国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2017 年 07 月 10 日-2017 年 07 月 16 日 **2017 年第 29 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 413 个，其中高危漏洞 178 个、中危漏洞 216 个、低危漏洞 19 个。漏洞平均分值为 6.40。本周收录的漏洞中，涉及 0day 漏洞 211 个（占 51%），其中互联网上出现“WinDjView 远程代码执行漏洞、Joomla! JoomRecipe 组件 SQL 注入漏洞”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 1192 个，与上周（1011 个）环比增长 18%。

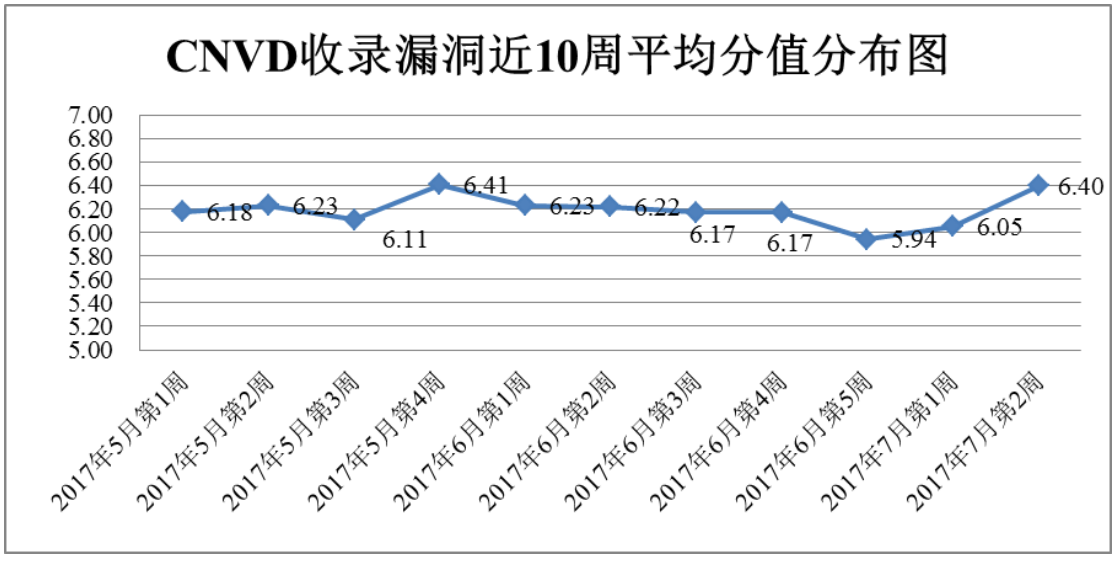

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 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 413 个漏洞。报送情况如表 1 所示。其中，天融信、安天实验室、H3C、华为技术有限公司、恒安嘉新等单位报送数量较多。360 网神、漏洞盒子、网信智安、中新网络信息安全股份有限

公司、江苏同袍信息科技有限公司、江西安服信息产业有限公司、上海零盾网络科技有限公司、六壬网安、清远职业技术学院、安徽新华博信息技术股份有限公司、深圳鼎安天下信息科技有限公司、北京安码科技有限公司、中国航天科工集团第四研究院软件评测中心（北京）、杭州朔方信息技术有限公司、南京联成科技发展股份有限公司、山石网科通信技术有限公司、中电长城网际系统应用有限公司、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、广州神月信息安全技术有限公司及其他个人白帽子向 CNVD 提交了 1192 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
天融信	171	2
安天实验室	160	0
漏洞盒子	150	150
H3C	141	1
华为技术有限公司	125	0
恒安嘉新	104	0
中国电信集团系统集成有限责任公司	91	12
启明星辰	82	5
杭州安恒信息技术有限公司	82	0
绿盟科技	76	0
厦门服云信息科技有限公司	24	0
北京数字观星科技有限公司	5	0
知道创宇	3	3
东软	3	3
西安四叶草信息技术有限公司	3	3
北京无声信息技术有限公司	2	0
南京铱迅信息技术股份有限公司	1	1

网信智安	25	25
中新网络信息安全股份有限公司	25	25
江苏同袍信息科技有限公司	14	14
江西安服信息产业有限公司	11	11
上海零盾网络科技有限公司	10	10
六壬网安	9	9
清远职业技术学院	8	8
安徽新华博信息技术股份有限公司	5	5
深圳鼎安天下信息科技有限公司	5	5
北京安码科技有限公司	4	4
中国航天科工集团第四研究院软件评测中心（北京）	4	4
杭州朔方信息技术有限公司	3	3
南京联成科技发展股份有限公司	3	3
山石网科通信技术有限公司	2	2
中电长城网际系统应用有限公司	2	2
上海犇众信息技术有限公司	1	1
广州软云计算机科技有限公司	1	1
广州神月信息安全技术有限公司	1	1
山西分中心	10	10
新疆分中心	9	9
吉林分中心	8	8
河北分中心	3	3

甘肃分中心	2	2
宁夏分中心	2	2
浙江分中心	2	2
陕西分中心	1	1
广东分中心	1	1
个人	841	841
报送总计	2235	1192
录入总计	413（去重）	1192

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 413 个漏洞。其中应用程序漏洞 210 个，web 应用漏洞 125 个，操作系统漏洞 48 个，网络设备漏洞 29 个，数据库漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	210
web 应用漏洞	125
操作系统漏洞	48
网络设备漏洞	29
数据库漏洞	1

表 2 漏洞按影响类型统计表

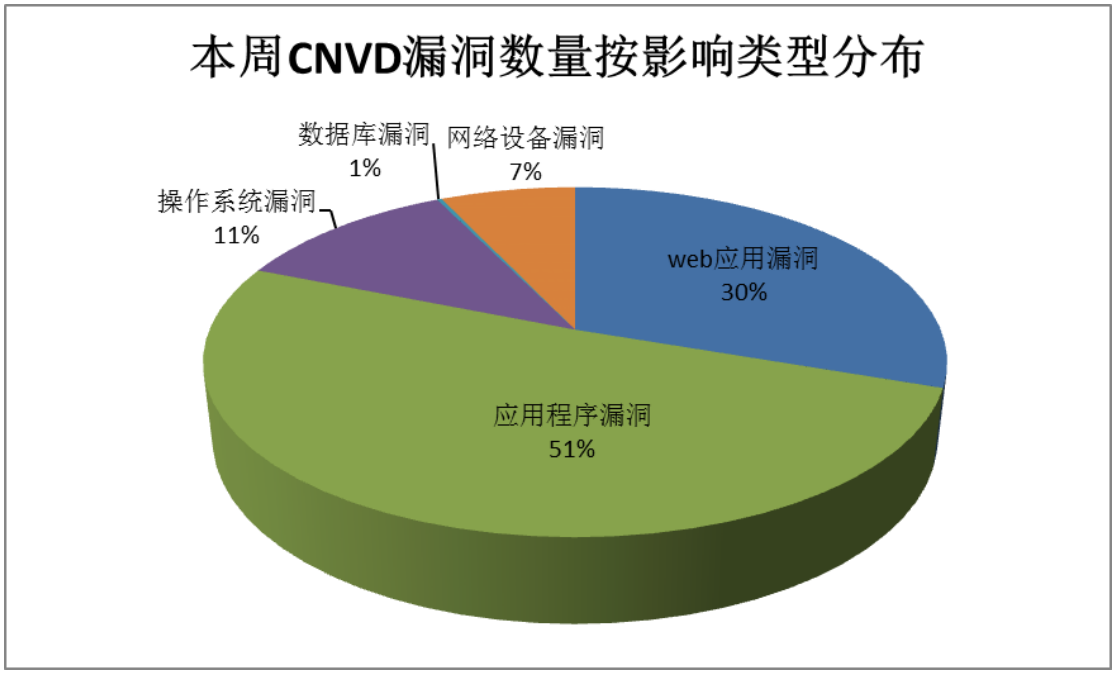

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、XnView、IrfanView 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	48	12%
2	XnView	34	8%
3	IrfanView	27	7%
4	Foscam	13	3%
5	Cisco	11	3%
6	Microsoft	10	2%
7	IBM	10	2%
8	SAP	8	2%
9	Siemens	6	1%
10	其他	246	60%

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 8 个电信行业漏洞，81 个移动互联网行业漏洞，2 个工控系统行业漏洞（如下图所示）。其中，“Teltonika RUT9XX 路由器任意命令执行漏洞、Siemens SIMATIC WinCC Sm@rtClient for Android 中间人攻击漏洞、

Google Android 高通组件存在多个漏洞、多款 Lenovo VIBE 手机权限访问漏洞、Apple macOS/iOS 用户授权检查竞争条件漏、Google Android Qualcomm 组件存在未明漏洞、Google Android WideVine DRM 安全绕过漏洞、Huawei P10 Plus 手机触摸屏驱动内存重复释放漏洞”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/

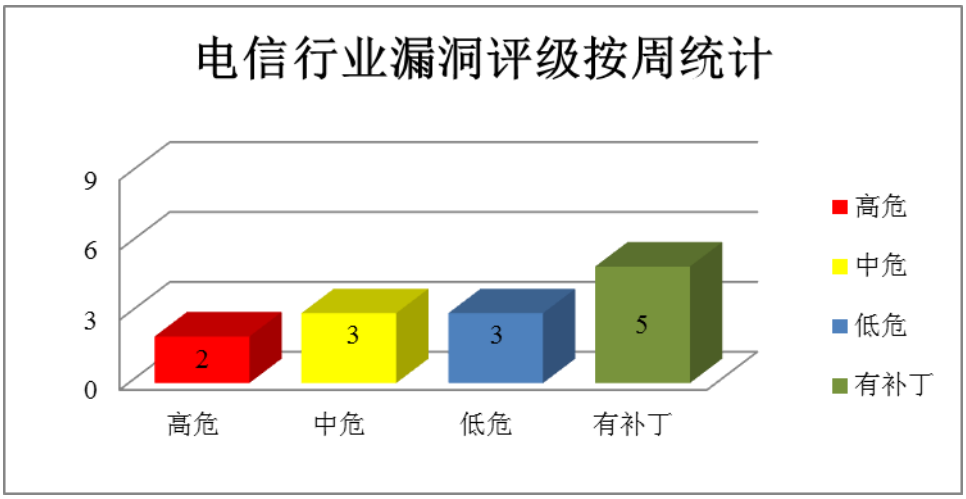

图 3 电信行业漏洞统计

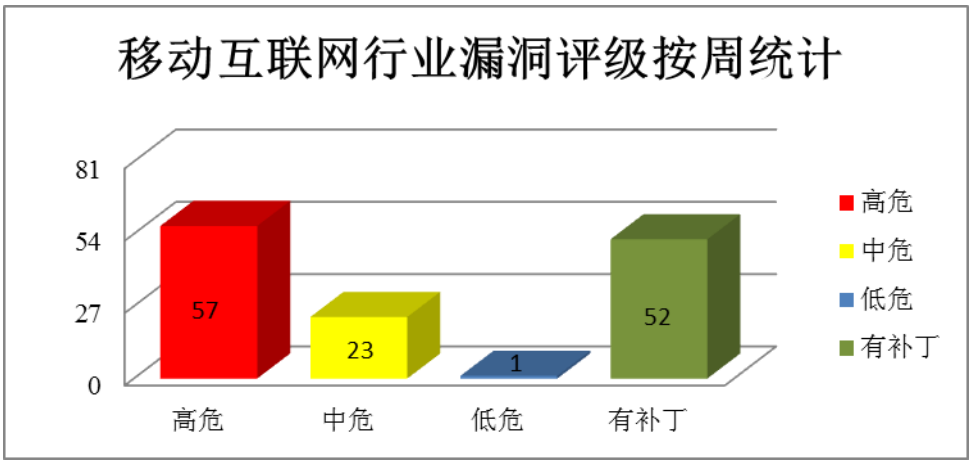

图 4 移动互联网行业漏洞统计

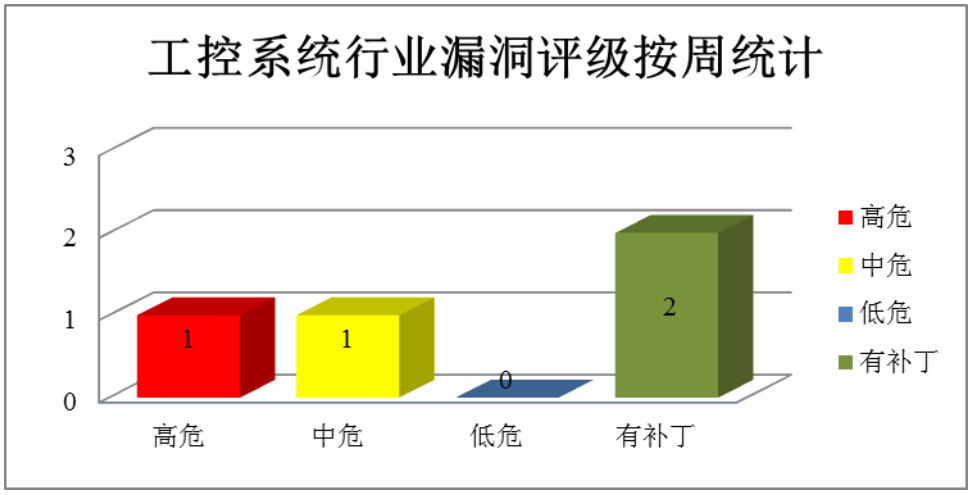

图 5 工控系统行业漏洞统计

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、Google 产品安全漏洞

Android 是一种基于 Linux 的自由及开放源代码的操作系统。本周，该产品被披露存在多个漏洞，攻击者可以利用漏洞获取敏感信息，执行任意代码，发起拒绝服务拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Google Android 高通组件存在多个漏洞（CNVD-2017-14380、CNVD-2017-14381、CNVD-2017-14382、CNVD-2017-14383、CNVD-2017-14384、CNVD-2017-14385、CNVD-2017-14386、CNVD-2017-14387）。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-2017-14380
http://www.cnvd.org.cn/flaw/show/CNVD-2017-14381
http://www.cnvd.org.cn/flaw/show/CNVD-2017-14382
http://www.cnvd.org.cn/flaw/show/CNVD-2017-14383
http://www.cnvd.org.cn/flaw/show/CNVD-2017-14384
http://www.cnvd.org.cn/flaw/show/CNVD-2017-14385
http://www.cnvd.org.cn/flaw/show/CNVD-2017-14386
http://www.cnvd.org.cn/flaw/show/CNVD-2017-14387

2、Microsoft 产品安全漏洞

Internet Explorer 是微软公司推出的一款网页浏览器。Microsoft Edge 是内置于 Windows 10 版本中的网页浏览器。本周，上述产品被披露存在内存破坏漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer 远程内存破坏漏洞（CNVD-2017-14447）、Microsoft Edge 脚本引擎远程内存破坏漏洞（CNVD-2017-14607、CNVD-2017-14608、CNVD-2017-14609、CNVD-2017-14448、CNVD-2017-14449、CNVD-2017-14450、CNVD-2017-14451）。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-2017-14447
http://www.cnvd.org.cn/flaw/show/CNVD-2017-14607
http://www.cnvd.org.cn/flaw/show/CNVD-2017-14608
http://www.cnvd.org.cn/flaw/show/CNVD-2017-14609
http://www.cnvd.org.cn/flaw/show/CNVD-2017-14448
http://www.cnvd.org.cn/flaw/show/CNVD-2017-14449
http://www.cnvd.org.cn/flaw/show/CNVD-2017-14450
http://www.cnvd.org.cn/flaw/show/CNVD-2017-14451

3、Foscam 产品安全漏洞

Foscam C1 Indoor HD Camera 是中国福斯康姆（Foscam）公司的一款无线高清 IP 摄像机。Foscam Indoor IP Camera C1 Series 是一款 C1 系列无线 IP 摄像机产品。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞注入任意命令、执行任意代码或泄露敏感信息等。

CNVD 收录的相关漏洞包括：Foscam C1 Indoor HD Camera 命令注入漏洞、Foscam C1 Indoor HD Camera 命令注入漏洞（CNVD-2017-14061、CNVD-2017-14362、CNVD-2017-14364）、Foscam C1 Indoor HD Camera 缓冲区溢出漏洞、Foscam C1 Indoor HD Camera 缓冲区溢出漏洞（CNVD-2017-14066）、Foscam C1 Indoor HD Camera 路径遍历漏洞、Foscam Indoor IP Camera C1 SeriesCGIProxy.fcgi SMTP 测试密码参数配置命令注入漏洞。其中，“Foscam Indoor IP Camera C1 SeriesCGIProxy.fcgi SMTP 测试密码参数配置命令注入漏洞”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-2017-14363
http://www.cnvd.org.cn/flaw/show/CNVD-2017-14061
http://www.cnvd.org.cn/flaw/show/CNVD-2017-14362
http://www.cnvd.org.cn/flaw/show/CNVD-2017-14064
http://www.cnvd.org.cn/flaw/show/CNVD-2017-14360
http://www.cnvd.org.cn/flaw/show/CNVD-2017-14066
http://www.cnvd.org.cn/flaw/show/CNVD-2017-14361

http://www.cnvd.org.cn/flaw/show/CNVD-2017-14100

4、Siemens 产品安全漏洞

Siemens SIMATIC WinCC Sm@rtClient for Android 是一款安卓系统上的客户端程序。SiPass server 是 SiPass 集中访问控制系统的组件。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身份验证机制、读取或写入文件、读取和修改数据等。

CNVD 收录的相关漏洞包括：Siemens SiPass integrated 认证绕过漏洞、Siemens SiPass integrated 文件读写漏洞、Siemens SiPass integrated 未授权操作漏洞、Siemens SiPass integrated 凭证获取漏洞、Siemens SIMATIC WinCC Sm@rtClient for Android 身份验证绕过漏洞、Siemens SIMATIC WinCC Sm@rtClient for Android 中间人攻击漏洞。除“Siemens SiPass integrated 凭证获取漏洞、Siemens SIMATIC WinCC Sm@rtClient for Android 身份验证绕过漏洞”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-2017-14604

http://www.cnvd.org.cn/flaw/show/CNVD-2017-14603

http://www.cnvd.org.cn/flaw/show/CNVD-2017-14602

http://www.cnvd.org.cn/flaw/show/CNVD-2017-14601

http://www.cnvd.org.cn/flaw/show/CNVD-2017-14606

http://www.cnvd.org.cn/flaw/show/CNVD-2017-14605

5、多款 WiMAX 路由器存在身份验证绕过漏洞

WiMAX(微波存取全球互通)是一种以 IEEE-802.16 标准为基础的通讯技术。本周，多款 WiMAX 路由器被披露存在身份验证绕过漏洞，攻击者可利用漏洞更改设备上的管理员密码。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-2017-14427

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-2017-13755	FreeRADIUS 服务器 TLS 认证绕过漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://freeradius.org/security.html
CNVD-2017-13899	EMC Isilon OneFS 权限提升漏洞	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.emc.com/
CNVD-2017-13997	OSCI Transport Library OSCI-Transport XXE 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.xoev.de
CNVD-2017-14147	Debian cron package 权限提升漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://bugs.debian.org/864466
CNVD-2017-14368	EMC Avamar Server Software 安全绕过漏洞	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：https://www.emc.com/
CNVD-2017-14369	EMC Avamar Server Software 任意文件上传漏洞	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.emc.com/
CNVD-2017-14420	AppCheck 和 AppCheck Pro 不可信搜索路径漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.jiransoft.co.jp/support/apc_1
CNVD-2017-14604	Siemens SiPass integrated 认证绕过漏洞	高	用户可联系供应商获得补丁信息：https://www.siemens.com/cert/advisories/
CNVD-2017-14603	Siemens SiPass integrated 文件读写漏洞	高	用户可联系供应商获得补丁信息：https://www.siemens.com/cert/advisories/
CNVD-2017-14602	Siemens SiPass integrated 未授权操作漏洞	高	用户可联系供应商获得补丁信息：https://www.siemens.com/cert/advisories/

表 4 部分重要高危漏洞列表

小结：本周，Google 被披露存在多个漏洞，攻击者可以利用漏洞获取敏感信息，执行任意代码，发起拒绝服务拒绝服务攻击等。此外，Microsoft Foscam、Siemens 等多款产品被披露存在多个漏洞，攻击者利用漏洞可泄露敏感信息、执行任意命令、绕过验证机制或读取和写入文件等。另外，多款 WiMAX 路由器被披露存在身份验证绕过漏洞，攻击者可利用漏洞更改设备上的管理员密码。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. 博通曝出 Wi-Fi 芯片中的 BroadPwn 漏洞

Google 发布了 Android 设备的每月安全更新。其中对于 Broadcom Wi-Fi 芯片组中发现的远程代码执行漏洞也进行了修复，目前暂命名为 BroadPWN。该漏洞可能会影响到数百万种 Android 设备，以及部分 iPhone 设备。

BroadPwn 中涉及到一个 critical 级别的的远程代码执行漏洞，目前追踪为 CVE-2017-9417，影响 Broadcom BCM43xx 系列 WiFi 芯片组。远程攻击者可以在没有用户交互的情况下触发漏洞问题，如果具有了内核操作特权，则可在该设备上执行恶意代码。

参考链接：http://www.freebuf.com/news/139773.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