

信息安全漏洞周报

2016 年 11 月 14 日-2016 年 11 月 20 日

2016 年第 47 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 268 个，其中高危漏洞 103 个、中危漏洞 144 个、低危漏洞 21 个。漏洞平均分为 6.02。本周收录的漏洞中，涉及 0day 漏洞 36 个（占 13%）。其中互联网上出现“Schoolhos CMS 'kelas'参数 SQL 注入漏洞、Teradata Virtual Machine Community Edition 权限提升漏洞”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 569 个，与上周（835 个）环比下降 32%。

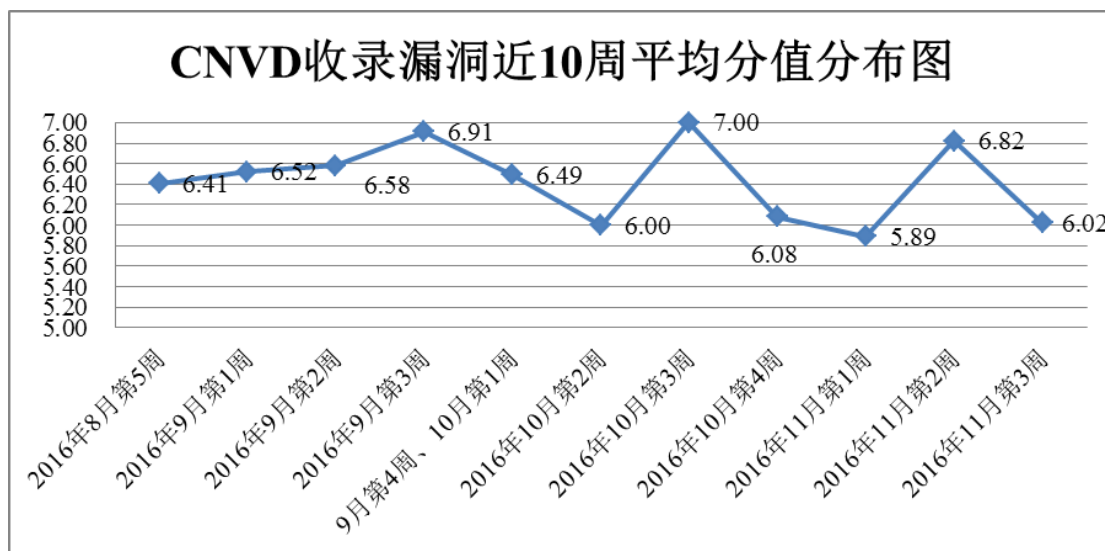


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 12 家成员单位、合作伙伴及企业用户、个人用户报送了本周收录的全部 268 个漏洞。报送情况如表 1 所示。其中，蓝盾信息技术有限公司、安天实验室、天

融信、恒安嘉新、绿盟科技等单位报送数量较多。360 网神、漏洞盒子、广西鑫瀚科技有限公司、新疆天山智汇信息科技有限公司、广州神月信息技术有限公司、南京铱迅信息技术股份有限公司、北京安码科技有限公司、福建榕基软件股份有限公司及其他个人白帽子向 CNVD 提交了 569 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	406	406
蓝盾信息安全技术有限公司	180	0
安天实验室	159	0
天融信	135	0
恒安嘉新	140	12
绿盟科技	106	3
杭州安恒信息技术有限公司	87	0
H3C	80	0
华为技术有限公司	52	2
中国电信集团系统集成有限责任公司	34	0
知道创宇	2	0
北京数字观星科技有限公司	1	0
漏洞盒子	87	87
广西鑫瀚科技有限公司	7	7
新疆天山智汇信息科技有限公司	3	3
广州神月信息技术有限公司	3	3
南京铱迅信息技术股份有限公司	1	1
北京安码科技有限公司	1	1
福建榕基软件股份有限公司	1	1

CNCERT 宁夏分中心	3	3
个人	40	40
报送总计	1528	569
录入总计	268（去重）	569

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 268 个漏洞。其中应用程序漏洞 118 个，操作系统漏洞 77 个，web 应用漏洞 50 个，网络设备漏洞 21 个，安全产品漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	118
操作系统漏洞	77
web 应用漏洞	50
网络设备漏洞	21
安全产品漏洞	2

表 2 漏洞按影响类型统计表

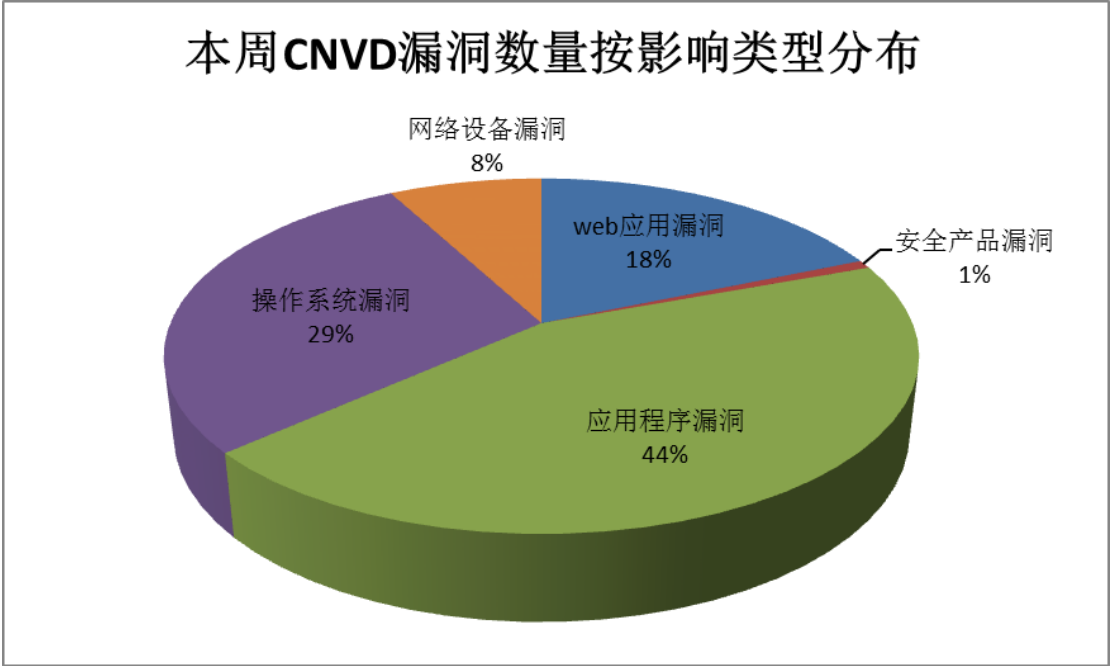


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Microsoft、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	66	25%
2	Microsoft	19	7%
3	IBM	17	6%
4	Linux	15	6%
5	TYPO3	9	3%
6	OIC	8	3%
7	HP	8	3%
8	Huawei	8	3%
9	Corega	4	1%
10	其他	115	43%

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 10 个电信行业漏洞，52 个移动互联网行业漏洞，7 个工控系统行业漏洞（如下图所示）。其中，“Google Android Webview 远程代码执行漏洞、Google Nexus Qualcomm bootloader 权限提升漏洞、Google Android Bluetooth 权限提升漏洞、Google Android Framework APIs 权限提升漏洞、Google Android Skia 内存破坏漏洞、Google Android libjpeg 远程代码执行漏洞、Google Android libzipfile 权限提升漏洞、Phoenix Contact ILC 信息泄露漏洞、Phoenix Contact ILC 身份验证绕过漏洞、Phoenix Contact ILC 安全绕过漏洞”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/>

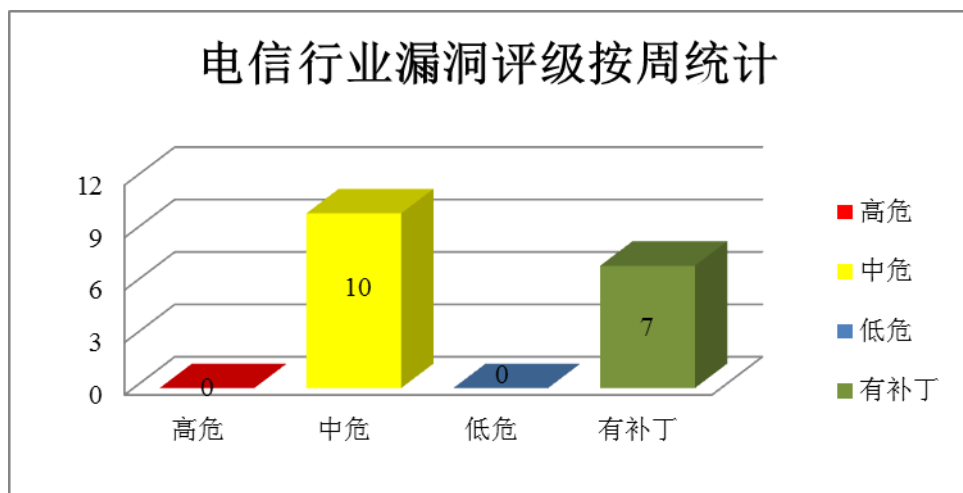


图 3 电信行业漏洞统计

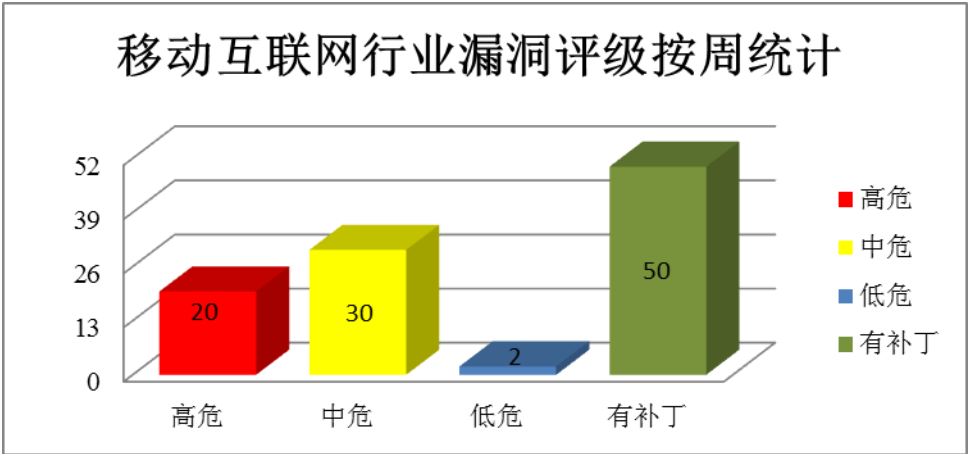


图 4 移动互联网行业漏洞统计

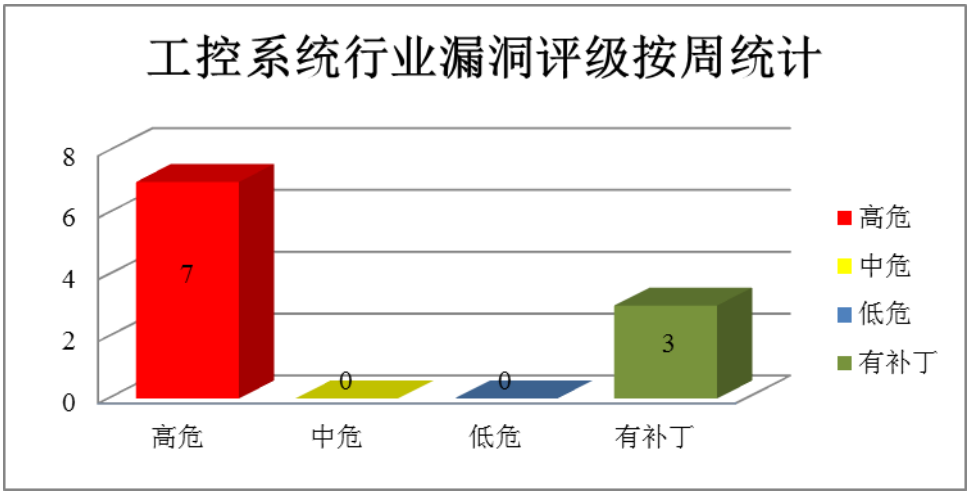


图 5 工控系统行业漏洞统计



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、Google 产品安全漏洞

Google Pixel C 是美国谷歌（Google）公司的一款平板电脑。NVIDIA GPU driver 是使用在其中的一个 NVIDIA 图形处理器驱动组件。Android 是一套以 Linux 为基础的开源操作系统。Mediaserver 是其中的一个多媒体服务组件。本周，上述产品被披露存在权限提升漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Google Pixel C NVIDIA GPU Driver 权限提升漏洞（CNVD-2016-11126、CNVD-2016-11127、CNVD-2016-11128、CNVD-2016-11129、CNVD-2016-11130、CNVD-2016-11131）、Google Android Mediaserver 权限提升漏洞（CNVD-2016-11042、CNVD-2016-11043）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/flaw/show/CNVD-2016-11126>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11127>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11128>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11129>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11130>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11131>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11042>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11043>

2、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。本周, 该产品被披露存在特权提升漏洞, 攻击者可利用漏洞提升特权。

CNVD 收录的相关漏洞包括: Microsoft Windows 通用日志文件系统驱动程序特权提升漏洞 (CNVD-2016-11019、CNVD-2016-11020、CNVD-2016-11022、CNVD-2016-11023)、Microsoft Windows 本地权限提升漏洞 (CNVD-2016-11013、CNVD-2016-11021)、Microsoft Windows IME 特权提升漏洞、Microsoft Windows 任务调度器特权提升漏洞等。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/flaw/show/CNVD-2016-11019>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11020>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11022>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11023>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11013>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11021>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11066>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11067>

3、IBM 产品安全漏洞

IBM Kenexa LMS on Cloud 功能齐全、可配置的企业级社交学习管理系统 (LMS), 集成了社交网络、协作和知识分享功能。IBM Security Privileged Identity Manager 是美国 IBM 公司的一款身份监管解决方案中的身份管理产品。IBM Connections 是一套社交软件平台。IBM BigFix Platform 一套系统管理软件。本周, 上述产品被披露存在多个漏洞, 攻击者可利用漏洞上传任意文件、泄露敏感信息或发起跨站脚本攻击等。

CNVD 收录的相关漏洞包括: IBM Kenexa LMS on Cloud 任意文件上传漏洞、IBM Kenexa LMS on Cloud 目录遍历漏洞、IBM Kenexa LMS on Cloud 目录遍历漏洞 (CNVD-2016-11279)、IBM BigFix Platform 远程命令注入漏洞、IBM Security Privile

ged Identity Manager 身份验证绕过漏洞、IBM Kenexa LMS on Cloud 存在未明跨站脚本漏洞、IBM Connections 信息泄露漏洞（CNVD-2016-11261）、IBM Resilient 跨站脚本漏洞等。其中，“IBM Kenexa LMS on Cloud 任意文件上传漏洞、IBM Kenexa LMS on Cloud 目录遍历漏洞、IBM Kenexa LMS on Cloud 目录遍历漏洞（CNVD-2016-11279）、IBM BigFix Platform 远程命令注入漏洞”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-2016-11292>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11280>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11279>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11086>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11281>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11291>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11261>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11231>

4、Linux 产品安全漏洞

Linux kernel 是美国 Linux 基金会发布的操作系统 Linux 所使用的内核。本周，该产品被披露存在信息泄露、拒绝服务和远程代码执行漏洞，攻击者可利用漏洞泄露敏感信息、远程执行任意代码或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Linux Kernel 信息泄露漏洞（CNVD-2016-11075、CNVD-2016-11074、CNVD-2016-11073、CNVD-2016-11072）、Linux kernel 拒绝服务漏洞（CNVD-2016-11071、CNVD-2016-11070、CNVD-2016-11069）、Linux Kernel 远程代码执行漏洞等。其中“Linux Kernel 远程代码执行漏洞”的危害等级为“高级”。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-2016-11075>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11074>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11073>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11072>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11071>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11070>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11069>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11060>

5、Teradata Virtual Machine Community Edition 代码执行漏洞

Teradata Virtual Machine Community Edition 是美国天睿（Teradata）公司的一个由

SUSE Linux 企业服务器（SLES）操作系统和 Teradata 数据库打包成的虚拟容器。本周，Teradata 被披露存在代码执行漏洞。攻击者可利用该漏洞在受影响应用程序上下文中执行任意代码。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-2016-11225>

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-2016-10997	Phoenix Contact ILC 安全绕过漏洞	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.phoenixcontact.com/online/portal/pc
CNVD-2016-10998	Phoenix Contact ILC 身份验证绕过漏洞	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.phoenixcontact.com/online/portal/pc
CNVD-2016-10999	Phoenix Contact ILC 信息泄露漏洞	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.phoenixcontact.com/online/portal/pc
CNVD-2016-11001	DotCMS SQL 注入漏洞（CNVD-2016-11001）	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://dotcms.com/
CNVD-2016-11002	DotCMS SQL 注入漏洞（CNVD-2016-11002）	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://dotcms.com/
CNVD-2016-11003	DotCMS SQL 注入漏洞（CNVD-2016-11003）	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://dotcms.com/
CNVD-2016-11004	DotCMS SQL 注入漏洞（CNVD-2016-11004）	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://dotcms.com/
CNVD-2016-11005	DotCMS SQL 注入漏洞（CNVD-2016-11005）	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://dotcms.com/
CNVD-2016-11006	DotCMS SQL 注入漏洞 (CNVD-2016-11006)	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://dotcms.com/
CNVD-2016-11007	DotCMS SQL 注入漏洞 (CNVD-2016-11007)	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://dotcms.com/

表 4 部分重要高危漏洞列表

小结：本周，Google 产品被披露存在权限提升漏洞，攻击者可利用漏洞执行任意代码。此外，Microsoft、Linux、IBM 等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、提升特权、远程执行任意代码和发起跨站脚本攻击等。另外，Teradata 被披露存在代码执行漏洞。攻击者可利用该漏洞在受影响应用程序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. 绕过密码就能访问 iPhone 照片或消息

根据国外媒体的最新报道，安全研究人员在 iOS8、iOS9 和 iOS10（包括 iOS10.2 beta 3）中发现了一个严重的安全漏洞，这个漏洞将允许攻击者绕过 iPhone 的锁屏密码，并利用苹果个人助手 Siri 的相关功能访问到目标用户 iPhone 中的个人数据。据了解，这个漏洞是由 EverythingApplePro（一位 YouTube 用户）和 iDeviceHelps（国外的一家科技网站）发现的。他们目前已经发布了一个演示视频，估计苹果公司会在下一个 iOS beta 版中修复这个漏洞。在苹果公司正式修复这个问题之前，iOS 用户可以禁用锁屏状态下的 Siri 功能来保护自己的安全。

参考链接：<http://www.freebuf.com/news/120366.html>

2. 英国最大的移动运营商 Three 遭黑客入侵

英国最大的移动运营商之一 Three 公司承认系统被黑客闯入。Three 公司称，黑客是使用其员工账号登录到客户升级数据库。黑客闯入的数据库可能涉及 600 万 Three 用户的信息，占客户总数的三分之二。虽然泄露数据包括客户的姓名、电话号码、地址和出生日期，但黑客未能获取客户的财务信息。他们已经在与警方和有关人员调查此事，黑客的目的是盗窃其高端智能手机（通过 Three 用户的升级帐号来获得换取手机的机会），用户的财务方面信息将不会有危险。Three 公司称黑客此次入侵是为了盗取该公司的新款智能手机，以此获利。

参考链接：<http://www.freebuf.com/news/120465.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