国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2016 年 06 月 13 日-2016 年 06 月 19 日 **2016 年第 25 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 161 个，其中高危漏洞 65 个、中危漏洞 91 个、低危漏洞 5 个。漏洞平均分值为 6.52 分。本周收录的漏洞中，涉及 0day 漏洞 11 个（占 7%）。其中互联网上出现“Cisco RV110W/RV130W/RV215W 路由器远程代码执行漏洞、SiteServer CMS 后台存在任意文件写入漏洞”等零日漏洞，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 1380 个，与上周（1235 个）环比增长 12%。本周，微软官方发布了业界称之为 “Bad Tunnel”的 Microsoft Windows WPAD 权限提升漏洞，且互联网上商用扫描软件已经发布了检测利用插件，有可能会诱发对高价值目标的定向攻击，为此 CNVD 已发布“关于 Microsoft Windows WPAD 权限提升漏洞（BadTunnel）的安全公告”。

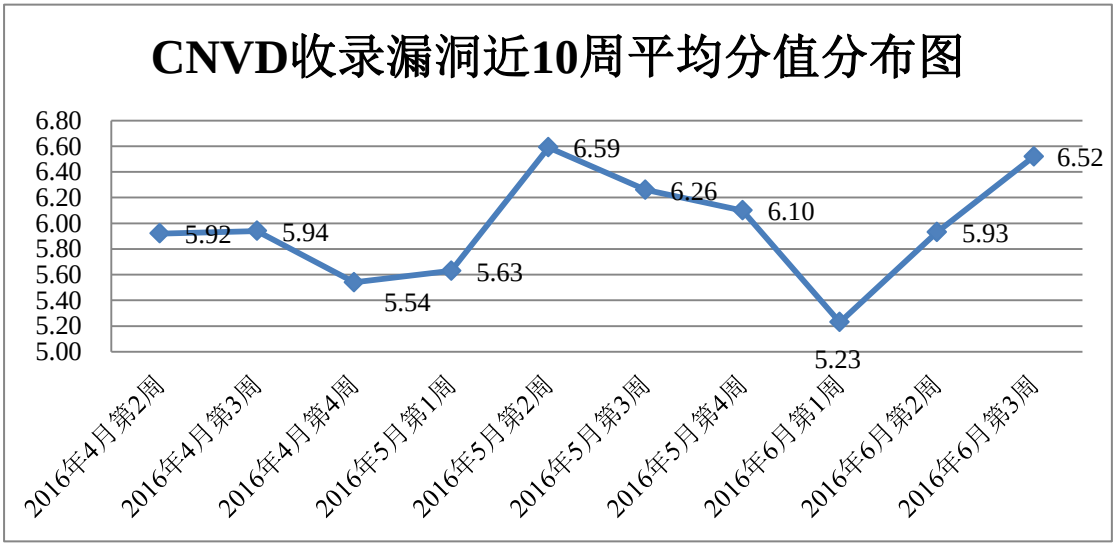

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 9 家成员单位、合作伙伴及个人报送了本周收录的全部 161 个漏洞。报送情况如表 1 所示。其中，启明星辰、安天实验室、恒安嘉新、天融信等单位报送数量较多。补天平台、乌云、漏洞盒子、西安四叶草信息技术有限公司、福建六壬网安股份有限公司、广州圣辉信息技术有限公司、腾讯玄武实验室及白帽子向 CNVD 提交了 1380 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)	750	750
启明星辰	217	0
安天实验室	153	0
恒安嘉新	117	20
天融信	114	0
绿盟科技	94	0
东软	74	0
中国电信集团系统集成有限责任公司	54	0
H3C	4	0
乌云	536	536
漏洞盒子	38	38
西安四叶草信息技术有限公司	9	9
福建六壬网安股份有限公司	5	5
广州圣辉信息技术有限公司	2	2
腾讯玄武实验室	1	1
CNCERT 安徽分中心	5	5
CNCERT 甘肃分中心	3	3
CNCERT 江西分中心	2	2

个人	9	9
报送总计	2187	1380
录入总计	161（去重）	1380

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 161 个漏洞。其中应用程序漏洞 108 个，操作系统漏洞 34 个，网络设备漏洞 16 个，Web 应用漏洞 3 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	108
操作系统漏洞	34
网络设备漏洞	16
web 应用漏洞	3

表 2 漏洞按影响类型统计表

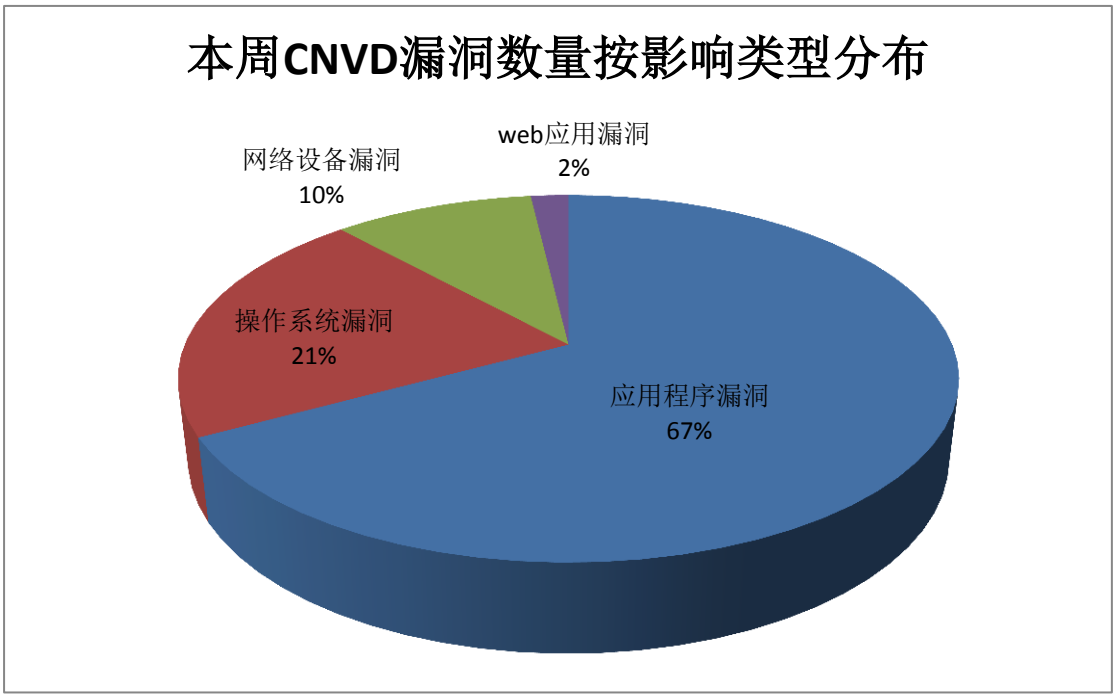

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft 、Google、Mozilla 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	Microsoft	32	20%
2	Google	17	11%

3	Mozilla	14	9%
4	IBM	11	7%
5	Apache	9	6%
6	HP	9	6%
7	Cisco	7	4%
8	Adobe	6	4%
9	Wireshark	6	4%
10	其他	50	29%

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 12 个电信行业漏洞，20 个移动互联网行业漏洞，3 个工控系统行业漏洞（如下图所示）。其中，“Huawei WS851 栈缓冲区溢出漏洞、Android Qualcomm Wi-Fi 驱动权限提升漏洞（CNVD-2016-04086）、Android Qualcomm 声音驱动权限提升漏洞（CNVD-2016-04087、CNVD-2016-04088）、Android Qualcomm Wi-Fi 驱动权限提升漏洞、Android Mediaserver 提权漏洞（CNVD-2016-03926、CNVD-2016-03925、CNVD-2016-03924、CNVD-2016-03923）、Android Mediaserver 权限提升漏洞（CNVD-2016-03963、CNVD-2016-03964、CNVD-2016-03965、CNVD-2016-03966、CNVD-2016-03967）”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/

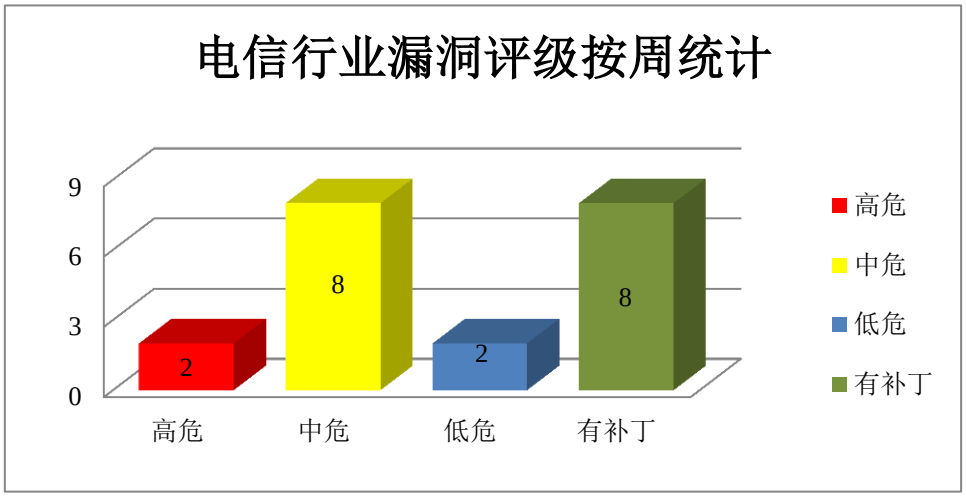

图 3 电信行业漏洞统计

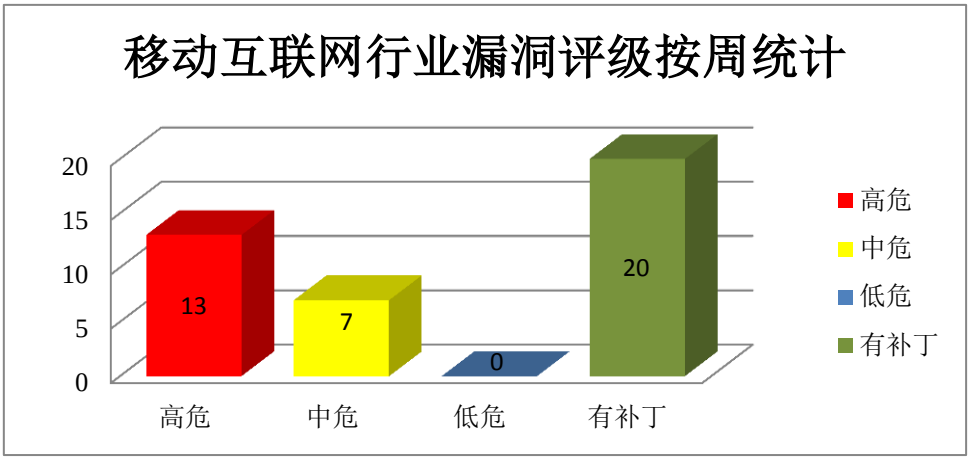

图 4 移动互联网行业漏洞统计

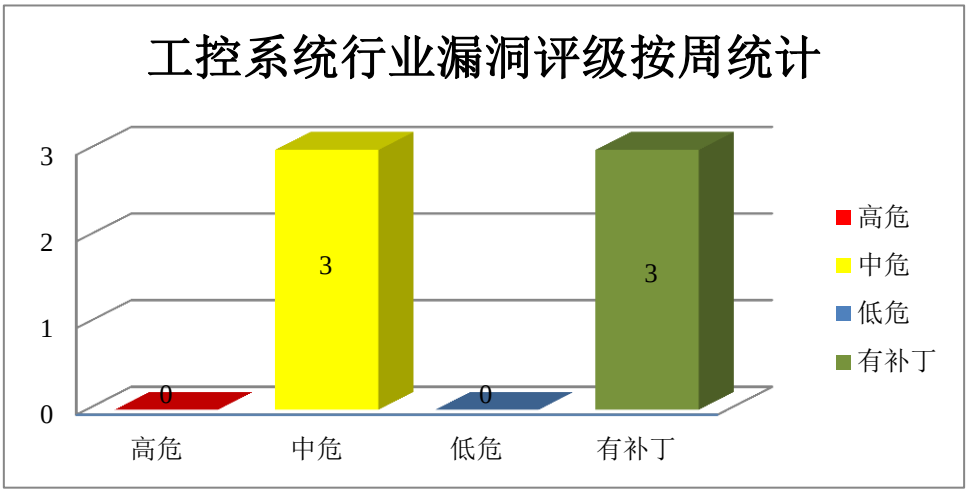

图 5 工控系统行业漏洞统计

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、 Microsoft 产品安全漏洞

6 月 14 日，微软发布了 2016 年 6 月份的月度例行安全公告，共含 16 项更新，修复了 Microsoft Windows、Internet Explorer、Edge、Office、OfficeService 和 Web Apps 中存在的 36 个安全漏洞。其中，5 项远程代码更新的综合评级为最高级“严重”级别。利用上述漏洞，攻击者可提升权限，远程执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer 脚本引擎内存破坏漏洞（CNVD-2016-04077、CNVD-2016-04052、CNVD-2016-04055、CNVD-2016-04056）、Microsoft Internet Explorer 内存破坏漏洞（CNVD-2016-04053、CNVD-2016-04058、CNVD-2016-04059）、Microsoft Windows WPAD 特权提升漏洞等。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/webinfo/show/3870

2、Apache 产品安全漏洞

Apache Struts 是美国阿帕奇（Apache）软件基金会负责维护的一个开源项目，是一套用于创建企业级 Java Web 应用的开源 MVC 框架，主要提供两个版本框架产品，Struts 1 和 Struts 2。Apache Struts 2 是 Apache Struts 的下一代产品，是在 Struts 1 和 WebWork 的技术基础上进行了合并的全新 Struts 2 框架，其体系结构与 Struts 1 差别较大。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息、执行 CSRF 攻击和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Apache Struts2 远程代码执行漏洞（CNVD-2016-04093、CNVD-2016-04092、CNVD-2016-04091、CNVD-2016-04090、CNVD-2016-04089、CNVD-2016-04040）、Apache Struts 1 跨站脚本漏洞、Apache Struts 1 存在多个漏洞。其中“Apache Struts2 远程代码执行漏洞（CNVD-2016-04040）”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-2016-04093
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04092
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04091
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04090
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04089
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04040
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03940
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03936

3、Google 产品安全漏洞

Android 是美国谷歌（Google）公司和开放手持设备联盟（简称 OHA）共同开发的一套以 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，攻击者可利用漏洞以提升的权限执行任意代码。

CNVD 收录的相关漏洞包括：Android Mediaserver 提权漏洞（CNVD-2016-03926、CNVD-2016-03925、CNVD-2016-03924、CNVD-2016-03923）、Android Mediaserver 权限提升漏洞（CNVD-2016-03964、CNVD-2016-03965、CNVD-2016-03966、CNVD-2016-03967）。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-2016-03926
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03925
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03924
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03923

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03964

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03965

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03966

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03967

4、Mozilla 产品安全漏洞

Mozilla Firefox 和 Firefox ESR 都是美国 Mozilla 基金会开发的浏览器产品。Firefox 是一款开源 Web 浏览器；Firefox ESR 是 Firefox 的一个延长支持版本。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息、发起拒绝服务攻击、实施跨站脚本攻击等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 和 Firefox ESR ANGLE 拒绝服务漏洞、Mozilla Firefox 和 Firefox ESR 权限获取漏洞、Mozilla Firefox 和 Firefox ESR 拒绝服务漏洞（CNVD-2016-04024）、Mozilla Firefox 跨站脚本漏洞（CNVD-2016-03997）、Mozilla Firefox 信息泄露漏洞（CNVD-2016-03998）、Mozilla Firefox 未授权访问漏洞、Mozilla Firefox 拒绝服务漏洞（CNVD-2016-04002）、Mozilla Firefox 和 Firefox ESR 缓冲区溢出漏洞（CNVD-2016-03987）。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-2016-04026

http://www.cnvd.org.cn/flaw/show/CNVD-2016-04025

http://www.cnvd.org.cn/flaw/show/CNVD-2016-04024

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03997

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03998

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03999

http://www.cnvd.org.cn/flaw/show/CNVD-2016-04002

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03987

5、Cisco RV110W/RV130W/RV215W 路由器远程代码执行漏洞

Cisco RV130W Wireless-N 是一款多功能 VPN 路由器；Cisco RV110W/RV215W 是集有线/无线网络连接、VPN、防火墙等功能于一身的路由器。本周，Cisco RV110W/RV130W/RV215W 路由器被披露存在远程代码执行漏洞。允许攻击者利用漏洞在目标系统执行任意代码。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-2016-04096

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-201	NTP.org ntpd 拒绝服务漏洞	高	目前厂商已经发布了升级补丁以修

6-03927			复此安全问题，补丁获取链接：http://support.ntp.org/bin/view/Main/NtpBug3046
CNVD-2016-03929	GNU C Library clntudp_call 函数栈缓冲区溢出漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://sourceware.org/bugzilla/show_bug.cgi?id=20112
CNVD-2016-03933	HUAWEI VP9660 和 RSE6500 畸形报文缓冲区溢出漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：http://www.huawei.com/cn/psirt/security-advisories/huawei-sa-20160601-01-videoconference-cn
CNVD-2016-03930	FonalityHUDweb for Google Chrome 插件任意代码执行漏洞	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.fonality.com/
CNVD-2016-03944	HPE Systems Insight Manager 拒绝服务漏洞	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://h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05131085
CNVD-2016-03946	HPE Insight Control server deployment 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://h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05150800
CNVD-2016-03955	IBM Domino KeyView PDF 过滤器堆缓冲区溢出漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：http://www.ibm.com/support/docview.wss?uid=swg21983292
CNVD-2016-03956	IBM Domino KeyView PDF 过滤器堆缓冲区溢出漏洞（CNVD-2016-03956）	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://www.ibm.com/support/docview.wss?uid=swg21983292
CNVD-2016-03954	IBM Domino KeyView PDF 过滤器堆缓冲区溢出漏洞（CNVD-2016-03954）	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://www.ibm.com/support/docview.wss?uid=swg21983292
CNVD-2016-03953	IBM Domino KeyView PDF 过滤器堆缓冲区溢出漏洞（CNVD-2016-03953）	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://www.ibm.com/support/docview.wss?uid=swg21983292

表 4 部分重要高危漏洞列表

小结：6 月 14 日，微软发布了 2016 年 6 月份的月度例行安全公告，共含 16 项更新，修复了 Microsoft Windows、Internet Explorer、Edge、Office、OfficeService 和 Web Apps 中存在的 36 个安全漏洞。其中，5 项远程代码更新的综合评级为最高级“严重”级别。利用上述漏洞，攻击者可提升权限，远程执行任意代码。此外，Apache、Google、Mozilla 等多款产品被披露存在多个安全漏洞，攻击者可利用漏洞获得敏感信息、获取访问权限、执行任意代码或发起拒绝服务攻击等。另外，Cisco RV110W/RV130W/RV215W 路由器被披露存在远程代码执行漏洞，允许攻击者利用漏洞在目标系统执行任意代码。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.Verizon 邮箱被爆漏洞，个人邮件可被转发到任意邮箱

Verizon 是美国三大电信巨头之一。最近 Verizon 的安全人员发现 Verizon 的邮箱系统存在一个高危漏洞，可以导致 Verizon 邮箱用户的邮件被任意转发到其它邮箱账户。

参考链接：http://www.freebuf.com/news/107089.html

2.Let’s Encrypt 泄露 7618 名用户邮箱地址

Let’s Encrypt 翻译成中文叫“让我们来加密”，实际上这是个为广大网站免费颁发 SSL/TLS 证书的项目。Let’s Encrypt 的来头不小，目前它是由 Linux 基金会托管的，发起该项目的组织包括 Mozilla、思科、EFF 等。这个项目对于 Web 世界由 HTTP 过渡到 HTTPS 是异常重要的。许多网站管理人员在享受这项服务的同时，还顺便订阅了 Let’s Encrypt 的简报。Let’s Encrypt 并没有选择自己给用户发邮件，而是找第三方服务代发。在这封简报邮件发出后，7618 名用户的邮件地址遭遇泄露。Let’s Encrypt ISRG 执行董事 Josh Aas 表示，这是系统中的 BUG 导致的。

参考链接：http://www.freebuf.com/news/106614.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