国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2017 年 02 月 27 日-2017 年 03 月 05 日 **2017 年第 10 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 229 个，其中高危漏洞 115 个、中危漏洞 101 个、低危漏洞 13 个。漏洞平均分值为 6.28。本周收录的漏洞中，涉及 0day 漏洞 73 个（占 32%）。其中互联网上出现“Netgear DGN2201 dnslookup.cgi 远程命令执行漏洞、WordPress Kama 插件 Click Counter SQL 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 347 个，与上周（504 个）环比下降 31%。

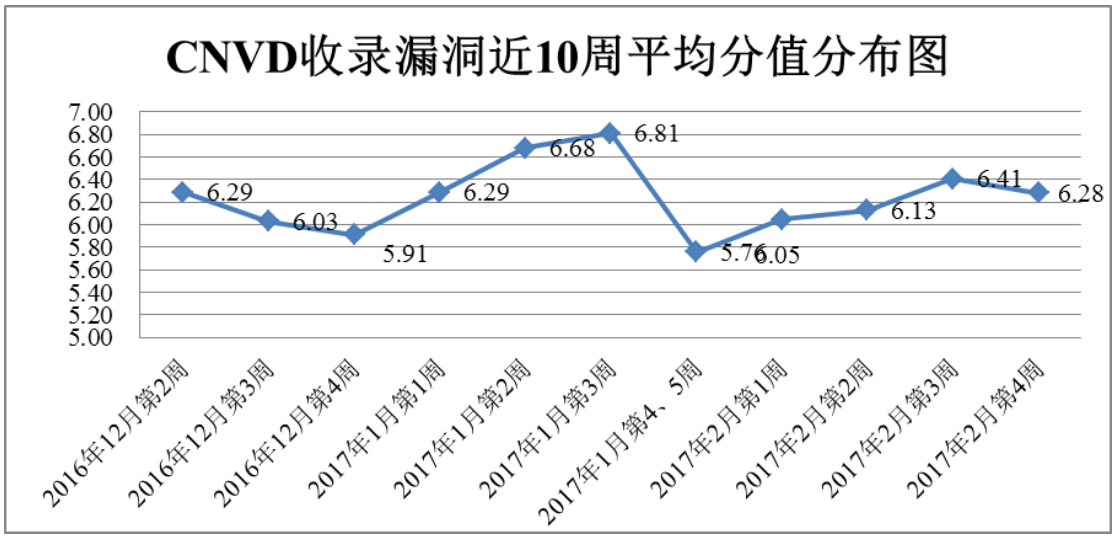

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 13 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 229 个漏洞。报送情况如表 1 所示。其中，安天实验室、启明星辰、天融信、华为技术有限公司等单位报送数量较多。漏洞盒子、广西鑫瀚科技有限公司、广州神月信息安全技

术有限公司、福建六壬网安股份有限公司、上海看雪科技有限公司及其他个人白帽子向 CNVD 提交了 347 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
安天实验室	132	0
启明星辰	100	0
天融信	111	1
华为技术有限公司	84	0
恒安嘉新	64	0
H3C	45	0
绿盟科技	39	0
安全狗	27	0
中国电信集团系统集成有限责任公司	25	0
杭州安恒信息技术有限公司	20	0
蓝盾信息安全技术有限公司	12	12
北京数字观星科技有限公司	5	0
深圳市深信服电子科技有限公司	1	1
漏洞盒子	220	220
广西鑫瀚科技有限公司	11	11
广州神月信息安全技术有限公司	2	2
福建六壬网安股份有限公司	1	1
上海看雪科技有限公司	1	1
CNCERT 福建分中心	16	16
CNCERT 上海分中心	13	13

CNCERT 吉林分中心	8	8
CNCERT 重庆分中心	5	5
CNCERT 四川分中心	4	4
CNCERT 广东分中心	4	4
CNCERT 安徽分中心	3	3
CNCERT 浙江分中心	2	2
CNCERT 新疆分中心	2	2
CNCERT 宁夏分中心	2	2
CNCERT 湖南分中心	1	1
CNCERT 贵州分中心	1	1
CNCERT 甘肃分中心	1	1
个人	36	36
报送总计	998	347
录入总计	229（去重）	347

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 229 个漏洞。其中应用程序漏洞 130 个，web 应用漏洞 88 个，网络设备漏洞 7 个，安全产品漏洞 2 个，操作系统漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	130
web 应用漏洞	88
网络设备漏洞	7
安全产品漏洞	2
操作系统漏洞	2

表 2 漏洞按影响类型统计表

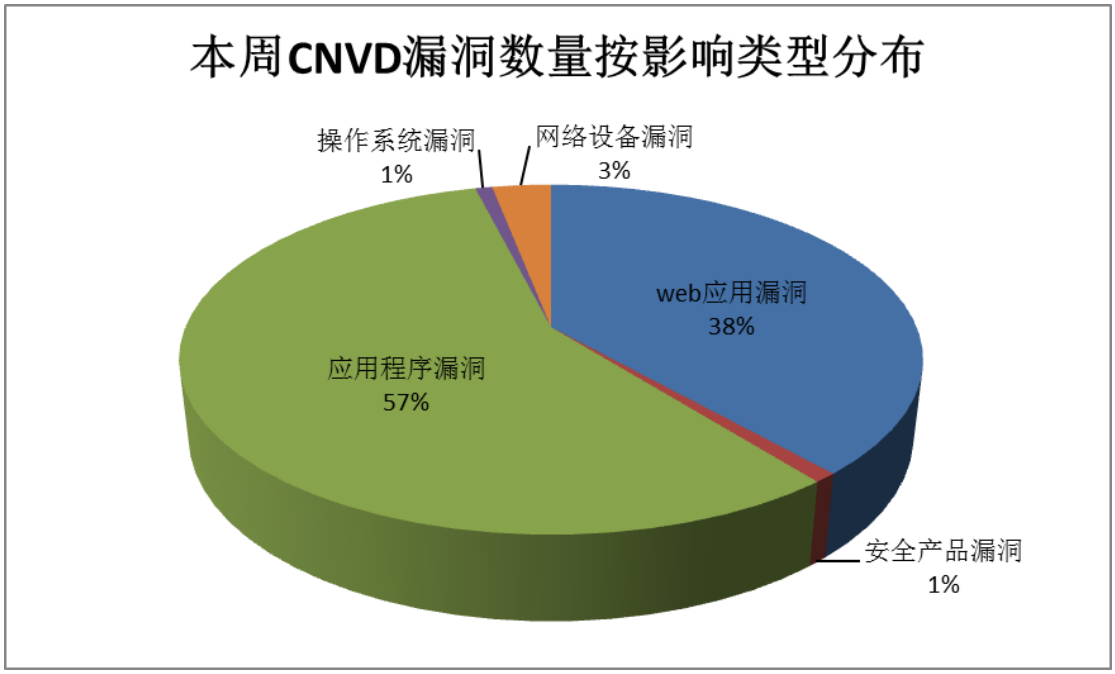

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Tcpdump、Google、Joomla 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	Tcpdump	30	10%
2	Google	23	7%
3	Joomla	17	6%
4	南京杰诺瀚软件科技有限公司	12	4%
5	IBM	8	3%
6	WordPress	6	2%
7	Autodesk	5	2%
8	NVIDIA	5	2%
9	phpcms	5	2%
10	其他	188	62%

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 5 个电信行业漏洞，4 个移动互联网行业漏洞（如下图所示）。其中，“Google Android Mediaserver 拒绝服务漏洞（CNVD-2017-02255）”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/

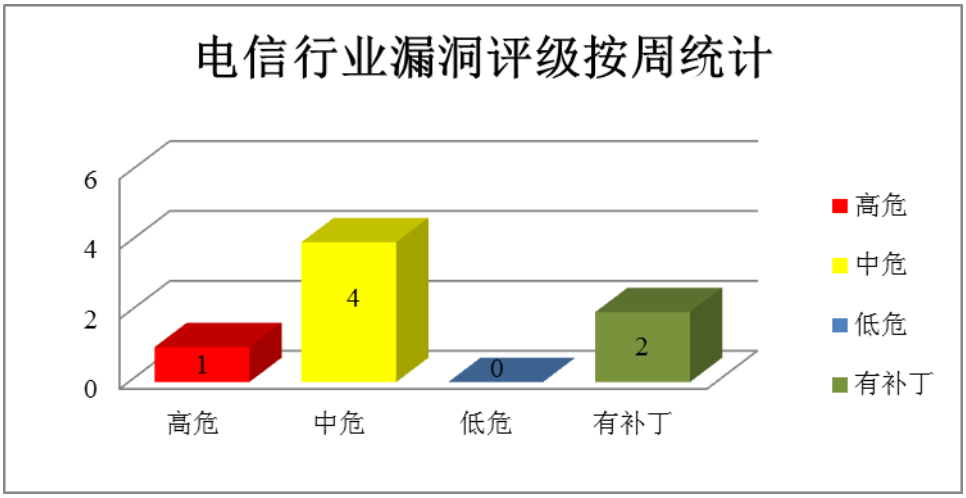

图 3 电信行业漏洞统计

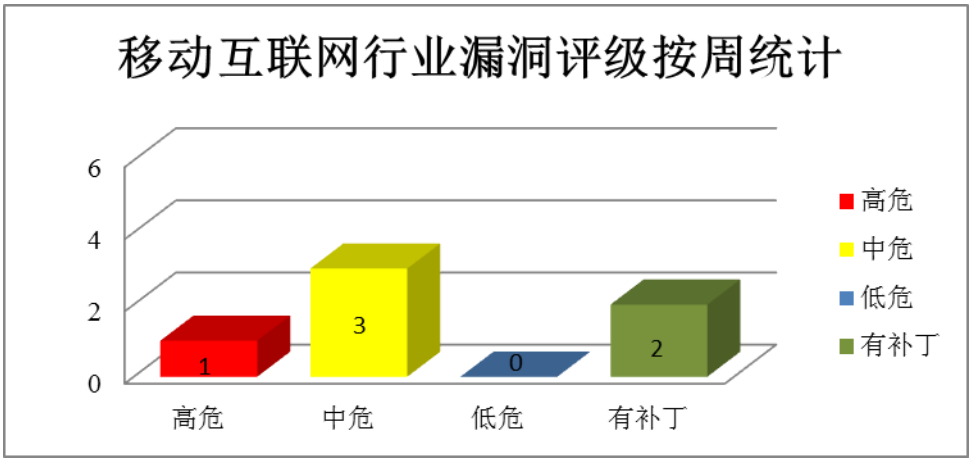

图 4 移动互联网行业漏洞统计

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、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。Google Chrome 是一款流行的 Web 浏览器。本周，上述产品被披露存在拒绝服务、跨站脚本和堆溢出代码执行漏洞，攻击者可利用漏洞发起拒绝服务攻击或执行任意代码。

CNVD 收录的相关漏洞包括：Google Android Mediaserver 拒绝服务漏洞（CNVD-2017-02255）、Google Chrome Blink 通用跨站脚本漏洞、Google Chrome Blink 通用跨

站脚本漏洞（CNVD-2017-02108、CNVD-2017-02109、CNVD-2017-02111）、Google Chrome FFmpeg 堆溢出代码执行漏洞、Google Chrome FFmpeg 堆溢出代码执行漏洞（CNVD-2017-02110）、Google Chrome Skia 堆溢出代码执行漏洞。其中，“Google Android Mediaserver 拒绝服务漏洞（CNVD-2017-02255）”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-2017-02255
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02107
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02108
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02109
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02111
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02100
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02110
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02102

2、IBM 存在产品安全漏洞

IBM Maximo Asset Management 是美国 IBM 公司的一款资产管理生命周期和工作流过程管理系统。IBM Development Package for Apache Spark 是一款软件开发包。IBM iNotes 是美国一套基于 Web 的电子邮件软件。IBM Integration Bus 是一款企业服务总线（ESB）产品。IBM WebSphere Message Broker 是一款企业服务总线产品。IBM Rational DOORS Next Generation 是一款需求管理解决方案。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发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：IBM Development Package for Apache Spark 拒绝服务漏洞、IBM iNotes 跨站脚本漏洞（CNVD-2017-02343）、IBM Integration Bus 和 WebSphere Message Broker XML 外部实体注入漏洞、IBM Rational DOORS Next Generation 信息泄露漏洞、IBM Rational Rhapsody Design Manager XML 外部实体注入漏洞、IBM WebSphere Message Broker 点击劫持漏洞、多款 IBM 产品本地信息泄露漏洞、多款 IBM 产品跨站脚本漏洞（CNVD-2017-02280）。其中，“IBM Integration Bus 和 WebSphere Message Broker XML 外部实体注入漏洞、IBM Rational Rhapsody Design Manager XML 外部实体注入漏洞”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-2017-01781
http://www.cnvd.org.cn/flaw/show/CNVD-2017-01782
http://www.cnvd.org.cn/flaw/show/CNVD-2017-01783
http://www.cnvd.org.cn/flaw/show/CNVD-2017-01784

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01785

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01786

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01787

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01780

3、Joomla 产品安全漏洞

Joomla 是一款开放源码的内容管理系统(CMS)。本周，该产品被披露存在 SQL 注入漏洞，攻击者可利用漏洞访问或修改数据库数据。

CNVD 收录的相关漏洞包括：Joomla com_civicrm 组件'id'参数 SQL 注入漏洞、Joomla com_comprofiler 组件 SQL 注入漏洞、Joomla com_fsf 组件'catid'参数 SQL 注入漏洞、Joomla com_glossary 组件'id'参数 SQL 注入漏洞、Joomla com_jajobboard 组件 SQL 注入漏洞、Joomla com_jumi 组件 SQL 注入漏洞、Joomla com_k2 组件'id'参数 SQL 注入漏洞、Joomla com_sgpprojects 组件 SQL 注入漏洞。上述漏洞的综合评级为“高危”。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-2017-02085

http://www.cnvd.org.cn/flaw/show/CNVD-2017-02088

http://www.cnvd.org.cn/flaw/show/CNVD-2017-02084

http://www.cnvd.org.cn/flaw/show/CNVD-2017-02087

http://www.cnvd.org.cn/flaw/show/CNVD-2017-02080

http://www.cnvd.org.cn/flaw/show/CNVD-2017-02086

http://www.cnvd.org.cn/flaw/show/CNVD-2017-02081

http://www.cnvd.org.cn/flaw/show/CNVD-2017-02089

4、tcpdump 产品安全漏洞

tcpdump 是 Tcpdump 团队开发的一套运行在命令行下的嗅探工具。本周，该产品被披露存在缓冲区溢出漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：tcpdump 缓冲区溢出漏洞（CNVD-2017-02235、CNVD-2017-02236、CNVD-2017-02237、CNVD-2017-02238、CNVD-2017-02239、CNVD-2017-02240、CNVD-2017-02241、CNVD-2017-02242）。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-2017-02235

http://www.cnvd.org.cn/flaw/show/CNVD-2017-02236

http://www.cnvd.org.cn/flaw/show/CNVD-2017-02237

http://www.cnvd.org.cn/flaw/show/CNVD-2017-02238

http://www.cnvd.org.cn/flaw/show/CNVD-2017-02239

http://www.cnvd.org.cn/flaw/show/CNVD-2017-02240

http://www.cnvd.org.cn/flaw/show/CNVD-2017-02241

http://www.cnvd.org.cn/flaw/show/CNVD-2017-02242

5、WordPress Kama 插件 Click Counter SQL 注入漏洞

WordPress 是 WordPress 软件基金会的一套使用 PHP 语言开发的博客平台。本周，WordPress 被披露存在 SQL 注入漏洞，攻击者可利用该漏洞访问或修改数据，泄露敏感信息。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-2017-02198

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-2017-02136	AppGoat 身份验证绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://jvn.jp/en/jp/JVN88176589/index.html
CNVD-2017-02202	NVIDIA GPU Display Driver 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：http://nvidia.custhelp.com/app/answers/detail/a_id/4398
CNVD-2017-02203	NVIDIA GPU Display Driver 本地权限提升漏洞（CNVD-2017-02203）	高	厂商已发布了漏洞修复程序，请及时关注更新：http://nvidia.custhelp.com/app/answers/detail/a_id/4398
CNVD-2017-02205	SAP KERNEL SAP Message Server HTTP 守护程序拒绝服务漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://sap.com/
CNVD-2017-02233	TigerVNC 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：https://github.com/TigerVNC/tigervnc/pull/399
CNVD-2017-02234	Linux ntfs-3g 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：http://www.linux.org/
CNVD-2017-02322	Trend Micro InterScan 任意文件写入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://success.trendmicro.com/solution/1116672
CNVD-2017-02392	X.org X Server 本地特权扩张漏洞	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.x.org/wiki/
CNVD-2017-02391	X.org X Server 本地内存错误引用漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页： https://www.x.org/wiki/
CNVD-2017-02401	CMS Made Simple Form Builder PHP 代码注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： https://daylight-it.com/security-advisory-dlcs0001.html

表 4 部分重要高危漏洞列表

小结：本周，Google 被披露存在拒绝服务、跨站脚本和堆溢出代码执行漏洞，攻击者可利用漏洞发起拒绝服务攻击或执行任意代码。此外，IBM、Joomla、tcpdump 等多款产品被披露存在多个漏洞，攻击者利用漏洞可泄露敏感信息、进行跨站脚本攻击、执行任意代码或发起拒绝服务攻击等。另外，WordPress 被披露存在 SQL 注入漏洞，攻击者可利用该漏洞访问或修改数据，泄露敏感信息。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. 中国制 GSM 语音网关存在 Root 权限后门

近日，网络安全公司 Trustwave 发布了一份报告，称在一家名为 DBL Technology（得伯乐科技）的中国公司生产的 GoIP GSM 语音网关中发现了一个隐藏后门（…due to a vendor backdoor…）。该后门存在于设备的 Telnet 服务中，黑客可利用其身份验证机制上的漏洞获取具有 root 权限的 shell。事实上，这也不是国产设备第一次被发现留有后门，如之前我们报道过的锐嘉科与上海广升。目前受到影响的网关版本为：GoIP 1，4，8，16 和 32。

参考链接：http://www.freebuf.com/news/128421.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