

国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2016 年 07 月 25 日-2016 年 07 月 31 日

2016年第31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 433 个，其中高危漏洞 159 个、中危漏洞 254 个、低危漏洞 20 个。漏洞平均分为 6.12 分。本周收录的漏洞中，涉及 0day 漏洞 108 个（占 25%）。其中互联网上出现“Barracuda Web App Firewall 和 Load Balancer 远程命令注入漏洞、Barracuda Networks Spam and Virus Firewall 远程命令注入漏洞”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 158 个，与上周（648 个）环比下降 76%。

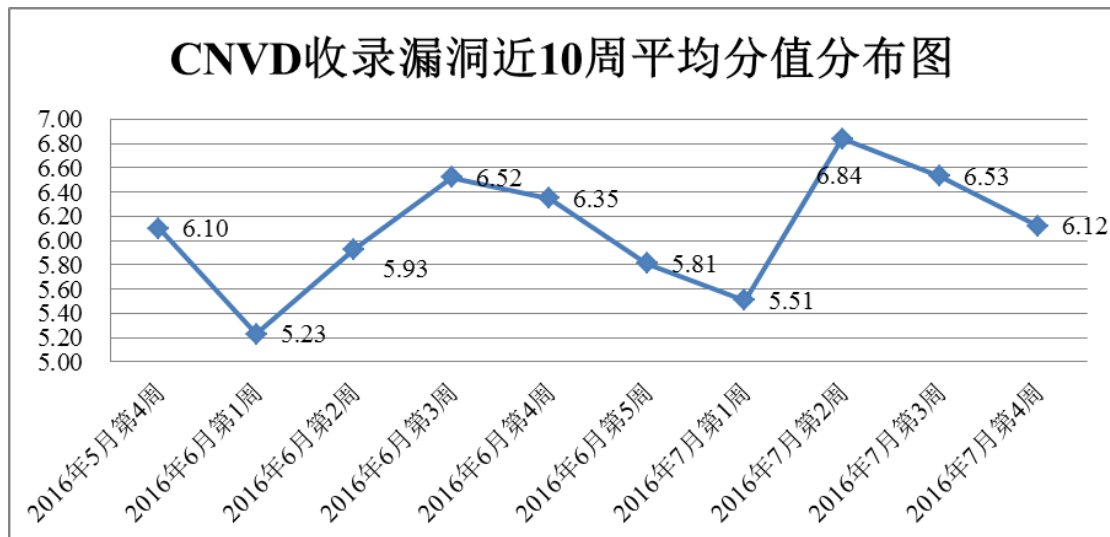


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 9 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 433 个漏洞。报送情况如表 1 所示。其中，天融信、绿盟科技、安天实验室、启明星辰等单位报送数量较多。漏洞盒子、深圳市深信服电子科技有限公司、中国科学院软件研究

所-总体部及其他个人白帽子向 CNVD 提交了 158 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	292	0
绿盟科技	262	0
安天实验室	249	0
启明星辰	200	4
恒安嘉新	91	5
H3C	66	0
杭州安恒信息技术有限公司	22	0
中国电信集团系统集成有限责任公司	25	0
东软	297	0
漏洞盒子	36	36
深圳市深信服电子科技有限公司	14	14
中国科学院软件研究所-总体部	12	12
CNCERT 上海分中心	16	16
CNCERT 陕西分中心	15	15
CNCERT 江西分中心	7	7
CNCERT 河南分中心	5	5
CNCERT 山西分中心	5	5
CNCERT 宁夏分中心	1	1
个人	38	38
报送总计	1653	158
录入总计	433（去重）	158

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 433 个漏洞。其中应用程序漏洞 274 个，web 应用漏洞 92 个，操作系统漏洞 26 个，数据库漏洞 22 个，网络设备漏洞 10 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	274
web 应用漏洞	92
操作系统漏洞	26
数据库漏洞	22
网络设备漏洞	10
安全产品漏洞	9

表 2 漏洞按影响类型统计表

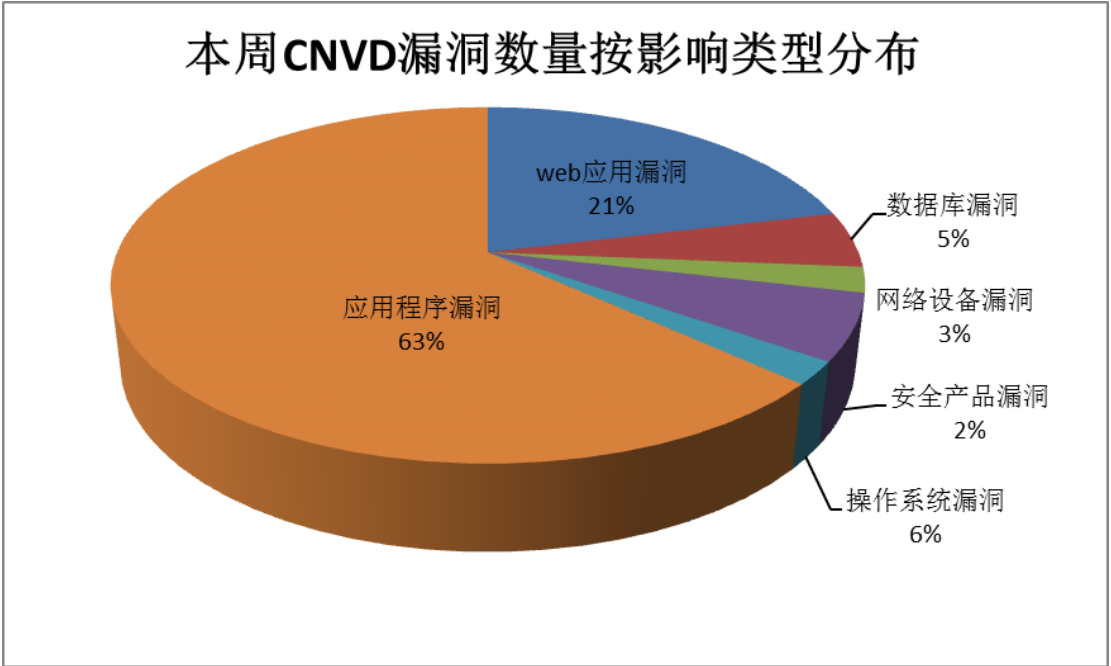


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、Google、Apple 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	177	41%
2	Google	19	4%
3	Apple	18	4%
4	PHP	11	3%
5	Drupal	10	2%
6	WordPress	10	2%

7	Cisco	5	1%
8	YPO3	5	1%
9	Siemens	4	1%
10	其他	174	41%

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 59 个电信行业漏洞，14 个移动互联网行业漏洞，6 个工控系统行业漏洞（如下图所示）。其中，“Oracle Fusion Middleware Outside In Technology 存在未明漏洞（CNVD-2016-05414、CNVD-2016-05415、CNVD-2016-05416、CNVD-2016-05417、CNVD-2016-05418、CNVD-2016-05419、CNVD-2016-05420、CNVD-2016-05421、CNVD-2016-05422、CNVD-2016-05423）、Apple Core Graphics BMP Framework img_decode_read 远程代码执行漏洞等”的综合评级为“高危”。详情请参照 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/>

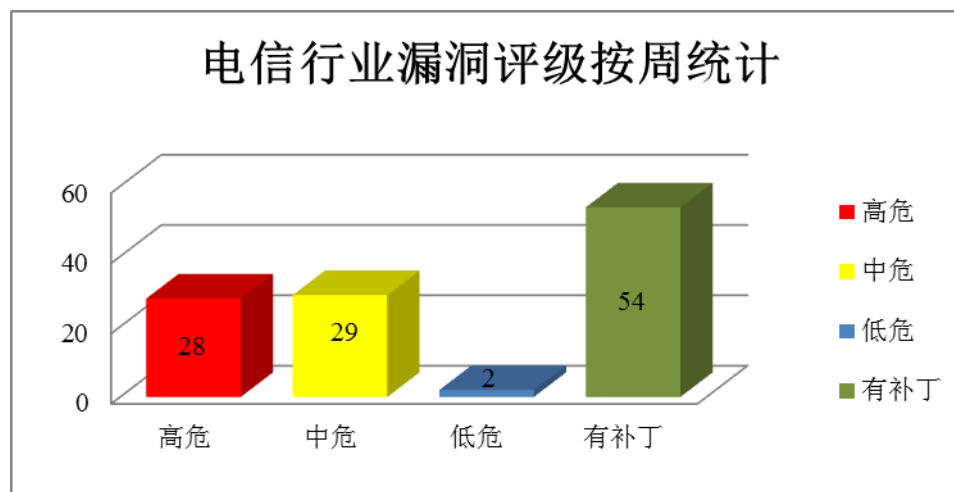


图 3 电信行业漏洞统计

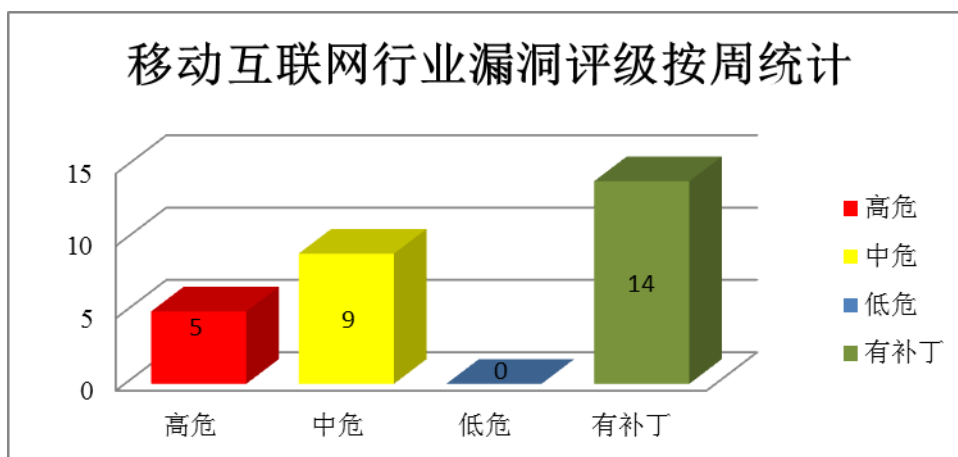


图 4 移动互联网行业漏洞统计

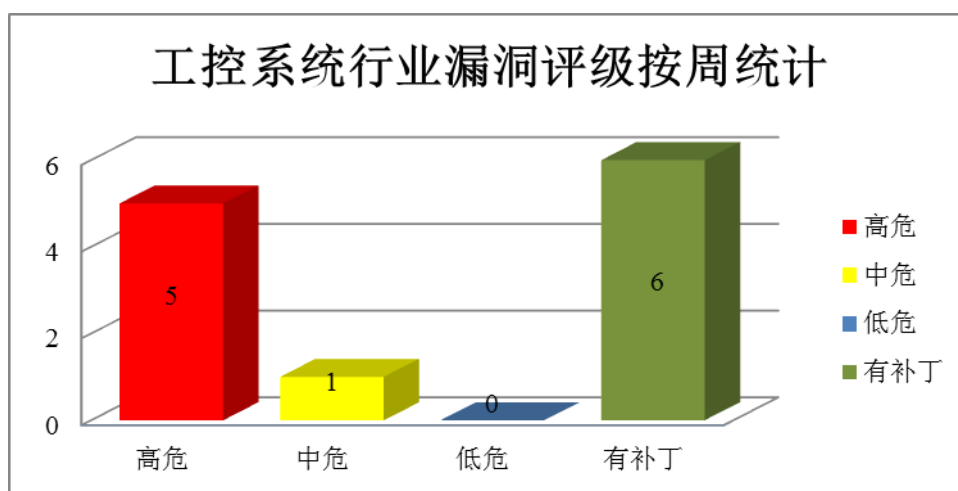


图 5 工控系统行业漏洞统计

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

Oracle MySQL Server 是一个轻量的关系型数据库系统。本周，该产品被披露存在未明漏洞，攻击者可利用漏洞影响可用性。

CNVD 收录的相关漏洞包括：Oracle MySQL Server 存在未明漏洞（CNVD-2016-05386、CNVD-2016-05387、CNVD-2016-05388、CNVD-2016-05389、CNVD-2016-05390、CNVD-2016-05391、CNVD-2016-05392、CNVD-2016-05393）等。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-2016-05386>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05387>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05388>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05389>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05390>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05391>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05392>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05393>

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，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞获取敏感信息或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Google Chrome 拒绝服务漏洞（CNVD-2016-05481）、Google Chrome V8 内存破坏漏洞（CNVD-2016-05586）、Google Chrome PAC 功能信息泄露漏洞、Google Chrome OS 堆缓冲区溢出漏洞、Google Chrome libxml2 内存错误引用漏洞、Google Chrome Extensions 子系统拒绝服务漏洞、Google Chrome CSPSource::schemeMatches 信息泄露漏洞、Google Chrome 'ByteArray::Get'方法堆缓冲区溢出漏洞等。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-2016-05481>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05586>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05594>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05690>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05639>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05515>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05597>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05518>

3、Apple 产品安全漏洞

Apple iOS、OS X、tvOS 和 watchOS 都是美国苹果（Apple）公司的产品。Apple iOS 是为移动设备所开发的一套操作系统；OS X 是为 Mac 计算机所开发的一套专用操作系统；tvOS 是一套智能电视操作系统；watchOS 是一套智能手表操作系统。kernel 是其中的一个内核组件。Safari 是一款 Web 浏览器，是 Mac OS X 和 iOS 操作系统附带的默认浏览器；WebKit 是 KDE 社区开发的一套开源 Web 浏览器引擎，目前被 Apple Safari 及 Google Chrome 等浏览器使用。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞泄露敏感信息、进行跨站脚本攻击或造成内存破坏等。

CNVD 收录的相关漏洞包括：多款 Apple 产品跨站脚本漏洞、多款 Apple 产品内存破坏漏洞（CNVD-2016-05667）、多款 Apple 产品 kernel 内存破坏漏洞（CNVD-2016-05665、CNVD-2016-05663）、多款 Apple 产品 WebKit 内存破坏漏洞（CNVD-2016-05672、CNVD-2016-05671、CNVD-2016-05669）、多款 Apple 产品 WebKit 信息泄露漏洞等。其

中，“多款 Apple 产品 kernel 内存破坏漏洞（CNVD-2016-05665、CNVD-2016-05663）”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-2016-05668>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05667>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05665>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05663>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05672>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05671>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05670>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05669>

4、PHP 产品安全漏洞

PHP 是广泛使用的通用目的脚本语言，特别适合于 Web 开发，可嵌入到 HTML 中。本周，该产品被披露存在远程代码执行、信息泄露和拒绝服务漏洞，攻击者可利用漏洞执行远程代码、获取敏感信息和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：PHP 远程代码执行漏洞（CNVD-2016-05253）、PHP virtual_file_ex 拒绝服务漏洞、PHP php_url_parse_ex 拒绝服务漏洞、PHP locale_accept_from_http 拒绝服务漏洞、PHP ext/snmp/snmp.c 拒绝服务漏洞、PHP ext/session/session.c 拒绝服务漏洞、PHP exif_process_user_comment 拒绝服务漏洞、PHP exif_process_IFD_in_MAKERNOTE 信息泄露漏洞等。其中，PHP 远程代码执行漏洞（CNVD-2016-05253）的综合评级为“高危”。目前，除“PHP 远程代码执行漏洞（CNVD-2016-05253）”外，厂商已发布其余漏洞的补丁程序。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-2016-05253>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05566>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05564>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05569>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05570>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05565>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05568>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05567>

5、Barracuda Web App Firewall 和 Load Balancer 远程命令注入漏洞

Barracuda Web Application Firewall 和 Load Balancer 都是美国梭子鱼（Barracuda Networks）公司的产品。前者是一款 Web 应用防火墙，后者是一款应用交付控制器。本周，Barracuda Web App Firewall 和 Load Balancer 被披露存在远程命令注入漏洞。攻

击者可利用该漏洞在受影响设备上下文中执行任意命令。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-2016-05692>

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-2016-05250	Accel-PPP 远程内存破坏漏洞	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://sourceforge.net/projects/accel-ppp/
CNVD-2016-05257	Pulse Secure Desktop Client 权限提升漏洞	高	厂商已在最新版本中修复该漏洞，请及时关注更新： https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA40241
CNVD-2016-05259	Drupal Scald File 模块远程代码执行漏洞	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://drupal.org/
CNVD-2016-05491	Veil-Evasion RPC 命令注入漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页： https://www.veil-framework.com/
CNVD-2016-05366	WordPress Video Player SQL 注入漏洞	高	用户可联系供应商获得补丁信息： https://www.wordpress.org/
CNVD-2016-05381	Zen Cart 'admin_account.php' 远程权限提升漏洞	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.zen-cart.com/
CNVD-2016-05458	op5 Monitor 'cmd_str' 参数远程命令执行漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： https://www.op5.com/blog/news/op5-monitor-7-2-0-release-notes/
CNVD-2016-05258	TYPO3 'Another Simple Gallery' 扩展 SQL 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，详情请关注厂商主页： https://typo3.com/
CNVD-2016-05477	IPFire 存在多个漏洞	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.ipfire.org/

CNVD-2016-05456	TYPO3 'http:BL Blocking'扩展存在多个漏洞	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://typo3.com/
-----------------	----------------------------------	---	---

表 4 部分重要高危漏洞列表

小结：本周，Oracle 产品被披露存在未明漏洞，攻击者可利用漏洞影响可用性。此外，Google、Apple、PHP 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取敏感信息、进行跨站脚本攻击和发起拒绝服务攻击等。另外，Barracuda Web App Firewall 和 Load Balancer 被披露存在远程命令注入漏洞。攻击者可利用该漏洞在受影响设备上下文中执行任意命令。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. 大量无线键盘存在 KeySniffer 漏洞，可嗅探用户输入

本周，大量无线键盘存在 KeySniffer 漏洞。存在漏洞的键盘与插入电脑的 USB 无线接收器之间的数据都是明文传输的。这样攻击者就能够检测到受害用户输入的文字了。也正由于没有加密，攻击者还能够在数据流中注入他们自己的键盘敲击。KeySniffer 攻击使用了逆向工程收发器的技术。KeySniffer 漏洞无法通过补丁修复。因此，建议广大用户们还是换个好一点的蓝牙键盘，或者索性换成有线键盘吧。

参考链接：<http://www.freebuf.com/vuls/110265.html>

2. LastPass 再曝多枚高危漏洞，用户账号信息存在被盗风险

LastPass 是全球最流行的云密码管理工具之一。这款工具主打用户的互联网账号和密码管理，和 1Pass 很相似。在 PC 端，用户可以使用 LastPass 提供的浏览器插件对自己的账号密码进行管理，在手机端则是 APP。来自 Google Project Zero 的研究人员 Tavis Ormandy 目前发现了几个 LastPass 0day 漏洞。LastPass 目前已经紧急修补了该漏洞，也没有公开漏洞细节。这里有一些情况我们不得为知。2016 年 7 月 27 日，某位安全研究人员发现了一枚 LastPass 的命令执行漏洞。LastPass 在信息通讯的过程中，会对 JS 代码做一个可信验证。LastPass 目前已经修复该漏洞，并且发表声明称这个漏洞只会影响到火狐的 LastPass 插件。

参考链接：<http://www.freebuf.com/news/110378.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