苹果不再为 Windows 版的 QuickTime 提供安全更新

根据苹果官方发表，他们将不再为 Windows 版本的 QuickTime 提供安全更新。这意味着他们在前不久放弃了 Windows 版本的 QuickTime。目前卸载这种易攻击的产品已经刻不容缓，专家们最近又在 QuickTime 上发现了两个远程代码执行漏洞。这两个都是可以被黑客远程执行代码的堆损坏漏洞。而且进行的攻击方式也极其简单，只要受害者访问了一个恶意制作的网站或文件就可以进行攻击。

参考链接：http://www.freebuf.com/news/101975.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