国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2017 年 01 月 02 日-2017 年 01 月 08 日 **2017 年第 2 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 101 个，其中高危漏洞 42 个、中危漏洞 52 个、低危漏洞 7 个。漏洞平均分值为 6.29。本周收录的漏洞中，涉及 0day 漏洞 13 个（占 13%）。其中互联网上出现“Joomla!组件 Blog Calendar SQL 注入漏洞、Wampserver 不安全的文件权限提升漏洞”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 511 个，与上周（547 个）环比下降 7%。

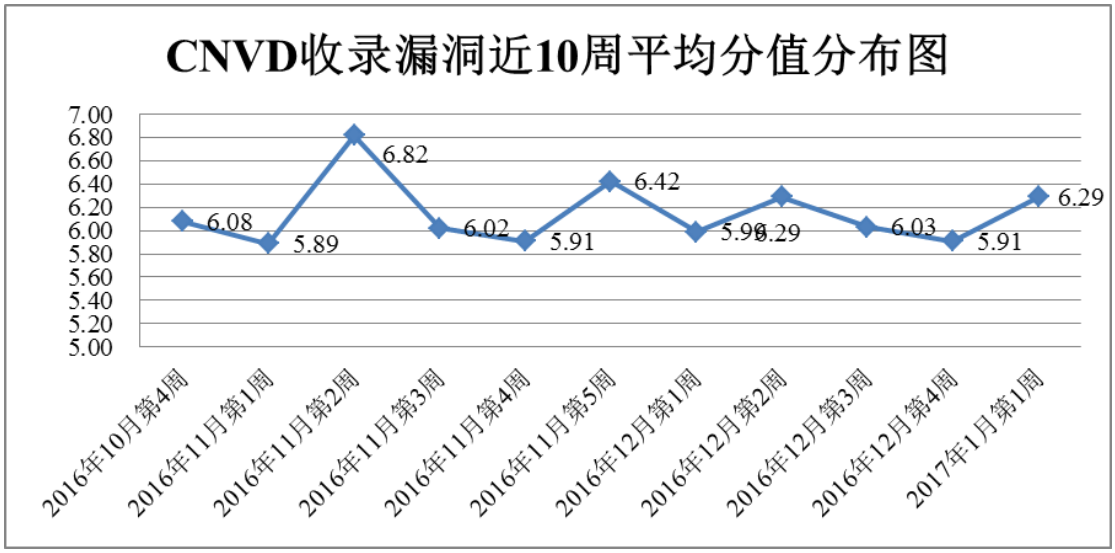

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 11 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 101 个漏洞。报送情况如表 1 所示。其中，安天实验室、启明星辰、蓝盾信息安全技术股份有限公司、天融信等单位报送数量较多。360 网神、漏洞盒子、清远职业技术学院、广

西鑫瀚科技有限公司、上海零盾网络科技有限公司、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 511 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	364	364
安天实验室	118	0
启明星辰	89	49
蓝盾信息安全技术股份有限公司	74	0
天融信	73	0
华为技术有限公司	62	0
中国电信集团系统集成有限责任公司	40	0
恒安嘉新	39	0
H3C	38	0
南京铱迅信息技术股份有限公司	2	2
北京数字观星科技有限公司	1	0
漏洞盒子	25	25
清远职业技术学院	6	6
广西鑫瀚科技有限公司	5	5
上海零盾网络科技有限公司	1	1
广州神月信息安全技术有限公司	1	1
CNCERT 宁夏分中心	1	1
个人	57	57
报送总计	996	511
录入总计	101（去重）	511

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 101 个漏洞。其中应用程序漏洞 62 个， web 应用漏洞 16 个，操作系统漏洞 12 个，网络设备漏洞 9 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	62
web 应用漏洞	16
操作系统漏洞	12
网络设备漏洞	9
安全产品漏洞	2

表 2 漏洞按影响类型统计表

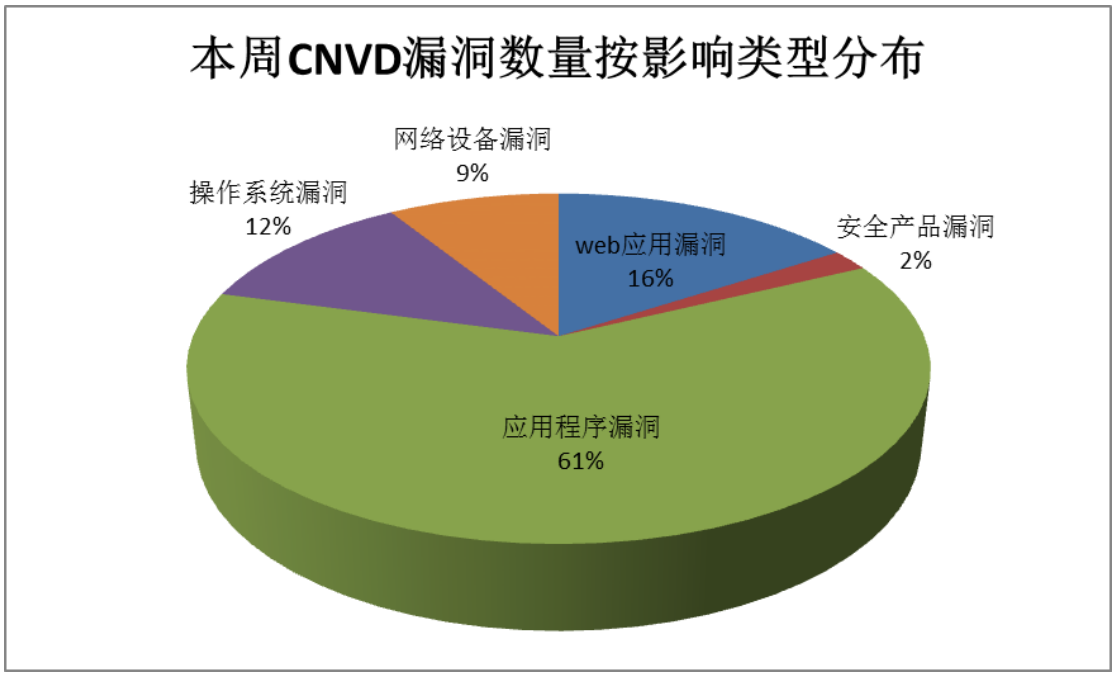

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、IBM、GStreamer 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	14	14%
2	IBM	10	10%
3	GStreamer	6	6%
4	ImageMagick	5	5%
5	PHP	4	4%
6	Piwigo	4	4%

7	WordPress	4	4%
8	NETGEAR	3	3%
9	DELL	2	2%
10	其他	49	49%

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 3 个电信行业漏洞，12 个移动互联网行业漏洞（如下图所示）。其中，“Google Nexus NVIDIA GPU Driver 权限提升漏洞（CNVD-2017-00179）、Google Android Qualcomm Video Driver 权限提升漏洞、Google Android Qualcomm GPU 驱动程序权限提升漏洞、Google Android 权限提升漏洞（CNVD-2017-00162、CNVD-2017-00160）”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/

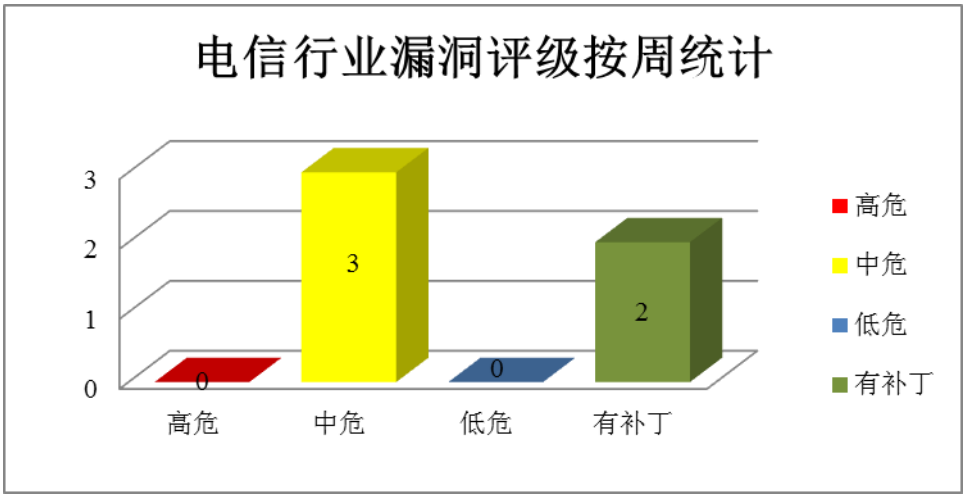

图 3 电信行业漏洞统计

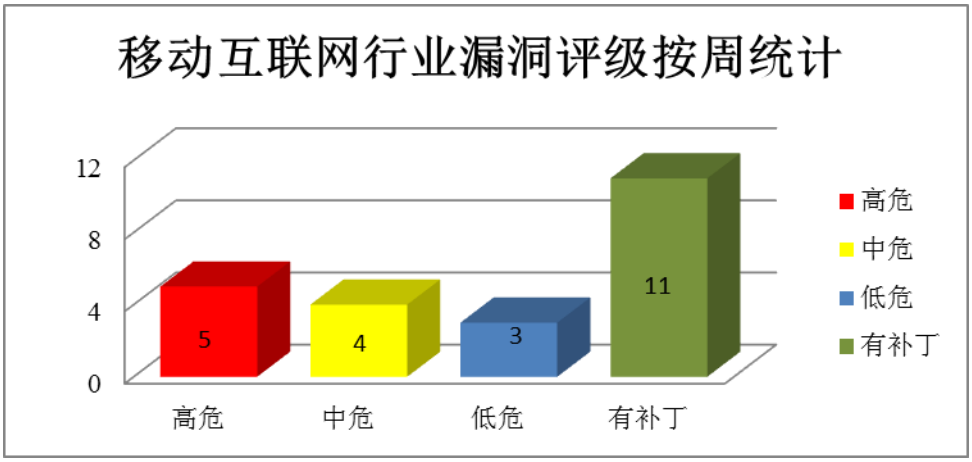

图 4 移动互联网行业漏洞统计

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、 phpmailer 以及其他 mailer 组件安全漏洞

PHPMailer 是一个用于发送电子邮件的 PHP 类库。SwiftMailer 是一个用于发送电子邮件的 PHP 函数包。Zend Framework（ZF）是美国 Zend 公司开发的一套开源的 PHP5 开发框架。上述产品被披露存在代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：PHPMailer 远程代码执行漏洞、PHPMailer 远程代码执行漏洞（CNVD-2017-00052）、SwiftMailer 远程代码执行漏洞、Zend Framework 'zend-mail'组件远程代码执行漏洞。除“PHPMailer 远程代码执行漏洞”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-2016-13107
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00052
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00012
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00047

2、 Google 产品安全漏洞

Google Nexus 是美国谷歌（Google）公司的智能设备。Google Pixel C 是一款平板电脑。NVIDIA GPU 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。Qualcomm GPU Driver 是使用在其中的一个美国高通（Qualcomm）公司开发的图形处理器驱动程序。本周，上述产品被披露存在权限提升漏洞，攻击者可利用漏洞获取提升的权限。

CNVD 收录的相关漏洞包括：Google Nexus Qualcomm Camera Driver 权限提升漏洞（CNVD-2017-00173、CNVD-2017-00174）、Google Pixel NVIDIA GPU Driver 权限提升漏洞、Google Pixel NVIDIA GPU Driver 权限提升漏洞（CNVD-2017-00175）、Go

ogle Android Qualcomm Video Driver 权限提升漏洞、Google Android Qualcomm GPU 驱动程序权限提升漏洞、Google Android 权限提升漏洞（CNVD-2017-00162、CNVD-2017-00160）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-2017-00173
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00174
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00176
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00175
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00180
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00163
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00162
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00160

3、IBM 产品安全漏洞

IBM UrbanCode Deploy 是美国 IBM 公司的一套应用自动化部署工具。IBM Security AppScan Source 是一套 Web 应用的安全测试工具。IBM WebSphere Application Server（WAS）是一款应用服务器产品，IBM License Metric Tool 是一套可帮助客户决定其处理器价值单元（PVU）许可需求的免费工具，BigFix Inventory 是一套用于软件控制和安全风险缓解的解决方案。IBM Security Guardium Database Activity Monitor 是一款数据库活动监控器产品。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞泄露敏感信息、执行任意代码或进行跨站脚本攻击等。

CNVD 收录的相关漏洞包括：IBM UrbanCode Deploy 信息泄露漏洞（CNVD-2017-00171）、IBM UrbanCode Deploy 远程代码执行漏洞、IBM Security AppScan Source 本地信息泄露漏洞、IBM WebSphere Application Server 跨站脚本漏洞、IBM License Metric Tool 和 BigFix Inventory XML 外部实体注入漏洞、IBM License Metric Tool 和 BigFix Inventory 信息泄露漏洞、IBM Security Guardium Database Activity Monitor 本地命令注入漏洞（CNVD-2017-00060）、IBM License Metric Tool 和 BigFix Inventory 开放重定向漏洞等。其中，“IBM UrbanCode Deploy 远程代码执行漏洞、IBM License Metric Tool 和 BigFix Inventory XML 外部实体注入漏洞、IBM Security Guardium Database Activity Monitor 本地命令注入漏洞（CNVD-2017-00060）、IBM License Metric Tool 和 BigFix Inventory 开放重定向漏洞”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-2017-00171
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00170
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00169

http://www.cnvd.org.cn/flaw/show/CNVD-2017-00076

http://www.cnvd.org.cn/flaw/show/CNVD-2017-00063

http://www.cnvd.org.cn/flaw/show/CNVD-2017-00059

http://www.cnvd.org.cn/flaw/show/CNVD-2017-00060

http://www.cnvd.org.cn/flaw/show/CNVD-2017-00051

4、GStreamer 产品安全漏洞

GStreamer 是一套用于处理流媒体的框架。BadPlug-ins 是一个解码组件。Good Plug-ins 是一个用于提高代码质量的组件。本周，上述产品被披露存在拒绝服务漏洞，攻击者可利用漏洞发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Gstreamer 拒绝服务漏洞、Gstreamer 拒绝服务漏洞（CNVD-2017-00123）、GStreamer Bad Plug-ins 拒绝服务漏洞（CNVD-2017-00121、CNVD-2017-00122）、GStreamer Bad Plug-ins 拒绝服务漏洞、GStreamer Good Plug-ins 拒绝服务漏洞。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-2017-00124

http://www.cnvd.org.cn/flaw/show/CNVD-2017-00123

http://www.cnvd.org.cn/flaw/show/CNVD-2017-00121

http://www.cnvd.org.cn/flaw/show/CNVD-2017-00122

http://www.cnvd.org.cn/flaw/show/CNVD-2017-00056

http://www.cnvd.org.cn/flaw/show/CNVD-2017-00057

5、Wampserver 不安全的文件权限提升漏洞

WampServer 是 Windos Apache Mysql PHP 集成安装环境。本周，WampServer 被披露存在不安全的文件权限提升漏洞。攻击者可以利用该漏洞获取系统管理员权限。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-2017-00019

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-2017-00072	ImageMagick 缓冲区溢出漏洞（CNVD-2017-00072）	高	用户可联系供应商获得补丁信息：http://www.imagemagick.org/
CNVD-2017-00048	WordPress 插件 Slider Templatic Tevolution 任意文件上传漏洞	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://templatic.com/wordpress-plugins/tevolution
CNVD-201	ImageMagick 缓冲区溢出漏洞	高	用户可联系供应商获得补丁信息：

7-00073	（CNVD-2017-00073）		http://www.imagemagick.org/
CNVD-2017-00069	PHP Standard PHP Library 内存错误引用漏洞	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://github.com/php/php-src/commit/bcd64a9bdd8afcf7f91a12e700d12d12eedc136b
CNVD-2017-00064	LibVNCServer 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，详情请关注厂商主页：http://libvnc.github.io/
CNVD-2017-00065	LibVNCServer 堆缓冲区溢出漏洞（CNVD-2017-00065）	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://libvnc.github.io/
CNVD-2017-00081	多个 Quick Heal 产品缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://www.quickheal.co.in/
CNVD-2017-00083	Shutter 任意命令执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://shutter-project.org/
CNVD-2017-00111	Lenovo Transition 本地权限提升漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.lenovo.com/us/zh/product_security/LEN-12508
CNVD-2017-00118	Serendipity 任意文件包含漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/s9y/Serendipity/commit/bba6a840f4d53cbaf62971a3078a98c8ddf92b85

表 4 部分重要高危漏洞列表

小结：phpmailer 以及其他 mailer 组件被披露存在代码执行漏洞，攻击者可利用漏洞执行任意代码。此外，Google、IBM、GStreamer 等多款产品被披露存在多个安全漏洞，攻击者利用漏洞可泄露敏感信息、绕过安全限制、执行任意代码或发起拒绝服务攻击等。另外，WampServer 被披露存在不安全的文件权限提升漏洞。攻击者可以利用该漏洞获取系统管理员权限。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. PhpMailer、SwiftMailer、ZendMail 接连曝 RCE 高危漏洞，影响数百万 Web 服务器

研究人员最近发现了一个存在于 3 个常见开源 PHP 库中的高危(Critical)漏洞，黑客可以利用这个漏洞远程执行任意命令，存在漏洞的 PHP 库包括 SwiftMailer、PhpMailer 和 ZendMail。来自波兰的研究员 Dawid Golunski 前一阵就披露了存在于 PHPMailer 中的漏洞(CVE-2016-10033)，该漏洞利用程序对参数过滤的不完善，来执行任意代码。利用新版本中的冲突问题，研究人员再次绕过了 5.2.18 版 PHPMailer 中的安全措施，因此申请了一个新的漏洞编号(CVE-2016-10045)。这一次漏洞波及范围更大，包括众多开源的 web 应用如 WordPress, Drupal, 1CRM, SugarCRM, Yii 和 Joomla 都可能遭到攻击。

参考链接：http://www.freebuf.com/news/124492.html

2. iOS 10 iMessage 字符崩溃 Bug 又来了

近日，黑客@vincedes3 发现了一个从 iOS 8 到 iOS 10.2.1 b2 通用的 iMessage 字符崩溃 Bug，该 Bug 同样利用了和当年 iOS 8 的 iMessage 短信 Bug 的类似手法，将一段恶意代码发送给受害者，在受害者打开短信的时候，触发了大量能够引起短信程序崩溃的字符，当用户浏览该短信的时候，cpu 进行了大量的计算直到短信 app 点不动。当用户关掉短信程序后，再次打开短信程序，系统试图加载上一次内容，依然会触发该 bug。

参考链接：http://www.freebuf.com/news/124291.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