国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2016 年 05 月 23 日-2016 年 05 月 29 日　　2016 年第 22 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 206 个，其中高危漏洞 72 个、中危漏洞 121 个、低危漏洞 13 个。漏洞平均分值为 6.10 分。本周收录的漏洞中，涉及 0day 漏洞 22 个（占 11%）。其中互联网上出现“ChitaSoft SQL 注入漏洞、Patron Info System 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 1210 个，与上周（1064 个）环比上升 14%。

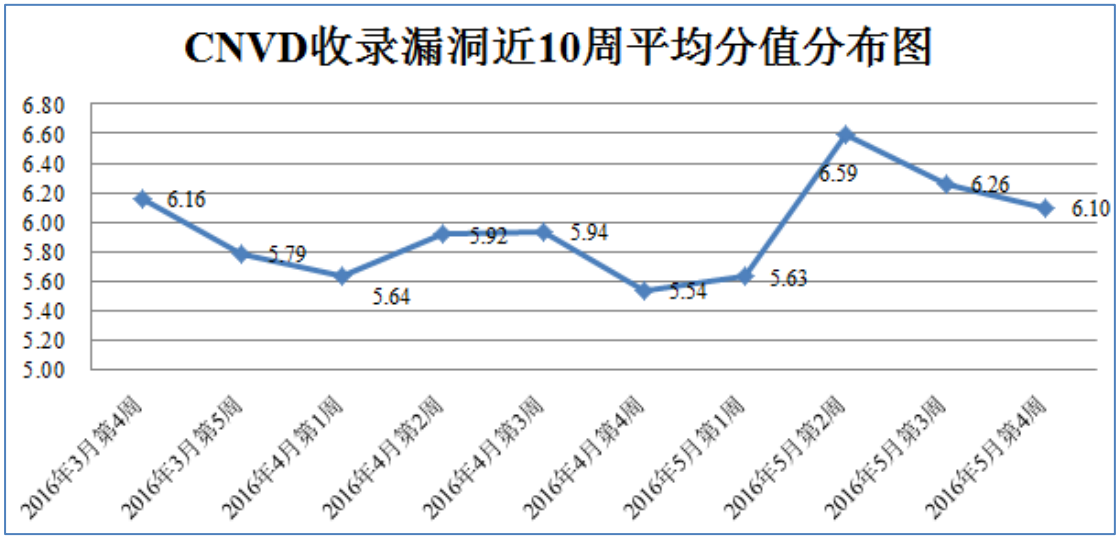

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 10 家成员单位、合作伙伴及个人报送了本周收录的全部 206 个漏洞。报送情况如表 1 所示。其中，天融信、安天实验室、启明星辰、恒安嘉新等单位报送数量较多。补天平台、乌云、漏洞盒子、西安四叶草信息技术有限公司、深圳市深信服电子

科技有限公司、福建六壬网安股份有限公司及白帽子向 CNVD 提交了 1211 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)	702	702
乌云	420	420
天融信	168	0
安天实验室	144	0
启明星辰	102	0
恒安嘉新	100	10
中国电信集团系统集成有限责任公司	49	1
东软	31	0
绿盟科技	43	0
杭州安恒信息技术有限公司	19	0
H3C	8	0
漏洞盒子	39	39
西安四叶草信息技术有限公司	8	8
福建六壬网安股份有限公司	5	5
深圳市深信服电子科技有限公司	1	1
江西分中心	1	1
个人	24	24
报送总计	1864	1211
录入总计	206（去重）	1211

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 206 个漏洞。其中应用程序漏洞 98 个，操作系统漏洞 68 个，Web 应用漏洞 24 个，网络设备漏洞 15 个，安全产品漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	98
操作系统漏洞	68
web 应用漏洞	24
网络设备漏洞	15
安全产品漏洞	1

表 2 漏洞按影响类型统计表

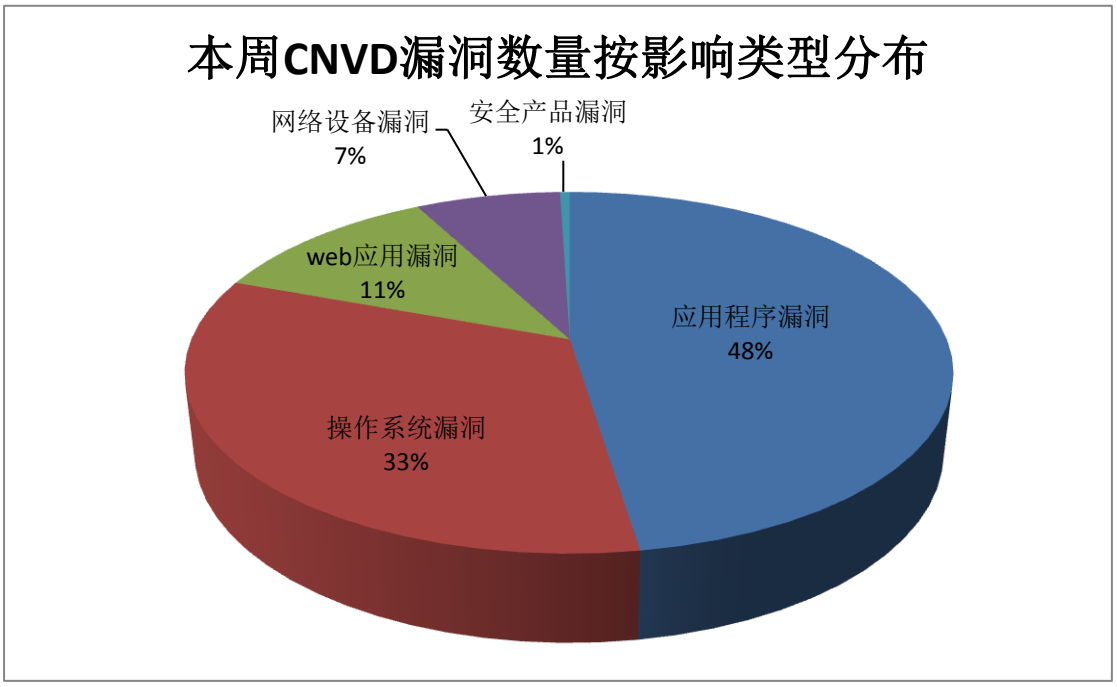

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Apple、libdwarf、IBM 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	Apple	68	33%
2	libdwarf	17	8%
3	IBM	10	5%
4	Huawei	6	3%
5	PHP	6	3%
6	Moxa	5	2%
7	WordPress	5	2%

8	Cisco	4	2%
9	Red Hat	3	1%
10	其他	82	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 7 个电信行业漏洞，37 个移动互联网行业漏洞（如下图所示）。其中，“Moxa EDR-G903 未授权操作漏洞、Moxa EDR-G903 拒绝服务漏洞、Moxa EDR-G903 内存泄露漏洞、Moxa EDR-G903 信息泄露漏洞、Moxa EDR-G903 信息泄露漏洞（CNVD-2016-03388）、Apple iOS/OS X El Capitan kernel 任意代码执行漏洞、Apple iOS/watchOS/tvOS 和 OS X El Capitan kernel 任意代码执行漏洞、Apple iOS/watchOS/tvOS 和 OS X El Capitan kernel 任意代码执行漏洞（CNVD-2016-03532、CNVD-2016-03533、CNVD-2016-03534）、Apple iOS/watchOS/tvOS 和 OS X El Capitan IOHIDFamily 任意代码执行漏洞、Apple iOS/watchOS/tvOS 和 OS X El Capitan IOHIDFamily 任意代码执行漏洞（CNVD-2016-03520）、Apple iOS/watchOS/tvOS 和 OS X El Capitan IOAcceleratorFamily 任意代码执行漏洞、Apple iOS/watchOS/tvOS 和 OS X El Capitan IOAcceleratorFamily 任意代码执行漏洞（CNVD-2016-03449、CNVD-2016-03451、CNVD-2016-03452）、Apple iOS/watchOS/tvOS 和 OS X El Capitan Disk Images 任意代码执行漏洞、Apple iOS/watchOS/tvOS 和 OS X El Capitan CoreCapture 任意代码执行漏洞”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/

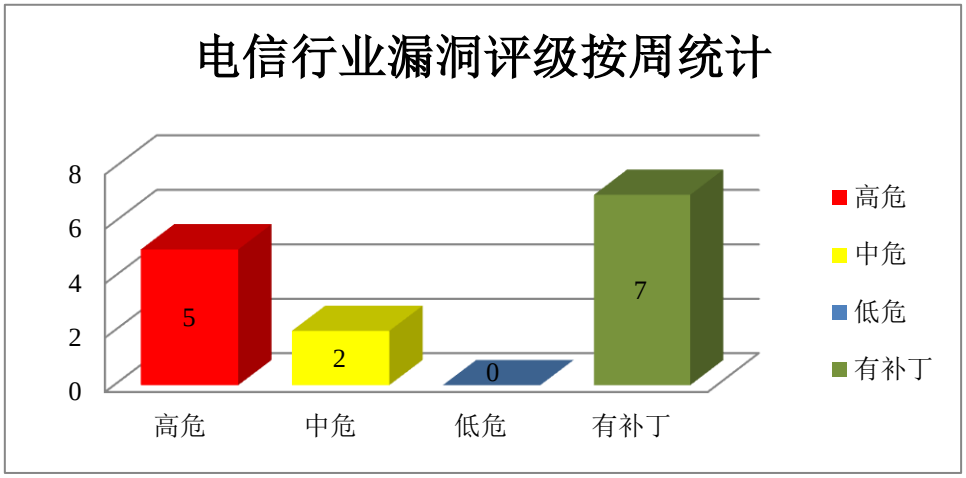

图 3 电信行业漏洞统计

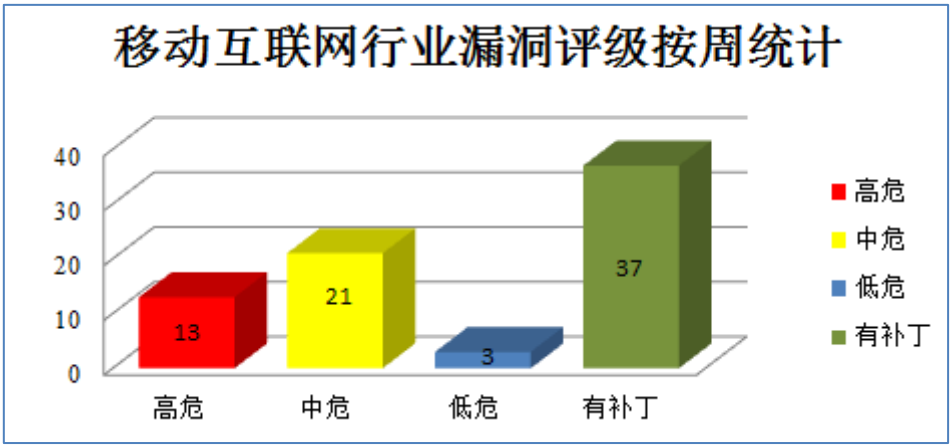

图 4 移动互联网行业漏洞统计

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、 Apple 产品安全漏洞

Apple iOS、watchOS、OS X El Capitan 和 tvOS 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；watchOS 是一套智能手表操作系统；OS X El Capitan 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。kernel 是其中的一个内核组件。本周，上述产品被披露存在任意代码执行漏洞，攻击者可利用该漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Apple iOS/watchOS/tvOS 和 OS X El Capitan IOAcceleratorFamily 任意代码执行漏洞、Apple iOS/watchOS/tvOS 和 OS X El Capitan IOAcceleratorFamily 任意代码执行漏洞（CNVD-2016-03449、CNVD-2016-03451、CNVD-2016-03452）、Apple iOS/watchOS/tvOS 和 OS X El Capitan kernel 任意代码执行漏洞、Apple iOS/watchOS/tvOS 和 OS X El Capitan kernel 任意代码执行漏洞（CNVD-2016-03532、CNVD-2016-03533、CNVD-2016-03534）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-2016-03448

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03449

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03451

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03452

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03532

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03533

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03534

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03535

2、libdwarf 产品安全漏洞

libdwarf 是一套用于读取和写入 DWARF2 调试信息的工具。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：libdwarf dwarf_line_table_reader.c 文件拒绝服务漏洞、libdwarf ‘dwarf_get_macro_startend_file()’函数拒绝服务漏洞、libdwarf dwarf_elf_access.c 文件拒绝服务漏洞、 libdwarf ‘print_exprloc_content’函数拒绝服务漏洞、libdwarf ‘dwarf_get_xu_hash_entry()’函数拒绝服务漏洞、libdwarf ‘print_frame_inst_bytes()’函数拒绝服务漏洞、libdwarf 拒绝服务漏洞、libdwarf ‘get_attr_value()’函数拒绝服务漏洞等。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-2016-03631

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03632

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03633

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03634

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03635

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03636

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03637

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03638

3、 IBM 产品安全漏洞

IBM RLKS（Rational License Key Server）是美国 IBM 公司的一款许可证密钥服务器。Administration and Reporting Tool 是其中的一个许可证密钥管理和报告工具。IBM Rational Team Concert（RTC）是一套基于 Jazz 平台且支持分散团队进行实时相关协作的软件生命周期管理解决方案。IBM Rational Engineering Lifecycle Manager 是美国 IBM 公司的一套工程生命周期管理软件。IBM InfoSphere Streams 是一套数据分析平台。IBM Security AppScan Source 是美国 IBM 公司的一套 Web 应用的安全测试工具。本周，上述产品被披露存在多个安全漏洞，攻击者利用上述漏洞可执行任意代码、注入任意 Web 脚本或 HTML、泄露敏感信息和发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：IBM RLKS Administration and Reporting Tool 信息泄露漏洞、IBM Rational Team Concert 拒绝服务漏洞、IBM Rational Engineering Lifecycle Manager 跨站脚本漏洞、IBM Rational Engineering Lifecycle Manager 跨站脚本漏洞（CNVD-2016-03396、CNVD-2016-03397）、 IBM Rational Engineering Lifecycle Manager 信息泄露漏洞、IBM InfoSphere Streams 权限获取漏洞、IBM Security AppScan Source 任意代码执行漏洞。其中，“IBM InfoSphere Streams 权限获取漏洞、IBM Security AppScan Source 任意代码执行漏洞”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-2016-03611

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03399

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03398

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03397

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03396

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03400

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03394

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03441

4、Huawei 产品安全漏洞

Huawei WearAPP 和 HiLink 都是中国华为（Huawei）公司的产品。前者是一套与智能穿戴设备配套使用的 APP，后者是一套华为网络连接终端的统一管理平台。Huawei AC6605 等都是中国华为公司的无线接入控制器产品。Huawei Mate 8 是中一款智能手机产品。Huawei NGFW Module 等都是中国华为公司的防火墙产品。 Huawei IPS Module 等都是中国华为公司的入侵防御和入侵检测产品。本周，上述产品被披露存在缓冲区溢出、设计缺陷和拒绝服务漏洞，允许攻击者利用漏洞执行任意代码和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：多款 Huawei 产品拒绝服务漏洞（CNVD-2016-03649）、Huawei Mate 8 缓冲区溢出漏洞（CNVD-2016-03576）、Huawei Mate 8 缓冲区溢出漏洞、多款 Huawei 产品缓冲区溢出漏洞（CNVD-2016-03608）、多款 Huawei 产品缓冲区溢出漏洞、Huawei WearAPP 和 HiLink 设计缺陷漏洞。其中，“多款 Huawei 产品拒绝服务漏洞（CNVD-2016-03649）、多款 Huawei 产品缓冲区溢出漏洞”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-2016-03649

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03576

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03577

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03608

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03569

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03512

5、Linux kernel 拒绝服务漏洞（CNVD-2016-03568）

Linux kernel 是美国 Linux 基金会发布的操作系统 Linux 所使用的内核。本周，Linux 被披露存在拒绝服务漏洞，攻击者可利用该漏洞造成拒绝服务（空指针逆向引用）。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-2016-03568

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-2016-03392	Moxa EDR-G903 未授权操作漏洞	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.moxa.com/
CNVD-2016-03391	Moxa EDR-G903 拒绝服务漏洞	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.moxa.com/
CNVD-2016-03390	Moxa EDR-G903 内存泄露漏洞	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.moxa.com/
CNVD-2016-03389	Moxa EDR-G903 信息泄露漏洞	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.moxa.com/
CNVD-2016-03388	Moxa EDR-G903 信息泄露漏洞（CNVD-2016-03388）	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.moxa.com/
CNVD-2016-03395	HPE Release Control Apache Commons Collections 任意代码执行漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：https://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05063986
CNVD-2016-03403	Resource Data Management Intuitive 650 TDB Controller 权限提升漏洞	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.resourcedm.com/en-us/support/software
CNVD-2016-03402	Idera Up.time client for Linux 任意文件读取漏洞	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://docs.uptimesoftware.com/display/UT/Release+Notes
CNVD-2016-03410	Chef Manage cookie 数据任意代码执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.chef.io/chef/
CNVD-201	PHP 双重释放漏洞	高	目前厂商已经发布了升级补丁以修

6-03566			复此安全问题，补丁获取链接： http://php.net/ChangeLog-7.php

表 4 部分重要高危漏洞列表

小结：本周 Apple 产品被披露存在任意代码执行漏洞，攻击者利用漏洞可执行任意代码。此外，libdwarf、IBM、Huawei 等多款产品被披露存在多个安全漏洞，攻击者可利用漏洞注入任意 Web 脚本或 HTML、泄露敏感信息、执行任意代码和发起拒绝服务攻击等。另外，Linux 被披露存在一个高危漏洞，攻击者可利用该漏洞造成拒绝服务（空指针逆向引用）。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.MySpace 出现史上最大规模数据泄露事件

近日有新闻曝光了 1.17 亿条 LinkedIn（领英）数据被泄露的消息，而最新的消息是社交网站 MySpace 也遭到了数据泄露，而泄露的数据比领英还要多。黑客宣称已经拿到了 3 亿 6000 万 MySpace 用户的电子邮件地址以及密码。如果情况属实，这将是史上最大规模的密码泄露事件。目前尚不清楚 MySpace 数据是如何被盗取的。

参考链接：http://www.freebuf.com/news/105589.html

2.【安全预警】Forbidden attack：HTTPS 网站可遭受内容篡改攻击

最近，根据某国际安全小组的研究表明，金融巨头 Visa 旗下部分受 HTTPS 保护的网站最近被发现了一种漏洞，该漏洞源于未能正确的传输层安全协议，在数据被加密时，错误重用了相同的加密随机数。它的存在可以让黑客注入恶意代码，访客浏览器将会访问到恶意内容。

参考链接：http://www.freebuf.com/vuls/105644.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