国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2015 年 09 月 28 日-2015 年 10 月 11 日　　**2015 年第 40、41 期**

本周漏洞基本情况

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 176 个，其中高危漏洞 58 个、中危漏洞 97 个、低危漏洞 21 个。上述漏洞中，可利用来实施远程攻击的漏洞有 159 个。本周收录的漏洞中，已有 155 个漏洞由厂商提供了修补方案，建议用户及时下载补丁更新程序，避免遭受网络攻击。其中互联网上出现“Boxoft WAV to MP3 Converter 缓冲区溢出漏洞”、“Cyberoam CR500iNG-XP SQL 注入漏洞” 等零日代码攻击，请使用相关产品的用户注意加强防范。

成员单位报送漏洞统计

本周，共 5 家成员单位、合作伙伴及个人报送了本周收录的全部 176 个漏洞。报送情况如表 1 所示。其中，奇虎(补天平台)、安天实验室、启明星辰、天融信等单位报送数量较多。此外，乌云、漏洞盒子、High-Tech Bridge Security Research 及白帽子向 CNVD 提交了 889 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)	364	364
安天实验室	267	0
启明星辰	202	0
天融信	187	0
绿盟科技	162	0
乌云	482	482

漏洞盒子	38	38
High-Tech Bridge Security Research	1	1
CNCERT 甘肃分中心	4	0
CNCERT 宁夏分中心	2	0
个人	4	4
报送总计	1713	889
录入总计	176（去重）	889

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Mozilla、Adobe、IBM 等多家厂商的产品，部分漏洞数量按厂商统计如表 2 所示。

序号	厂商（产品）	漏洞数量	所占比例
1	Mozilla	28	16%
2	Adobe	23	13%
3	IBM	21	12%
4	Apple	15	9%
5	Cisco	9	5%
6	Drupal	5	3%
7	FireEye	4	2%
8	McAfee	3	2%
9	Apache	3	2%
10	其他	65	36%

表 2 漏洞产品涉及厂商分布统计表

漏洞按影响类型统计

本周，CNVD 收录了 176 个漏洞。其中应用程序漏洞 127 个，操作系统漏洞 19 个，Web 应用漏洞 12 个，网络设备漏洞 9 个，安全产品漏洞 9 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	127
操作系统漏洞	19
Web 应用漏洞	12

网络设备漏洞	9
安全产品漏洞	9

表 3 漏洞按影响类型统计表

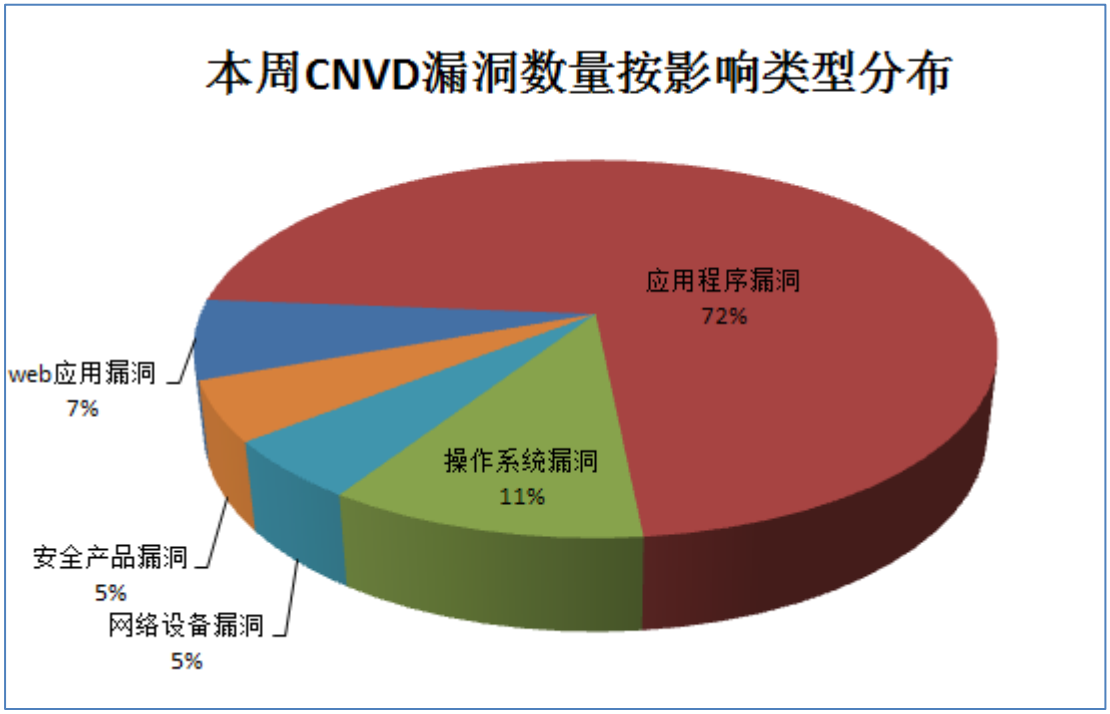

图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 15 个电信行业漏洞、12 个移动互联网行业漏洞、6 个工系统行业漏洞（如下图表所示）。其中，“Huawei eSpace U1900 Series Switches 拒绝服务漏洞、Cisco IOS/IOS XE IPv6 监听拒绝服务漏洞、Cisco IOS/IOS XE IPv6 监听拒绝服务漏洞（CNVD-2015-06345）、Cisco IOS/IOS XE SSHv2 身体验证绕过漏洞、Cisco IOS XE 网络地址转换拒绝服务漏洞”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。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2015-06257	Cisco ASR 9000 IOS DHCPv6 服务器拒绝服务漏洞	中	是
电信	CNVD-2015-06258	Cisco IOS 和 IOS XE 拒绝服务漏洞	中	是
电信	CNVD-2015-06266	Securifi Almond 中间人攻击漏洞	中	否
电信	CNVD-2015-06331	Huawei eSpace U1900 Series Switches 拒绝服务漏洞	高	是
电信	CNVD-2015-06344	Cisco IOS/IOS XE IPv6 监听拒绝服务漏洞	高	是
电信	CNVD-2015-06345	Cisco IOS/IOS XE IPv6 监听拒绝服务漏	高	是

		洞（CNVD-2015-06345）		
电信	CNVD-2015-06343	Cisco IOS/IOS XE SSHv2 身体验证绕过漏洞	高	是
电信	CNVD-2015-06342	Cisco IOS XE 网络地址转换拒绝服务漏洞	高	是
电信	CNVD-2015-06364	IBM WebSphere eXtreme Scale 访问权限绕过漏洞	低	是
电信	CNVD-2015-06362	IBM WebSphere eXtreme Scale 证书暴力破解漏洞	中	是
电信	CNVD-2015-06360	IBM WebSphere eXtreme Scale 信息泄露漏洞	低	是
电信	CNVD-2015-06358	IBM WebSphere eXtreme Scale 跨站脚本漏洞	低	是
电信	CNVD-2015-06356	IBM WebSphere eXtreme Scale 安全绕过漏洞	低	是
电信	CNVD-2015-06366	IBM WebSphere eXtreme Scale 应答注入漏洞	低	是
电信	CNVD-2015-06396	IBM WebSphere eXtreme Scale 跨站请求伪造漏洞	低	是
移动互联网	CNVD-2015-06241	Apple iOS Siri 信息泄露漏洞	低	是
移动互联网	CNVD-2015-06242	Apple iOS CFNetwork HTTPProtocol 组件信息泄露漏洞	中	是
移动互联网	CNVD-2015-06250	Newphoria Reversi 应用程序存在漏洞	中	是
移动互联网	CNVD-2015-06251	Newphoria Koritore 应用程序存在全漏洞	中	是
移动互联网	CNVD-2015-06252	Newphoria MEGAPHONE MUSIC 应用程序存在漏洞	中	是
移动互联网	CNVD-2015-06263	Apple iOS 同源策略绕过漏洞	中	是
移动互联网	CNVD-2015-06262	Apple iOS 同源策略绕过漏洞（CNVD-2015-06262）	中	是
移动互联网	CNVD-2015-06267	Newphoria Photon 应用程序身份验证绕过漏洞	中	否
移动互联网	CNVD-2015-06268	Newphoria Auction Camera 应用程序身份验证绕过漏洞	中	否
移动互联网	CNVD-2015-06269	Newphoria applican framework 身份验证绕过漏洞	中	否
移动互联网	CNVD-2015-06363	MoboTap Dolphin Browser for Android 任意文件写入漏洞	高	否
移动互联网	CNVD-2015-06398	Google Android 锁屏绕过漏洞	中	是
工控系统	CNVD-2015-06243	Wind River VxWorks 整数溢出漏洞	中	否
工控系统	CNVD-2015-06341	IBC Solar ServeMaster 源码漏洞	中	是
工控系统	CNVD-2015-06340	IBC Solar ServeMaster 纯文本密码漏洞	中	是
工控系统	CNVD-2015-06339	IBC Solar ServeMaster 跨站脚本漏洞	中	是
工控系统	CNVD-2015-06338	Resource Data Management 跨站请求伪造	中	是

		漏洞		
工控系统	CNVD-2015-06337	Resource Data Management 权限提升漏洞	中	是

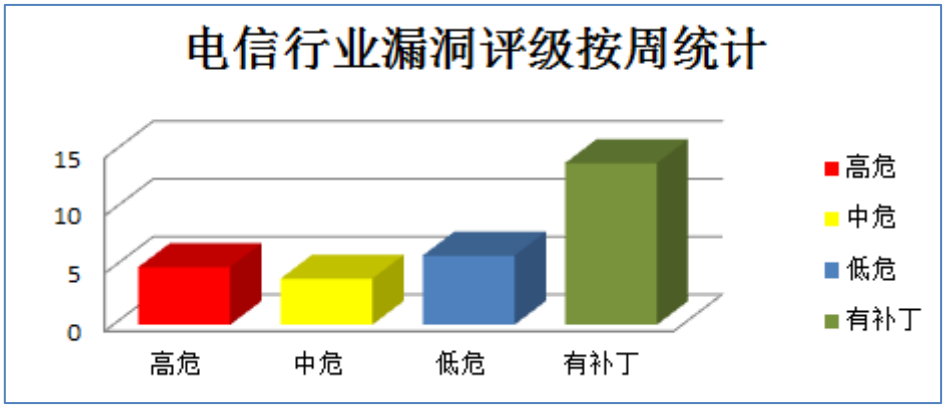

图 1 电信行业漏洞统计

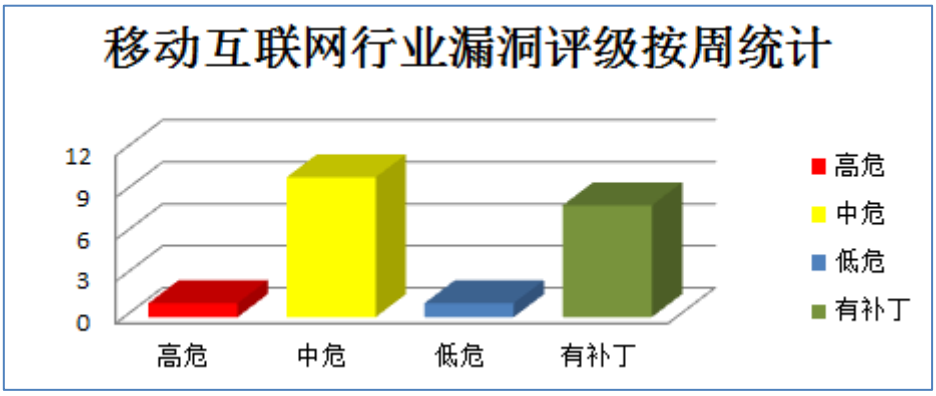

图 2 移动互联网行业漏洞统计

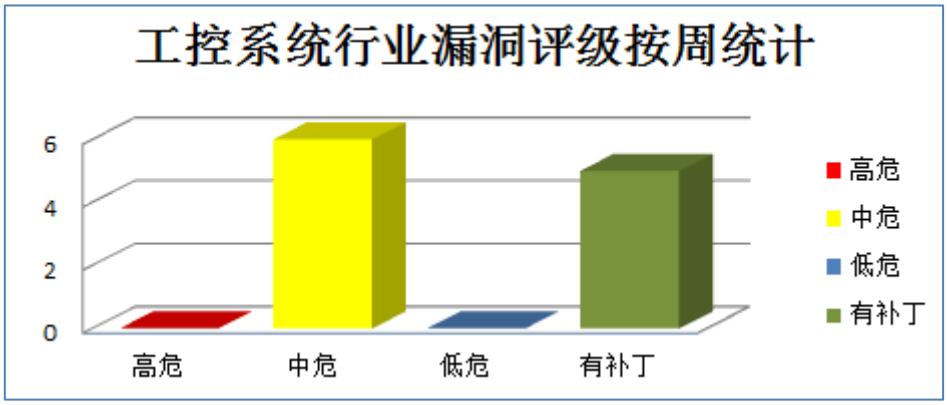

图 3 工控系统行业漏洞统计

本周重要漏洞信息

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、Apple 产品安全漏洞

Apple OS X 是一款苹果公司开发的操作系统。本周，该产品被披露存在多个安全漏

洞。攻击者利用漏洞可获得敏感信息和执行任意代码等。

CNVD 收录的相关漏洞包括：Apple OS X MB 内核内存破坏漏洞、Apple OS X SMBClient 内存泄露漏洞、Apple OS X 终端恶意文本误导用户漏洞、Apple OS X 时间机器架构备份漏洞、Apple OS X RSH 代码执行漏洞、Apple OS X keychain 锁定状态跟踪漏洞、Apple OS X kSecRevocationRequirePositiveResponse 标记处理漏洞、Apple OS X 证书显示处理漏洞。其中“Apple OS X MB 内核内存破坏漏洞、Apple OS X RSH 代码执行漏洞”的综合评级均为“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-2015-06405
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06406
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06407
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06408
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06401
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06402
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06403
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06404

2、 Adobe 产品安全漏洞

Adobe Flash Player 是一款 Flash 文件处理程序。Adobe AIR 是 Adobe 公司出品的跨操作系统的运行时库，通过它开发者可利用现有的 Web 开发技术。本周，该产品被披露存在内存破坏漏洞。攻击者利用漏洞可执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Flash Player 存在未明内存破坏漏洞（CNVD-2015-06304、CNVD-2015-06305、CNVD-2015-06306、CNVD-2015-06317、CNVD-2015-06318、CNVD-2015-06319、CNVD-2015-06324）、Adobe Flash Player 内存错误引用内存破坏漏洞（CNVD-2015-06308）。上述漏洞的综合评级均为“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-2015-06304
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06305
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06306
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06317
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06318
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06319
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06324
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06308

3、 Mozilla 产品安全漏洞

Mozilla Firefox 是一款开源 Web 浏览器。本周，该产品被披露存在缓冲区溢出漏洞。攻击者利用漏洞可执行任意代码。

CNVD 收录的相关漏洞包括：Mozilla Firefox 和 Firefox ESR ‘ConvertDialogOptions’函数缓冲区溢出漏洞、Mozilla Firefox 和 Firefox ESR ‘nsUnicodeToUTF8::GetMaxLength’函数缓冲区溢出漏洞、Mozilla Firefox 和 Firefox ESR ‘nsAttrAndChildArray::GrowBy’函数缓冲区溢出漏洞、Mozilla Firefox 和 Firefox ESR ‘AnimationThread’函数缓冲区溢出漏洞、Mozilla Firefox 和 Firefox ESR ‘XULContentSinkImpl::AddText’函数缓冲区溢出漏洞、Mozilla Firefox 存在未明缓冲区溢出漏洞、Mozilla Firefox 存在未明缓冲区溢出漏洞（CNVD-2015-06291）、Mozilla Firefox 和 Firefox ESR ‘InitTextures’缓冲区溢出漏洞。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-2015-06282
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06283
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06284
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06285
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06286
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06288
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06291
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06334

4、IBM 产品安全漏洞

IBM WebSphere eXtreme Scale 是一套分布式高速缓存解决方案。IBM Maximo Asset Management 是美国 IBM 公司的一套综合性资产生命周期和维护管理解决方案。本周，上述产品被披露存在多个安全漏洞。攻击者利用漏洞可获得敏感信息、绕过安全限制、进行跨站脚本和跨站请求伪造攻击等。

CNVD 收录的相关漏洞包括：IBM WebSphere eXtreme Scale 安全绕过漏洞、IBM WebSphere eXtreme Scale 跨站脚本漏洞、IBM WebSphere eXtreme Scale 信息泄露漏洞、IBM WebSphere eXtreme Scale 证书暴力破解漏洞、IBM WebSphere eXtreme Scale 跨站请求伪造漏洞、IBM WebSphere eXtreme Scale 访问权限绕过漏洞、IBM WebSphere eXtreme Scale 应答注入漏洞、IBM Maximo Asset Management 弱加密漏洞。目前，厂商已发布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-2015-06356
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06358
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06360
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06362

http://www.cnvd.org.cn/flaw/show/CNVD-2015-06396

http://www.cnvd.org.cn/flaw/show/CNVD-2015-06364

http://www.cnvd.org.cn/flaw/show/CNVD-2015-06366

http://www.cnvd.org.cn/flaw/show/CNVD-2015-06395

5、MoboTap Dolphin Browser for Android 任意文件写入漏洞

MoboTap Dolphin Browser for Android 是一款基于 Android 平台的海豚浏览器。本周，MoboTap Dolphin Browser 被披露存在高危漏洞。攻击者利用该漏洞可写入任意文件。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-2015-06363

更多高危漏洞如表 3 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-2015-06254	GE Digital Energy MDS PulseNET 和 MDS PulseNET Enterprise 绝对路径遍历漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://ics-cert.us-cert.gov/advisories/ICSA-15-258-03
CNVD-2015-06255	GE Digital Energy MDS PulseNET 和 MDS PulseNET Enterprise 远程代码执行漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://ics-cert.us-cert.gov/advisories/ICSA-15-258-03
CNVD-2015-06259	SAP NetWeaver J2EE Engine BP_FIND_JOBS_WITH_PROGRAM 函数模块 SQL 注入漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://service.sap.com/sap/support/notes/2193389
CNVD-2015-06373	IKEView.exe 栈缓冲区溢出漏洞	高	暂无
CNVD-2015-06271	多款 Adobe 产品任意代码执行漏洞（CNVD-2015-06271）	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://helpx.adobe.com/security/products/flash-player/apsb15-23.html
CNVD-2015-06274	多款 Adobe 产品内存错误引用漏洞（CNVD-2015-06274）	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://helpx.adobe.com/security/products/flash-player/apsb15-23.html
CNVD-2015-06279	多款 Adobe 产品输入验证漏洞	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://helpx.adobe.com/security/products/flash-player/apsb15-23.html

CNVD-2015-06278	多款 Adobe 产品缓冲区溢出漏洞（CNVD-2015-06278）	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://helpx.adobe.com/security/products/flash-player/apsb15-23.html
CNVD-2015-06303	Bolt 任意代码执行漏洞	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://bolt.cm/newsitem/bolt-2-2-5-released
CNVD-2015-06322	SIS XGI VGA 显示管理程序提权漏洞	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.korelogic.com/Resources/Advisories/KL-001-2015-004.txt

表 3 部分高危漏洞列表

小结：本周， Apple 产品被披露存在多个安全漏洞。攻击者利用漏洞可获得敏感信息和执行任意代码等。此外，Adobe、Mozilla、IBM 多款产品被披露存在多个安全漏洞，攻击者利用漏洞可获得敏感信息、绕过安全限制、进行跨站脚本攻击、跨站请求伪造攻击或执行任意代码。另外，MoboTap Dolphin Browser 被披露存在一个高危零日漏洞，攻击者利用该漏洞可写入任意文件。建议相关用户应随时关注上述厂商主页，及时获取修复补丁或解决方案。

本周重要漏洞修补信息

CNVD 整理和发布以下重要安全修补信息。

1、Linux 修补 Kernel 产品漏洞

Linux kernel 是一款开源的操作系统。

本周，IBM 修补了上述产品存在的安全绕过漏洞，避免攻击者利用漏洞绕过安全限制，执行未授权操作。CNVD 已收录相关补丁，请广大用户及时下载更新，避免引发漏洞相关的网络安全事件。

补丁下载链接：http://www.cnvd.org.cn/patchInfo/show/64830

本周要闻速递

1. 杀毒软件 Avast 被曝 0day 漏洞

Google 安全专家 Tavis Ormandy，发现一个 Avast 杀毒软件的 0day 漏洞，该漏洞可能导致攻击者侵入用户电脑，并在用户电脑上执行恶意代码。目前，Avast 已经宣布发布一个补丁对他们的杀毒软件进行修复更新。

参考链接：http://www.freebuf.com/news/81102.html

2. 网件（Netgear）路由器被曝严重的 DNS 漏洞

近日，网件（Netgear）路由器被发现存在严重的 DNS 漏洞，目前，网件还未修补该已公布的漏洞，该漏洞允许攻击者篡改受影响的路由器的 DNS 设置，会影响其路由器的安全性，预估超过 10,000 台路由器已经遭受攻击。

参考链接：http://www.freebuf.com/news/81272.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