国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2017 年 12 月 25 日-2017 年 12 月 31 日 **2017 年第 53 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 294 个，其中高危漏洞 91 个、中危漏洞 162 个、低危漏洞 41 个。漏洞平均分值为 5.78 本周收录的漏洞中，涉及 0day 漏洞 64 个（占 22%），其中互联网上出现“GPWeb 任意文件上传漏洞”等零日代码攻击漏洞。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 610 个，与上周（466 个）环比减少 24%。

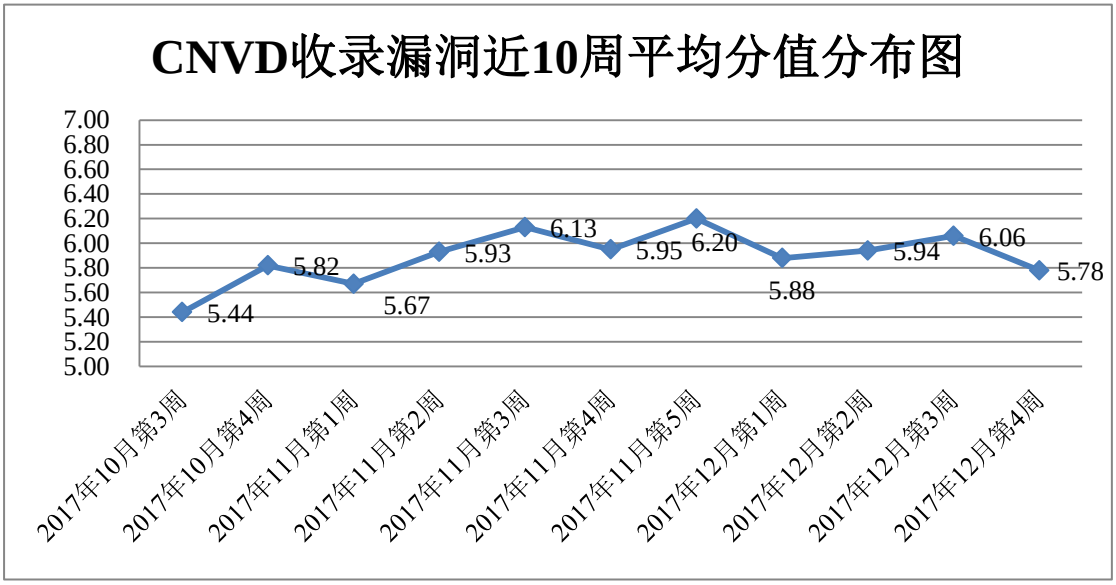

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞事件处置情况

本周，CNVD 向基础电信企业通报漏洞事件 22 起，向银行、证券、保险、能源等重要行业单位通报漏洞事件 34 起，协调 CNCERT 各分中心验证和处置涉及地方重要部门漏洞事件 319 起，协调教育行业应急组织验证和处置高校科研院所系统漏洞事件 55 起，向国家上级信息安全协调机构上报涉及部委门户、子站或直属单位信息系统漏洞事

件 32 起。

此外，CNVD 通过已建立的联系机制或涉事单位公开联系渠道向以下单位通报了其信息系统或软硬件产品存在的漏洞，具体处置单位情况如下所示：

广州光大教育软件科技股份有限公司、上海顶想信息科技有限公司、航天信息股份有限公司、江苏远古信息技术有限公司、成都龙兵科技有限公司、广州商淘信息科技有限公司、中国建筑工程总公司、北京百容千域软件技术开发有限公司、长沙米拓信息技术有限公司、广州智选网络科技有限公司、合肥盈云信息科技有限公司、武汉贝云网络科技有限公司、南昌市驰硕网络科技有限公司、北京一诺互联科技有限公司、中粮集团有限公司、上海乐乎网络科技有限公司、苏州朗业网络科技有限公司、福建讯盟软件有限公司、济南爱程网络科技有限公司、北京昂道网络科技有限公司、内蒙古百佳信科技有限公司、雷风影视、SeaCMS、SemCms、中国科学技术学会、Catfish CMS、MacCMS、中国感光学会光催化专业委员会、追格、5068 儿童网。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，华为技术有限公司、天融信、安天实验室、H3C、启明星辰等单位报送数量较多。四川虹微技术有限公司（子午攻防实验室）、中新网络信息安全股份有限公司、北京智游网安科技有限公司、漏斗社区、福建省海峡信息技术公司及其他个人白帽子向 CNVD 提交了 610 个以事件型漏洞为主的原创漏洞。

表 1 漏洞报送情况统计表

报送单位或个人	漏洞报送数量	原创漏洞数量
华为技术有限公司	201	0
漏洞盒子	179	179
天融信	148	2
安天实验室	143	0
H3C	128	0
网神	122	122
启明星辰	69	0
杭州安恒信息技术有限公司	51	2
绿盟科技	49	0

中国电信集团系统集成有限责任公司	43	0
恒安嘉新	36	0
卫士通信息产业股份有限公司	13	0
南京铱迅信息技术股份有限公司	2	2
四川虹微技术有限公司（子午攻防实验室）	9	9
中新网络信息安全股份有限公司	6	6
北京智游网安科技有限公司	3	3
漏斗社区	3	3
福建省海峡信息技术公司	1	1
江西分中心	12	12
重庆分中心	11	11
福建分中心	8	8
上海分中心	7	7
贵州分中心	6	6
山西分中心	6	6
陕西分中心	3	3
湖南分中心	2	2
吉林分中心	1	1
个人	225	225
报送总计	1487	610

本周漏洞按类型和厂商统计

本周，CNVD 收录了 294 个漏洞。其中应用程序漏洞 138 个，网络设备漏洞 62 个，web 应用漏洞 41 个，操作系统漏洞 30 个，安全产品漏洞 21 个，数据库漏洞 2 个。

表 2 漏洞按影响类型统计表

漏洞影响对象类型	漏洞数量
应用程序漏洞	138
网络设备漏洞	62
web 应用漏洞	41
操作系统漏洞	30
安全产品漏洞	21
数据库漏洞	2

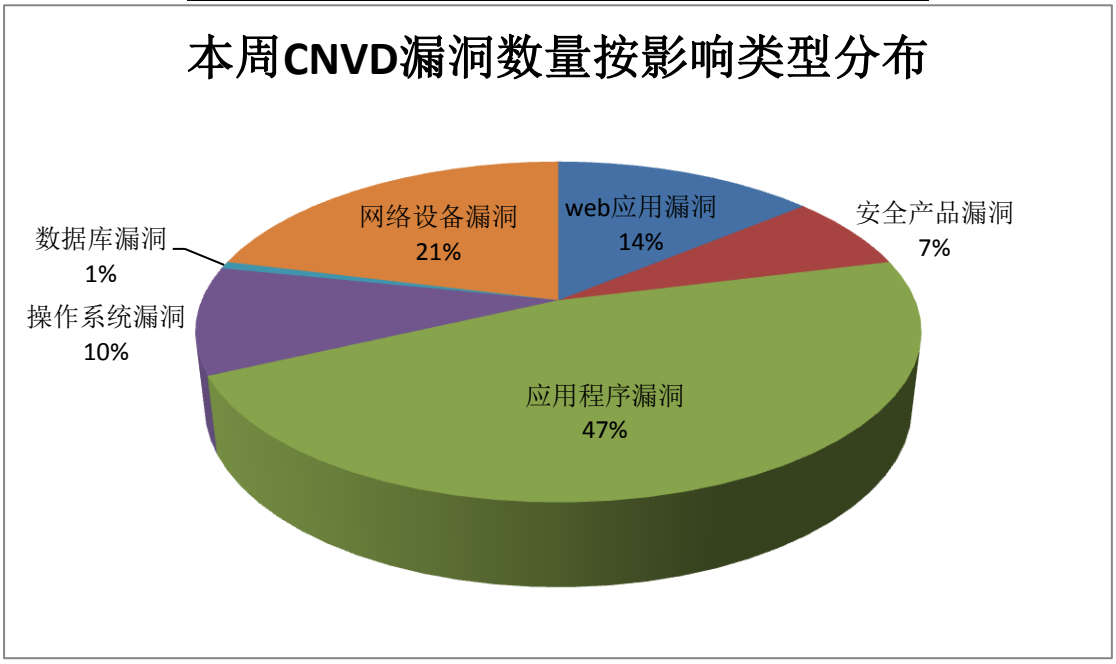

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Huawei、Linux、Nasm 等多家厂商的产品，部分漏洞数量按厂商统计如表 3 所示。

表 3 漏洞产品涉及厂商分布统计表

序号	厂商（产品）	漏洞数量	所占比例
1	Huawei	44	15%
2	Linux	12	4%
3	Nasm	11	4%
4	Google	10	3%
5	Piwigo	9	3%
6	IBM	9	3%
7	TG Soft	8	3%
8	TP-Link	7	2%
9	IKARUS Security Software	7	2%

10	其他	177	61%

本周行业漏洞收录情况

本周，CNVD 收录了 18 个电信行业漏洞，20 个移动互联网行业漏洞，1 个工控行业漏洞（如下图所示）。其中，“华为多款产品内存泄露漏洞、多款 HP 产品远程代码执行漏洞、美国网件 R7000 存在命令执行漏洞、多款 Apple 产品 WebKit 任意代码执行漏洞、Google Android Qualcomm 组件缓冲区溢出漏洞”等漏洞的综合评级为“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/

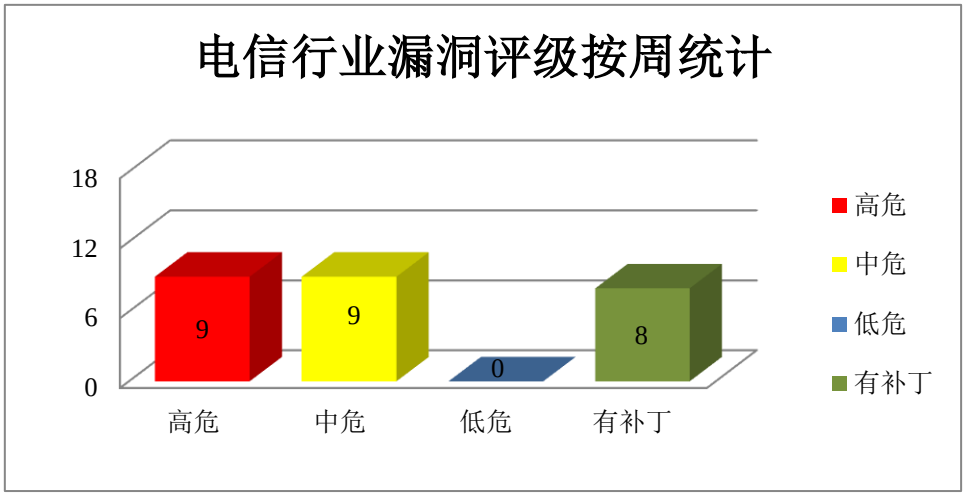

图 3 电信行业漏洞统计

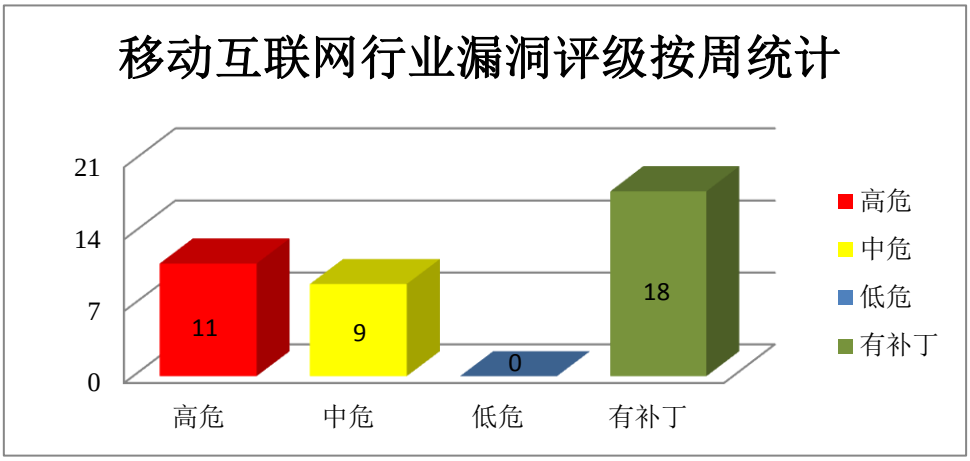

图 4 移动互联网行业漏洞统计

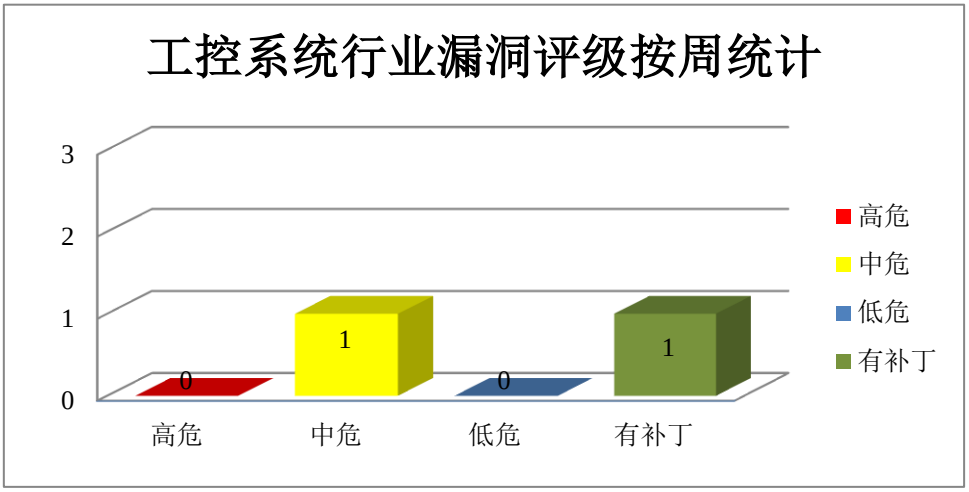

图 5 工控行业漏洞统计

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 on Google Pixel 和 Nexus 是美国谷歌公司的一套运行于 Google Pixel 和 Nexus 中并以 Linux 为基础的开源操作系统。本周，该产品被披露存在信息泄露、缓冲区溢出和内存错误引用漏洞，攻击者可利用漏洞获取敏感信息或执行任意代码等。

CNVD 收录的相关漏洞包括：Google Android Media framework 信息泄露漏洞（CNVD-2017-38460、CNVD-2017-38467）、Google Android Qualcomm 组件缓冲区溢出漏洞（CNVD-2017-38441、CNVD-2017-38442、CNVD-2017-38443）、Google Android Qualcomm 组件内存错误引用漏洞（CNVD-2017-38438、CNVD-2017-38439、CNVD-2017-38440）。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-2017-38460

http://www.cnvd.org.cn/flaw/show/CNVD-2017-38467

http://www.cnvd.org.cn/flaw/show/CNVD-2017-38441

http://www.cnvd.org.cn/flaw/show/CNVD-2017-38442

http://www.cnvd.org.cn/flaw/show/CNVD-2017-38443

http://www.cnvd.org.cn/flaw/show/CNVD-2017-38438

http://www.cnvd.org.cn/flaw/show/CNVD-2017-38439

http://www.cnvd.org.cn/flaw/show/CNVD-2017-38440

2、Linux 产品安全漏洞

Linux kernel 是一种计算机操作系统内核，以 C 语言和汇编语言写成，符合 POSIX 标准，按 GNU 通用公共许可证发行。本周，该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：Linux kernel 拒绝服务漏洞（CNVD-2017-38511、CNVD-2017-38512、CNVD-2017-38513、CNVD-2017-38514、CNVD-2017-38515、CNVD-2017-38516、CNVD-2017-38517、CNVD-2017-38518）。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-2017-38511

http://www.cnvd.org.cn/flaw/show/CNVD-2017-38512

http://www.cnvd.org.cn/flaw/show/CNVD-2017-38513

http://www.cnvd.org.cn/flaw/show/CNVD-2017-38514

http://www.cnvd.org.cn/flaw/show/CNVD-2017-38515

http://www.cnvd.org.cn/flaw/show/CNVD-2017-38516

http://www.cnvd.org.cn/flaw/show/CNVD-2017-38517

http://www.cnvd.org.cn/flaw/show/CNVD-2017-38518

3、Huawei 产品安全漏洞

Huawei DP300 是中国华为（Huawei）公司的一款视频会议终端。Huawei MT8-EMUI4.1、NTS-AL00、Mate 10 和 Mate 10 Pro 都是智能手机。Huawei FusionSphere OpenStack 是一套 FusionSphere 在 ICT 场景中的云平台软件。GaussDB 是其中的一个数据库。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、执行任意代码或发起拒绝服务等。

CNVD 收录的相关漏洞包括：Huawei DP300 CIDAM 协议输入校验漏洞（CNVD-2017-38106）、Huawei DP300 CIDAM 协议输入验证漏洞、Huawei DP300 CIDAM 协议输入验证漏洞（CNVD-2017-38104、CNVD-2017-38105）、Huawei FusionSphere OpenStack GaussDB 缓冲区溢出漏洞、多款 Huawei 产品 CIDAM 协议信息泄露漏洞、Huawei Mate 10 和 Mate 10 Pro 栈溢出漏洞、Huawei MT8-EMUI4.1 和 NTS-AL00 拒绝服务漏洞。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-2017-38106

http://www.cnvd.org.cn/flaw/show/CNVD-2017-38103

http://www.cnvd.org.cn/flaw/show/CNVD-2017-38104

http://www.cnvd.org.cn/flaw/show/CNVD-2017-38105

http://www.cnvd.org.cn/flaw/show/CNVD-2017-38271

http://www.cnvd.org.cn/flaw/show/CNVD-2017-38099

http://www.cnvd.org.cn/flaw/show/CNVD-2017-38110

http://www.cnvd.org.cn/flaw/show/CNVD-2017-38524

4、IKARUS Security Software 产品安全漏洞

IKARUS anti.virus 是奥地利 IKARUS Security Software 公司一套杀毒软件产品。本周，该产品被披露存在任意写入漏洞，攻击者可利用漏洞执行任意的写入操作。

CNVD 收录的相关漏洞包括：IKARUS anti.virus ntguard.sys 驱动程序任意写入漏洞、IKARUS anti.virus ntguard.sys 驱动程序任意写入漏洞（CNVD-2017-37946、CNVD-2017-37947、CNVD-2017-37948、CNVD-2017-37949、CNVD-2017-37950、CNVD-2017-37951）。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-2017-37945

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37946

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37947

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37948

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37949

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37950

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37951

5、多款 TP-Link 产品命令注入漏洞

TP-Link TL-WVR 等都是中国普联（TP-LINK）公司的无线路由器产品。本周，TP-Link 被披露存在命令注入漏洞，远程攻击者可通过向 cgi-bin/luci 发送 face 字段中带有 shell 元字符的 admin/diagnostic 命令利用该漏洞执行任意命令。目前，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 -2017-37952

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-2017-38230	Canonical Bazaar 命令执行漏洞	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://bazaar.canonical.com/en/
CNVD-2017-38234	Artica Web Proxy 跨站脚本漏洞	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://artica-proxy.com/
CNVD-2017-38254	Haxx curl 和 libcurl 缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://curl.haxx.se/docs/adv_2017-12e7.html
CNVD-2017-38255	Haxx curl 和 libcurl 拒绝服务漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://curl.haxx.se/docs/adv_2017-ae72.html
CNVD-201	Xen PoD P2M 错误处理不当	高	厂商已发布漏洞修复程序，请及时关

7-38299	漏洞		注更新：https://xenbits.xen.org/xsa/advisory-247.html
CNVD-2017-38338	Coremail 论客邮箱系统安卓版存在越权访问漏洞	高	厂商已提供漏洞修补方案，请关注厂商主页及时更新：http://www.lunkr.cn/
CNVD-2017-38341	美国网件 R7000 存在命令执行漏洞	高	R7000 v1.0.9.18 已修复此漏洞，建议用户下载使用：http://www.netgear.com.cn/
CNVD-2017-38434	Sony Media Go 不可信搜索路径漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://jvn.jp/en/jp/JVN08517069/index.html
CNVD-2017-38435	Sony Music Center for PC 不可信搜索路径漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://jvn.jp/en/jp/JVN08517069/index.html
CNVD-2017-38520	Ubiquiti UniFi Video 本地权限提升漏洞	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.ubnt.com/

表 4 部分重要高危漏洞列表

小结：本周，Google 被披露存在信息泄露、缓冲区溢出和内存错误引用漏洞，攻击者可利用漏洞获取敏感信息或执行任意代码等。此外，Linux、Huawei、IKARUS Security Software 等多款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、执行任意代码或发起拒绝服务攻击等。另外，TP-Link 被披露存在命令注入漏洞，远程攻击者可通过向 cgi-bin/luci 发送 face 字段中带有 shell 元字符的 admin/diagnostic 命令利用该漏洞执行任意命令。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。

本周重要漏洞攻击验证情况

本周，CNVD 建议注意防范以下已公开漏洞攻击验证情况。

1、多款 WordPress 插件跨站脚本漏洞

验证描述

WordPress 是 WordPress 软件基金会的一套使用 PHP 语言开发的博客平台，该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。WordPress Clockwork Free and Paid SMS Notifications 等都是使用在其中的不同类型的短信通知插件。

多款 WordPress 插件中的 Clockwork SMS clockwork-test-message.php 文件存在跨站脚本漏洞。远程攻击者可通过向 wp-admin/admin.php 文件发送带有特制‘to’参数的 cl

ockwork-test-message 请求利用该漏洞执行 JavaScript 代码。

验证信息

POC 链接：https://packetstormsecurity.com/files/145469/Clockwork-SMS-Cross-Site-Scripting.html

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD -2017-38121

信息提供者

恒安嘉新(北京)科技股份公司

注：以上验证信息(方法)可能带有攻击性，仅供安全研究之用。请广大用户加强对漏洞的防范工作，尽快下载相关补丁。

本周漏洞要闻速递

1. 僵尸网络 Mirai 最新变种 Satori ：利用 0day“绑架”华为家用路由器 HG532

时隔多日，2016 年 10 月开始活跃的 Mirai 僵尸网络创始人即便已经锒铛入狱，最近可能又将占据头条。之前在 12 月初，其最新的变种 Satori（觉醒）的“凌空出世”——Satori（觉醒）新僵尸网络出现，在过去的 12 个小时内已经激活超过 28 万个不同的 IP，而这两天对该事件的后续报道也正在进行。Check Point 安全研究人员在过去半个月内仔细观察了这次僵尸网络的感染过程，也观察到一些有趣的活动。这次的 Satori（觉醒），感染 IoT 的速度非常快，在极短的时间内就达到了数以万计的感染数量。研究人员认为名为 “Nexus Zeta” 的黑客创造了这次的 Mirai 变种 Satori 。

参考链接：http://www.freebuf.com/news/158116.html

2. 三星浏览器被爆高危同源策略绕过漏洞

近日，三星安卓浏览器被爆严重漏洞，该漏洞预装在数以亿计的三星安卓设备上，如受害者通过三星安卓浏览器访问黑客控制的网站，将被窃取私人敏感数据。而此次由 Dhiraj Mishra 发现的三星浏览器漏洞正是绕过了浏览器的同源策略，允许恶意网站读取非同源站点的用户数据，达到窃取敏感信息的目的。

参考链接：http://www.freebuf.com/news/158777.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：010-82991537