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 06 日-2016 年 06 月 12 日　　2016 年第 24 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 118 个，其中高危漏洞 36 个、中危漏洞 75 个、低危漏洞 7 个。漏洞平均分值为 5.93 分。本周收录的漏洞中，涉及 0day 漏洞 6 个（占 5%）。其中互联网上出现“Valve Steam 本地提权漏洞”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 1235 个，与上周（1263 个）环比下降 2%。

本周，根据 CNVD 白帽子 z_zz_zzz 在 5 月底提交的漏洞情况，CNVD 秘书处 CNCERT 组织各分中心集中开展了 weblogic java 反序列化漏洞案例的专项验证和处置，共协调处置 1900 个境内存在上述漏洞的的服务器 IP，协助服务器管理者积极修复漏洞。

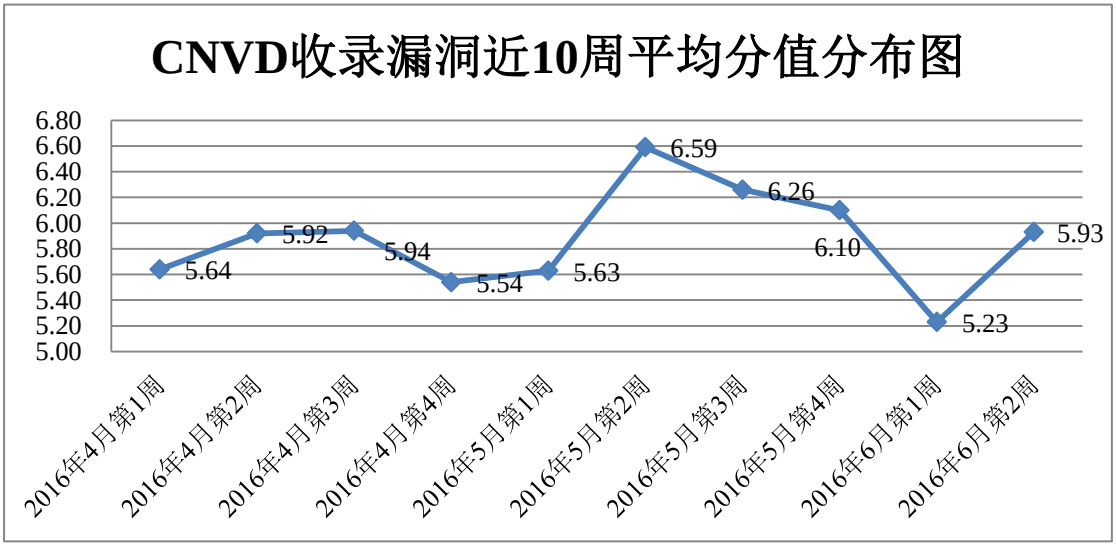

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 8 家成员单位、合作伙伴及个人报送了本周收录的全部 118 个漏洞。报送情况如表 1 所示。其中，天融信、安天实验室、恒安嘉新、启明星辰等单位报送数量较多。补天平台、乌云、漏洞盒子、福建六壬网安股份有限公司、上海零盾网络科技有限公司及白帽子向 CNVD 提交了 1235 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)	692	692
天融信	113	0
安天实验室	112	0
恒安嘉新	83	2
启明星辰	78	0
中国电信集团系统集成有限责任公司	48	2
东软	34	0
H3C	2	0
乌云	463	463
漏洞盒子	49	49
福建六壬网安股份有限公司	8	8
上海零盾网络科技有限公司	2	2
CNCERT 甘肃分中心	1	1
个人	16	16
报送总计	1701	1235
录入总计	118（去重）	1235

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 118 个漏洞。其中应用程序漏洞 82 个，操作系统漏洞 21 个，安全产品漏洞 8 个，网络设备漏洞 5 个，Web 应用漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	82
操作系统漏洞	21
安全产品漏洞	8
网络设备漏洞	5
web 应用漏洞	2

表 2 漏洞按影响类型统计表

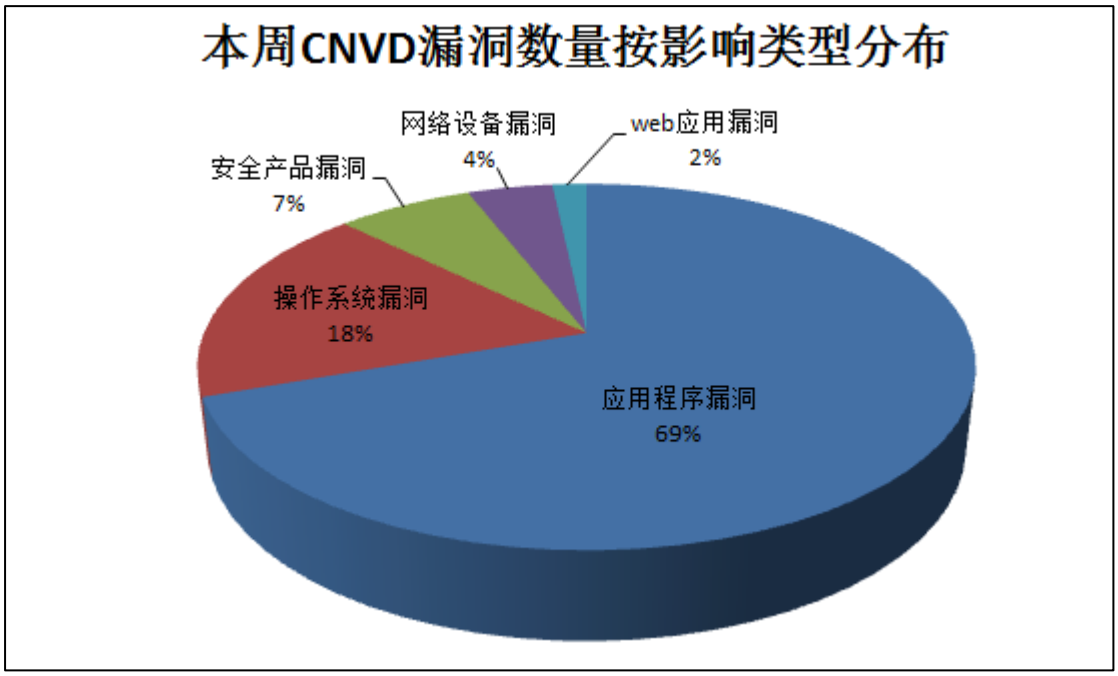

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、ImageMagick、Cisco 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	44	37%
2	ImageMagick	7	6%
3	Cisco	6	5%
4	HPE	4	3%
5	ntpd	4	3%
6	Apache	4	3%
7	Symantec	4	3%
8	Trend Micro	4	3%
9	IBM	3	3%
10	其他	38	34%

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 2 个电信行业漏洞，19 个移动互联网行业漏洞，1 个工控系统行业漏洞（如下图所示）。其中，“GE 多款产品配置选项控制漏洞、Android SD Card 用户控件模拟层权限提升漏洞、Android Mediaserver 权限提升漏洞（CNVD-2016-03921、CNVD-2016-03919）、Android Qualcomm 摄像头驱动权限提升漏洞、Android Qualcomm 视频驱动权限提升漏洞、Android Broadcom Wi-Fi 驱动权限提升漏洞、Android libwebm 远程代码执行漏洞、Android Mediaserver 远程代码执行漏洞（CNVD-2016-03851）、Android Qualcomm 声音驱动提权漏洞、Android Qualcomm 摄像头驱动提权漏洞、Siemens SIMATIC S7-300 CPU 拒绝服务漏洞”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/

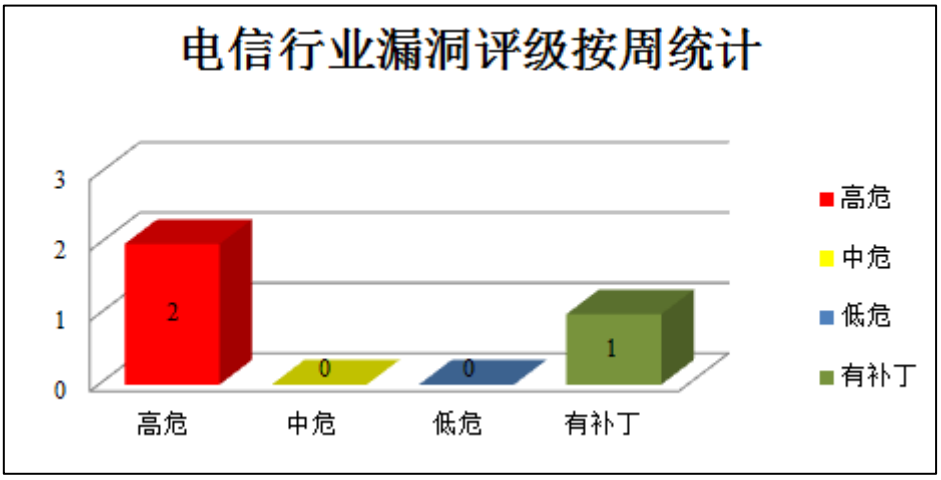

图 3 电信行业漏洞统计

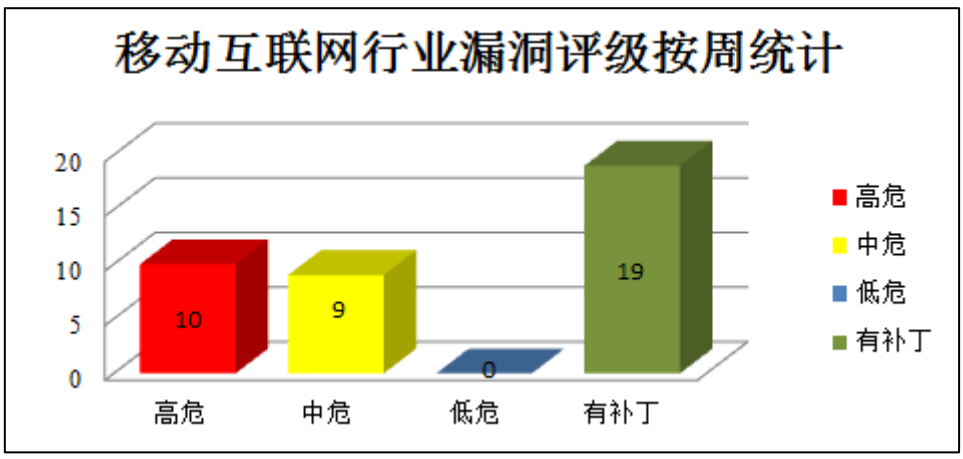

图 4 移动互联网行业漏洞统计

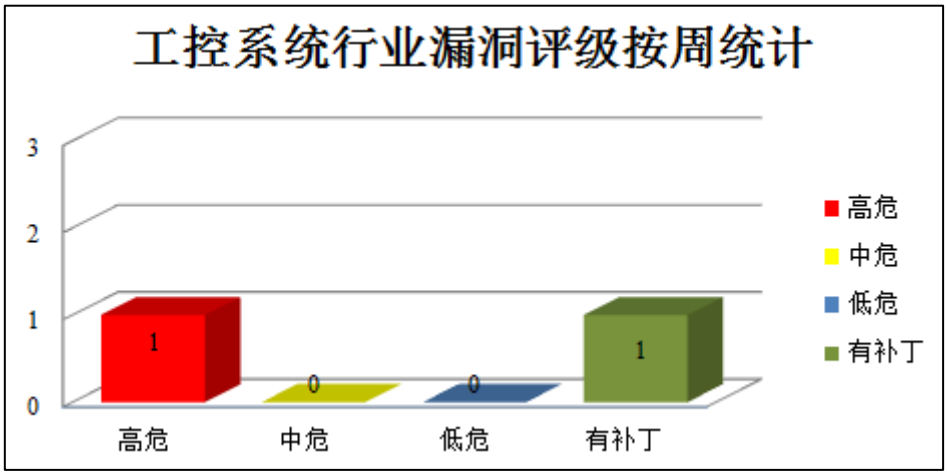

图 5 工控系统行业漏洞统计

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、 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，攻击者可利用漏洞执行任意代码、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-2016-03831）、Google Chrome SkRegion::readFromMemory 函数拒绝服务漏洞、Google Chrome 存在未明漏洞（CNVD-2016-03796）、Google Chrome ServiceWorker 存在未明漏洞、Google Chrome Skia 堆缓冲区溢出漏洞、Google Chrome media 堆缓冲区溢出漏洞、Google Chrome 信息泄露漏洞（CNVD-2016-03814）、Google Chrome V8 堆缓冲区溢出漏洞（CNVD-2016-03805）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-2016-03831

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03832

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03796

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03809

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03810

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03812

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03814

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03805

2、ImageMagick 产品安全漏洞

ImageMagick 是美国 ImageMagick Studio 公司的一套开源的图象处理软件。该软件可读取、转换、写入多种格式的图片。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：ImageMagick 'DrawDashPolygon'函数拒绝服务漏洞、ImageMagick 拒绝服务漏洞（CNVD-2016-03861、CNVD-2016-03862、CNVD-2016-03863、CNVD-2016-03864、CNVD-2016-03865、CNVD-2016-03866）。其中，“ImageMagick 拒绝服务漏洞（CNVD-2016-03861）”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-2016-03860
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03861
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03862
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03863
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03864
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03865
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03866

3、Cisco 产品安全漏洞

Cisco Aironet 1800/2800/3800 Series Access Point 是中小型无线网络接入点产品。Cisco IP 8800 phone 是美国思科（Cisco）公司的一款提供视频和 VoIP 通信功能的电话产品。Cisco Prime Network Analysis Module 和 Cisco Prime Virtual Network Analysis Module 是用于网络管理员对网络的使用情况、运行状态等进行管理和配置的网络分析软件。本周，上述产品被披露存在命令注入、权限获取和远程代码执行漏洞，攻击者可利用漏洞获取权限和执行任意命令。

CNVD 收录的相关漏洞包括：Cisco Aironet Access Points 命令注入漏洞、Cisco IP 8800 phone 权限获取漏洞、Cisco Prime Network Analysis Module 和 Cisco Prime Virtual Network Analysis Module 本地命令注入漏洞、Cisco Prime Network Analysis Module 远程代码执行漏洞（CNVD-2016-03816、CNVD-2016-03804）、Cisco Prime Network Analysis Module 远程代码执行漏洞。其中，“Cisco IP 8800 phone 权限获取漏洞、Cisco Prime Network Analysis Module 远程代码执行漏洞”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-2016-03858
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03859
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03824
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03816

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03804

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03803

4、Apache 产品安全漏洞

Apache Shiro 是美国阿帕奇（Apache）软件基金会的一套用于执行认证、授权、加密和会话管理的 Java 安全框架。Apache Struts 是一款用于创建企业级 Java Web 应用的开源框架。Apache Ranger 是一套为 Hadoop 集群实现全面安全措施的架构，它针对授权、结算和数据保护等核心企业安全要求，提供中央安全政策管理。Apache Tika 是美国阿帕奇（Apache）软件基金会的一个集成了 POI（使用 Java 程序对 Microsoft Office 格式文档提供读和写功能的开源函数库）、Pdfbox（读取和创建 PDF 文档的纯 Java 类库）并为文本抽取工作提供了统一界面的内容抽取工具集合。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和发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Apache Shiro 信息泄露漏洞、Apache Struts2 拒绝服务漏洞、Apache Ranger SQL 注入漏洞、Apache Tika XM 外部实体漏洞。其中“Apache Ranger SQL 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-2016-03869

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03789

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03828

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03819

5、 Sixnet BT-5xxx BT-6xxx M2M devices 权限提升漏洞

Red Lion Sixnet BT-5xxx 是美国 Red Lion 公司的提供无线连接功能的 BT 系列路由器。本周，Sixnet BT-5xxx BT-6xxx M2M devices 被披露存在权限提升漏洞。该漏洞源于允许反序列化不可信的数据，攻击者可利用漏洞获取访问权限。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-2016-03825

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-2016-03794	GE 多款产品配置选项控制漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.gegridsolutions.com/
CNVD-2016-03820	ntpd 存在未明漏洞	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://support.ntp.org/bin/view/Main/NtpBug3045
CNVD-201	ntpd 拒绝服务漏洞（CNVD-2016-	高	目前厂商已经发布了升级补丁以修

6-03823	03823）		复此安全问题，补丁获取链接：http://support.ntp.org/bin/view/Main/NtpBug3042
CNVD-2016-03821	ntpd 存在未明漏洞（CNVD-2016-03821）	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://support.ntp.org/bin/view/Main/NtpBug3044
CNVD-2016-03822	ntpd 存在未明漏洞（CNVD-2016-03822）	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://support.ntp.org/bin/view/Main/NtpBug3043
CNVD-2016-03827	Fonality FTP 硬编码漏洞	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.fonality.com/
CNVD-2016-03826	Fonality 任意命令执行漏洞	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.fonality.com/
CNVD-2016-03840	HPE LoadRunner 和 Performance Center 存在多个漏洞（CNVD-2016-03840）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05157423
CNVD-2016-03839	HPE LoadRunner 和 Performance Center 存在多个漏洞（CNVD-2016-03839）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05157423
CNVD-2016-03838	HPE LoadRunner 和 Performance Center 存在多个漏洞（CNVD-2016-03838）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05157423

表 4 部分重要高危漏洞列表

小结：本周 Google 产品被披露存在多个安全漏洞，攻击者可利用漏洞执行任意代码、获取敏感信息或发起拒绝服务攻击等。此外，ImageMagick、Cisco、Apache 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，Sixnet BT-5xxx BT-6xxx M2M devices 被披露存在一个高危漏洞，攻击者可利用漏洞获取访问权限。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.大量思科设备存在 IPv6 死亡之 Ping 漏洞

思科最近向企业网管们发出警告，旗下某些网络设备在处理 IPv6 包时存在漏洞，该漏洞可能会导致远程未授权 DoS 攻击的产生——黑客可以发送恶意的 IPv6 邻居发现包，至存在漏洞的设备。由于这些设备“低效的处理逻辑”，在处理这样的 IPv6 邻居包之后，设备会停止再接收 IPv6 流量，导致 DoS。该漏洞的影响范围还不仅限于思科自家的产品。目前，思科还没有针对该漏洞还放出补丁。

参考链接：http://www.freebuf.com/news/106545.html

2.运维配置缺陷导致大量 MongoDB 数据信息遭泄露

近日，黑客组织 GhostShell 泄露了大量的 MongoDB 数据库用户资料。由于开放的端口、缺乏双重因素身份验证登录暴露了严重的安全隐患，攻击者可以利用获取到的权限进行删除数据库，创建新的数据库以及篡改数据等操作。

参考链接：http://www.freebuf.com/news/106204.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