

信息安全漏洞周报

2017 年 07 月 31 日-2017 年 08 月 04 日

2017 年第 32 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 212 个，其中高危漏洞 90 个、中危漏洞 116 个、低危漏洞 6 个。漏洞平均分为 6.53。本周收录的漏洞中，涉及 0day 漏洞 80 个（占 38%），其中互联网上出现“FineCms 远程代码执行漏洞”等零日代码攻击漏洞。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 2257 个，与上周（2841 个）环比下降 21%

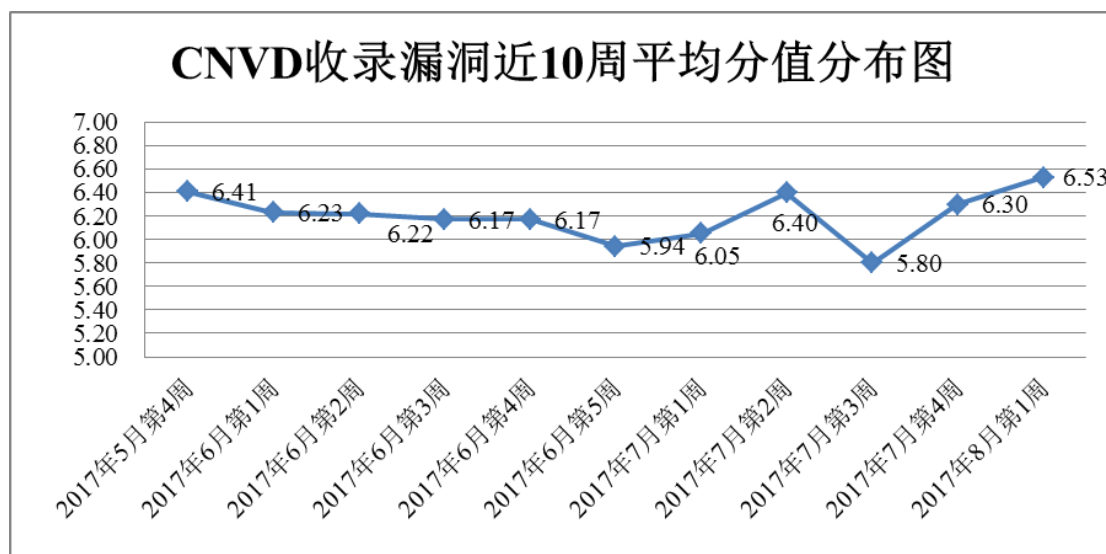


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 16 家成员单位、企业用户及个人用户报送了本周收录的全部 212 个漏洞。报送情况如表 1 所示。其中，H3C、天融信、安天实验室、启明星辰、中国电信集团系统集成有限责任公司等单位报送数量较多。360 网神、漏洞盒子、江苏同袍信息科技有限公司、南京联成科技发展股份有限公司、中新网络信息安全股份有限公司、广州软云

计算机科技有限公司、深圳鼎安天下信息科技有限公司、中国航天科工集团第四研究院软件评测中心（北京）、安徽新华博信息技术股份有限公司、上海零盾网络科技有限公司、江西安服信息产业有限公司、杭州朔方信息技术有限公司、上海犇众信息技术有限公司、中电长城网际系统应用有限公司、广州神月信息技术有限公司、山石网科通信技术有限公司、江西卓安网络科技有限公司及其他个人白帽子向 CNVD 提交了 2257 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	454	454
漏洞盒子	422	422
H3C	307	0
天融信	238	0
安天实验室	189	0
启明星辰	105	6
中国电信集团系统集成有 限责任公司	102	21
恒安嘉新	92	0
北京数字观星科技有限公 司	88	0
杭州安恒信息技术有限公 司	51	0
华为技术有限公司	45	0
绿盟科技	36	0
深圳市腾讯计算机系统有 限公司（玄武实验室）	26	26
厦门服云信息科技有限公 司	18	1
东软	6	6
知道创宇	1	1
江苏同袍信息科技有限公 司	20	20
南京联成科技发展股份有 限公司	18	18

中新网络信息安全股份有限公司	15	15
广州软云计算科技有限公司	9	9
深圳鼎安天下信息科技有限公司	8	8
中国航天科工集团第四研究院软件评测中心（北京）	8	8
安徽新华博信息技术股份有限公司	7	7
上海零盾网络科技有限公司	7	7
江西安服信息产业有限公司	5	5
杭州朔方信息技术有限公司	4	4
上海彝众信息技术有限公司	3	3
中电长城网际系统应用有限公司	3	3
广州神月信息安全技术有限公司	2	2
山石网科通信技术有限公司	2	2
江西卓安网络科技有限公司	1	1
君立华域	1	1
六壬网安	1	1
山东安云信息技术有限公司	1	1
智容科技有限公司	1	1
CNCERT 吉林分中心	3	3
CNCERT 陕西分中心	3	3
CNCERT 新疆分中心	2	2
CNCERT 河北分中心	2	2
CNCERT 海南分中心	1	1

个人	1193	1193
报送总计	3500	2257
录入总计	212（去重）	2257

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 212 个漏洞。其中应用程序漏洞 108 个，web 应用漏洞 62 个，操作系统漏洞 28 个，网络设备漏洞 10 个，数据库漏洞 3 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	108
web 应用漏洞	62
操作系统漏洞	28
网络设备漏洞	10
数据库漏洞	3
安全产品漏洞	1

表 2 漏洞按影响类型统计表

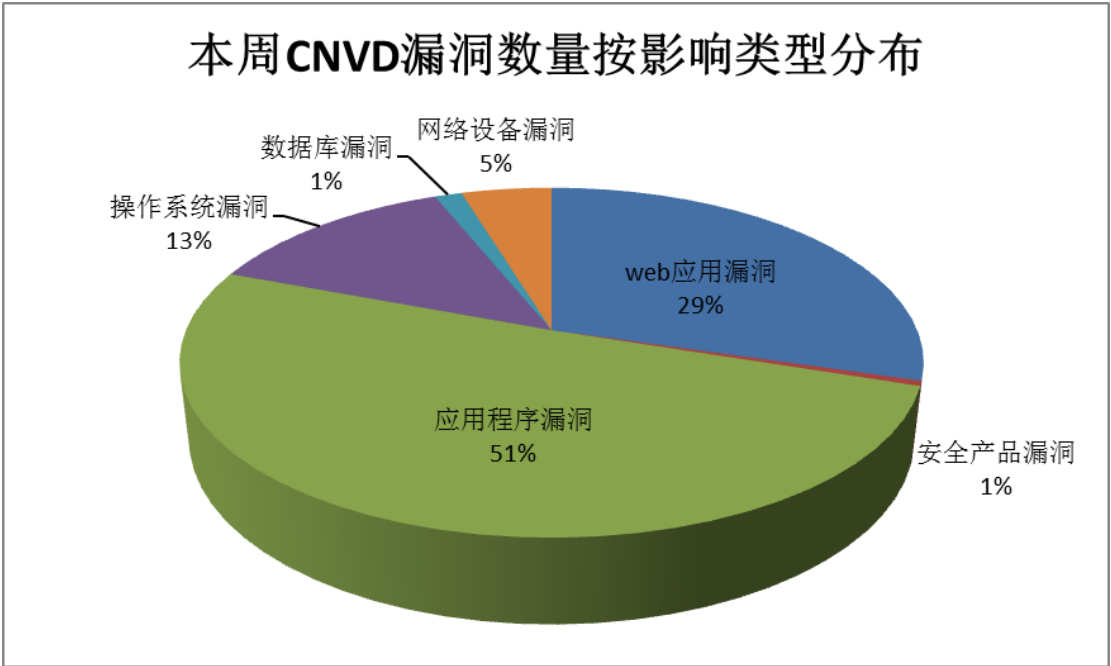


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、ImageMagick、Google 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	Oracle	48	23%

2	ImageMagick	16	8%
3	Google	12	6%
4	Microsoft	10	5%
5	FontForge	10	5%
6	FineCms	9	4%
7	Linux	7	3%
8	Televes	3	1%
9	Cacti	2	1%
10	其他	96	44%

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 12 个电信行业漏洞, 14 个移动互联网行业漏洞 (如下图所示)。其中, “Oracle Database Server 存在未明漏洞 (CNVD-2017-18569)、oogle Android Qualcomm 组件竞争条件漏洞、Google Android 身份验证绕过漏洞、Google Android Qualcomm 组件缓冲区溢出漏洞、Google Android Qualcomm 组件整数溢出漏洞 (CNVD-2017-18951)” 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/>

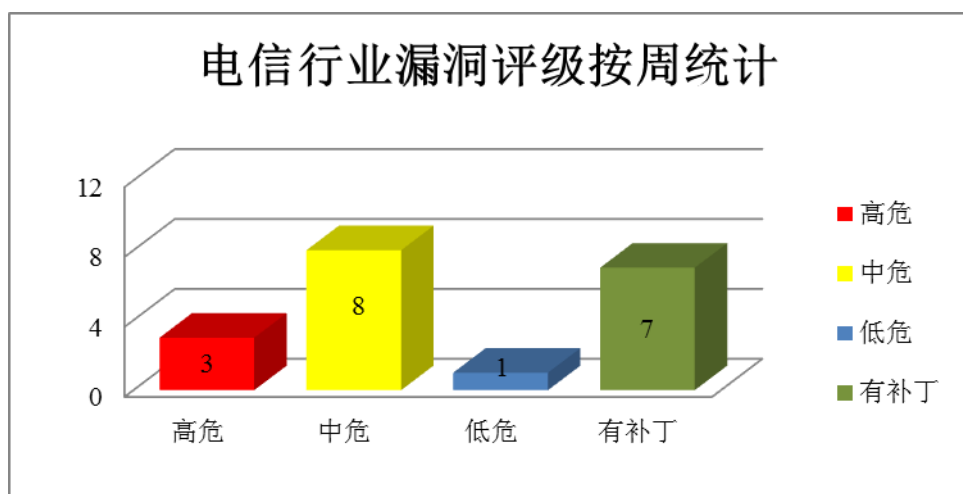


图 3 电信行业漏洞统计

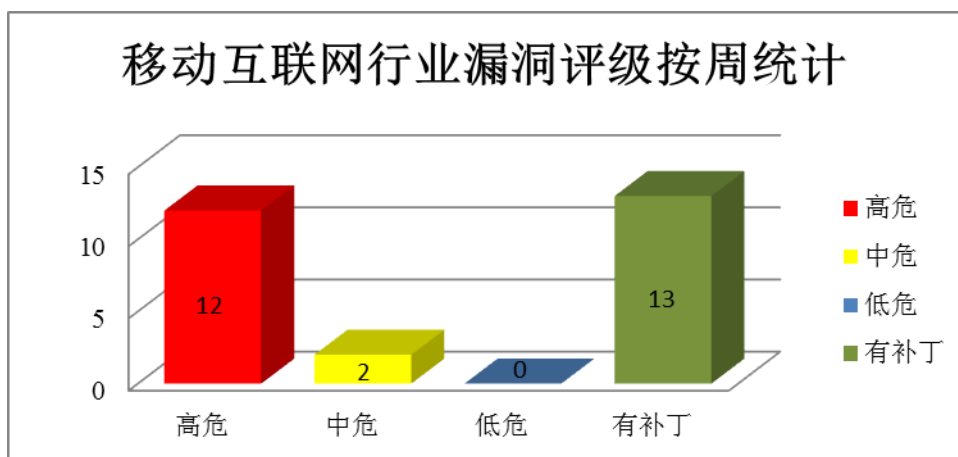


图 4 移动互联网行业漏洞统计

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、Oracle 产品安全漏洞

Oracle Fusion Middleware 是一个全面的中间件产品系列，BI Publisher 是其中的一个报表组件。本周，上述产品被披露存在多个漏洞等，攻击者可利用漏洞影响系统的机密性、完整性。

CNVD 收录的相关漏洞包括：Oracle Fusion Middleware BI Publisher 存在未明漏洞（CNVD-2017-17496、CNVD-2017-17497、CNVD-2017-17498、CNVD-2017-17499、CNVD-2017-17500、CNVD-2017-17501、CNVD-2017-17502、CNVD-2017-17503）。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-2017-17496>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-17497>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-17498>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-17499>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-17500>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-17501>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-17502>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-17503>

2、Google 产品安全漏洞

Android 是美国谷歌公司一套以 Linux 为基础的开源操作系统。Qualcomm 是一个使用在其中的设备专用高通组件。本周，该产品被披露存在缓冲区溢出、竞争条件错误和整数溢出漏洞，攻击者可利用漏洞执行任意代码或执行未授权操作。

CNVD 收录的相关漏洞包括：Google Android Qualcomm 组件缓冲区溢出漏洞（C

NVD-2017-18943、CNVD-2017-18947）、Google Android Qualcomm 组件竞争条件漏洞、Google Android Qualcomm 组件竞争条件漏洞（CNVD-2017-18946、CNVD-2017-18948）、Google Android Qualcomm 组件整数溢出漏洞、Google Android Qualcomm 组件整数溢出漏洞（CNVD-2017-18950、CNVD-2017-18951）。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-2017-18943>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-18947>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-18945>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-18946>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-18948>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-18949>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-18950>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-18951>

3、Microsoft 产品安全漏洞

Microsoft Windows 是美国微软（Microsoft）公司发布的一系列操作系统。Graphics 是其中的一个图形驱动器组件。win32k 是一个内核模式设备驱动程序。Microsoft Outlook 是一款 Office 套件中所捆绑的电子邮件客户端软件。Microsoft scripting engine 是一款用于 Microsoft Internet Explorer（IE）和 Edge 浏览器中的 JavaScript 引擎。本周，上述产品被披露存在权限提升和远程代码执行漏洞，攻击者可利用漏洞执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Microsoft scripting 引擎远程代码执行漏洞（CNVD-2017-18579）、Microsoft scripting 引擎远程代码执行漏洞、Microsoft Windows HoloLens 远程代码执行漏洞、Microsoft Office Outlook 任意代码执行漏洞（CNVD-2017-18936）、Microsoft Office Outlook 任意代码执行漏洞、Microsoft Windows Win32k 权限提升漏洞（CNVD-2017-18938、CNVD-2017-18939）、Microsoft Windows Graphics 组件权限提升漏洞。其中，“Microsoft scripting 引擎远程代码执行漏洞（CNVD-2017-18579）、Microsoft scripting 引擎远程代码执行漏洞、Microsoft Windows HoloLens 远程代码执行漏洞、Microsoft Office Outlook 任意代码执行漏洞（CNVD-2017-18936）”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-2017-18578>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-18579>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-18935>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-18936>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-18937>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-18938>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-18939>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-18940>

4、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。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：ImageMagick 拒绝服务漏洞（CNVD-2017-18099、CNVD-2017-18100、CNVD-2017-18102、CNVD-2017-18112、CNVD-2017-18114、CNVD-2017-18116、CNVD-2017-18117、CNVD-2017-18103）。其中，“ImageMagick 拒绝服务漏洞（CNVD-2017-18117、CNVD-2017-18103）”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-2017-18099>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-18100>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-18102>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-18112>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-18114>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-18116>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-18117>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-18103>

5、Joomla Ultimate Property Listing 组件 SQL 注入漏洞

Joomla 是一套使用 PHP 和 MySQL 开发的开源、跨平台的内容管理系统。本周，Joomla 被披露存在逻辑漏洞，攻击者可利用漏洞获取数据库敏感信息。目前，互联网上已经出现了针对该漏洞的攻击代码，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-2017-18697>

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-2017-17783	Linux Kernel 'virtio_gpu_object_create'函数拒绝服务漏洞	高	用户可联系供应商获得补丁信息： https://linux.cn/
CNVD-2017-17780	Linux kernel 'mq_notify'内存错误引用漏洞	高	厂商已发布漏洞修复程序，请及时关注更新： https://github.com/torvalds/linux/commit/f991af3daabaecff34684fd51fac80

			319d1baad1
CNVD-2017-18103	ImageMagick 拒绝服务漏洞 (CNVD-2017-18103)	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/ImageMagick/ImageMagick/issues/537
CNVD-2017-18104	Subrion CMS SQL 注入漏洞 (CNVD-2017-18104)	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/intelliants/subrion/issues/480
CNVD-2017-18105	Subrion CMS SQL 注入漏洞 (CNVD-2017-18105)	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/intelliants/subrion/issues/479
CNVD-2017-18117	ImageMagick 拒绝服务漏洞 (CNVD-2017-18117)	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/ImageMagick/ImageMagick/issues/528
CNVD-2017-18519	NancyFX Nancy 远程代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://github.com/NancyFx/Nancy/releases/tag/v1.4.4
CNVD-2017-18617	Google Android 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： https://www.android.com/
CNVD-2017-18634	nss_compat_oss1 存在未明漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： https://bugzilla.redhat.com/show_bug.cgi?id=1238326
CNVD-2017-18635	rkhunter 远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： http://rkhunter.cvs.sourceforge.net/viewvc/rkhunter/rkhunter/files/CHANGELOG

表 4 部分重要高危漏洞列表

小结：本周，Oracle 被披露存在多个漏洞等，攻击者可利用漏洞影响系统的机密性、完整性。此外，Google、Microsoft、ImageMagick 等多款产品被披露存在多个漏洞，攻击者可利用漏洞或执行未经授权操作、执行任意代码或发起拒绝服务攻击等。另外，Joomla 被披露存在逻辑漏洞，攻击者可利用漏洞获取数据库敏感信息。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. 福特、宝马、英菲尼迪和日产汽车 TCU 存在漏洞

TCU 是 Continental AG 公司生产的一种 2G 调制解调器，现在的汽车普遍用它来传输数据。利用这个模块汽车之间可以互相通讯，还可以用 web 控制台和手机 app 来远程控制手机。漏洞影响的是 S-Gold 2 (PMB 8876)蜂窝基带芯片，其中一个漏洞是 TCU 中处理 AT 命令的组件存在缓冲区溢出漏洞（漏洞编号 CVE-2017-9647），这些命令包括 AT+STKPROF, AT+XAPP, AT+XLOG 和 AT+FNS，这些命令中有很多是苹果在 2015 年修复的 iPhone 漏洞。不过要执行这个攻击，攻击者需要对汽车有物理权限。

参考链接：<http://www.freebuf.com/news/143040.html>

2. 中国深圳一家厂商的智能摄像头曝出漏洞

安全企业 Bitdefender 和 Checkmarx 均发布报告表示，安全研究员在多个常用智能摄像头中发现远程侵入漏洞，涉及 VStarcam、Loftek、以及 Neo IP camera。其中的 Neo IP camera 就是中国深圳厂商丽欧电子（Neo Electronics）生产的智能摄像头设备，此次安全企业提供的报告中具体列出了丽欧电子的两款产品：iDoorbell 以及 Neo Coolcam NIP-22 两种摄像头均存在缓冲区溢出问题，受影响的设备可以被攻击者远程入侵，执行任意代码并彻底接管。。

参考链接：<http://www.freebuf.com/news/143024.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