

信息安全漏洞周报

2015 年 01 月 26 日-2015 年 02 月 01 日

2015 年第 5 期

本周漏洞基本情况

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 215 个，其中高危漏洞 66 个、中危漏洞 120 个、低危漏洞 29 个。上述漏洞中，可利用来实施远程攻击的漏洞有 192 个。本周收录的漏洞中，已有 188 个漏洞由厂商提供了修补方案，建议用户及时下载补丁更新程序，避免遭受网络攻击。本周互联网上出现“Cat Bot SQL 注入漏洞”、“Apple Mac OS X IOKit IntelAccelerator 空指针引用本地代码执行漏洞”等零日攻击代码，请使用相关产品的用户注意加强防范。

本周，互联网上披露了 GNU glibc 函数库存在的缓冲区溢出高危漏洞（又称“幽灵”漏洞）。CNVD 组织测试分析认为漏洞影响非常广泛，评级高危。但从披露情况看要达到在远程渗透需要较多前提（如服务依赖关系和攻击数据包长度），短期内大规模远程攻击可能性还较小。目前，除一些系统服务和邮件服务经测试有可能受到影响外，Wordpress 以及 PHP 等相关 web 应用都有可能受到影响。

成员单位报送漏洞统计

本周，共 6 家成员单位、合作伙伴及个人报送了本周收录的全部 215 个漏洞。报送情况如表 1 所示。其中，奇虎 360、恒安嘉新、启明星辰、安天实验室、绿盟科技等单位报送数量较多。此外，CNCERT 各分中心、High-Tech Bridge Security Research Lab、上海天泰网络技术有限公司及白帽子向 CNVD 提交了 1458 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
奇虎 360	1447	1447
恒安嘉新	154	0

启明星辰	152	0
安天实验室	126	0
绿盟科技	102	0
天融信	94	0
High-Tech Bridge Security Research Lab	5	5
上海天泰网络技术有 限公司	1	1
CNCERT 福建分中心	2	2
CNCERT 宁夏分中心	2	2
个人	1	1
报送总计	2086	1458
录入总计	215（去重）	1458

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Oracle、Google、Apple 等多家厂商的产品，部分漏洞数量按厂商统计如表 2 所示。

序号	厂商（产品）	漏洞数量	所占比例
1	Oracle	59	27%
2	Google	28	13%
3	Apple	8	4%
4	SAP	4	2%
5	Linux	3	1%
6	WordPress	3	1%
7	MantisBT	3	1%
8	Apache	2	1%
9	Adobe	2	1%
10	其他	103	49%

表 2 漏洞产品涉及厂商分布统计表

本周，CNVD 收录了 215 个漏洞。其中应用程序漏洞 160 个，WEB 应用漏洞 23 个，操作系统漏洞 12 个，数据库漏洞 9 个，网络设备漏洞 7 个，安全产品漏洞 4 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	160
WEB 应用漏洞	23
操作系统漏洞	12
数据库漏洞	9
网络设备漏洞	7
安全产品漏洞	4

表 3 漏洞按影响类型统计表

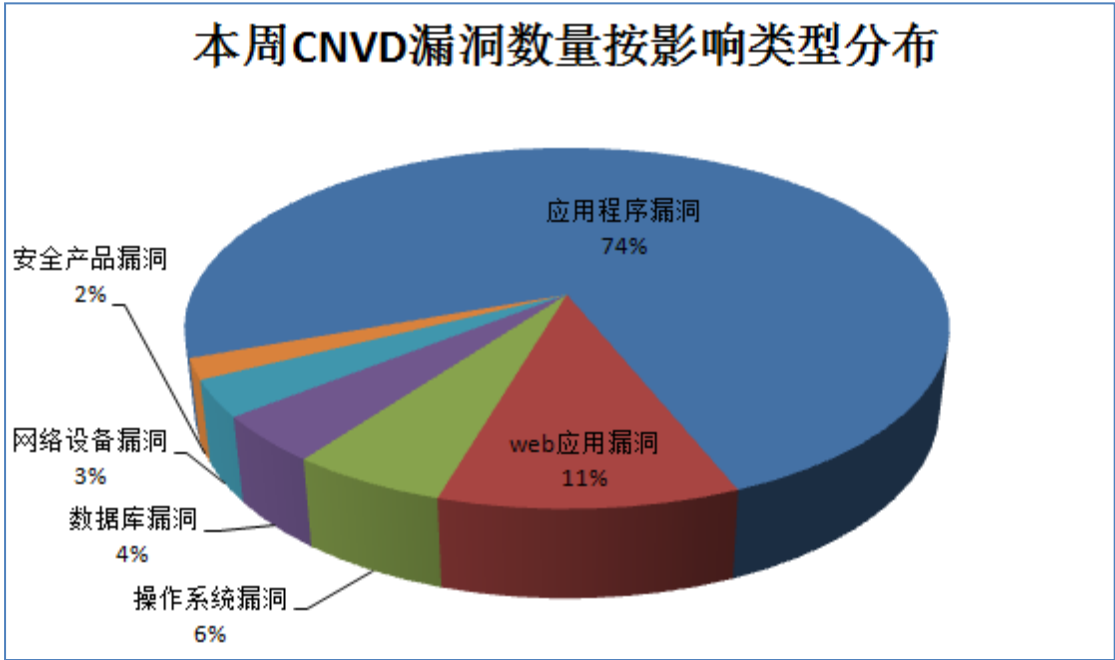


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 18 个电信行业漏洞，1 个移动互联网行业漏洞，4 个工控系统行业漏洞（如下图表所示）。其中，“Oracle MySQL Server 存在未明漏洞（CNVD-2015-00623）、Siemens Scalance X Switches 'HTTP'请求拒绝服务漏洞、SAP Adaptive Server Enterprise SQL 注入漏洞、IBM Tivoli Monitoring 远程命令执行漏洞、Cisco 2900 Series Integrated Services Router 拒绝服务漏洞”的综合评级均为“高危”。相关厂商已经发布了上述漏洞的修补程序。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2015-00583	Oracle Forms Services 子件存在未明漏洞	中	是
电信	CNVD-2015-00587	D-Link DSL-2730B router 存在多个跨	中	是

		站脚本漏洞		
电信	CNVD-2015-00609	Cisco Unified Communications Manager 文件泄露漏洞	中	否
电信	CNVD-2015-00626	Oracle MySQL Server 存在未明漏洞 (CNVD-2015-00626)	低	是
电信	CNVD-2015-00625	Oracle MySQL Server 存在未明漏洞 (CNVD-2015-00625)	中	是
电信	CNVD-2015-00624	Oracle MySQL Server 存在未明漏洞 (CNVD-2015-00624)	中	是
电信	CNVD-2015-00623	Oracle MySQL Server 存在未明漏洞 (CNVD-2015-00623)	高	是
电信	CNVD-2015-00622	Oracle MySQL Server 存在未明漏洞 (CNVD-2015-00622)	中	是
电信	CNVD-2015-00621	Oracle MySQL Server 存在未明漏洞 (CNVD-2015-00621)	低	是
电信	CNVD-2015-00629	Oracle MySQL Server 存在未明漏洞 (CNVD-2015-00629)	低	是
电信	CNVD-2015-00628	Oracle MySQL Server 存在未明漏洞 (CNVD-2015-00628)	中	是
电信	CNVD-2015-00627	Oracle MySQL Server 存在未明漏洞 (CNVD-2015-00627)	中	是
电信	CNVD-2015-00656	Siemens Scalance X Switches 拒绝服务漏洞	中	是
电信	CNVD-2015-00657	ADB P.DGA4001N 路由器存在未明漏洞	高	否
电信	CNVD-2015-00663	Siemens Scalance X Switches 'HTTP'请求拒绝服务漏洞	高	是
电信	CNVD-2015-00698	SAP Adaptive Server Enterprise SQL注入漏洞	高	是
电信	CNVD-2015-00725	IBM Tivoli Monitoring 远程命令执行漏洞	高	是
电信	CNVD-2015-00740	Cisco 2900 Series Integrated Services Router 拒绝服务漏洞	高	是
移动互联网	CNVD-2015-00728	多个 Android Devices 存在拒绝服务漏洞	中	否
工控系统	CNVD-2015-00585	Siemens SIMATIC S7-1200 打开重定向漏洞	中	否
工控系统	CNVD-2015-00647	Schneider Electric ETG3000 FactoryCast HMI Gateway 验证绕过漏洞	中	是
工控系统	CNVD-2015-00648	Schneider Electric ETG3000 FactoryCast HMI Gateway 未授权访问漏洞	中	是
工控系统	CNVD-2015-00754	Infinite Automation Systems Mango Automation 跨站脚本漏洞	中	是

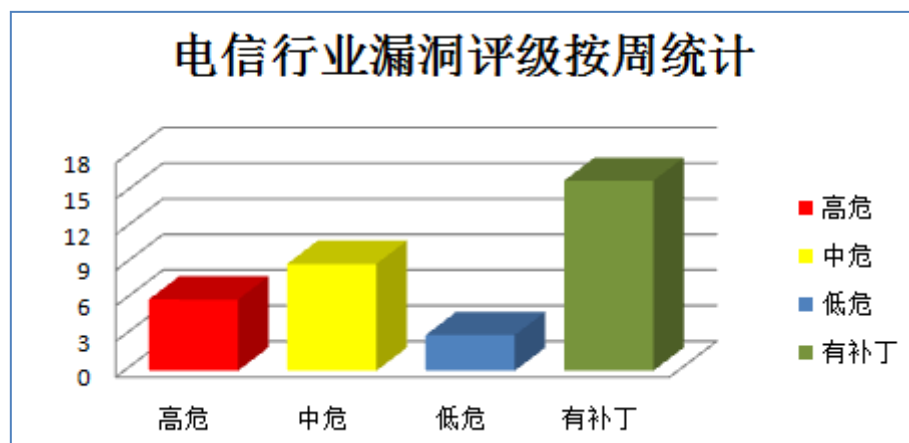


图 1 电信行业漏洞统计

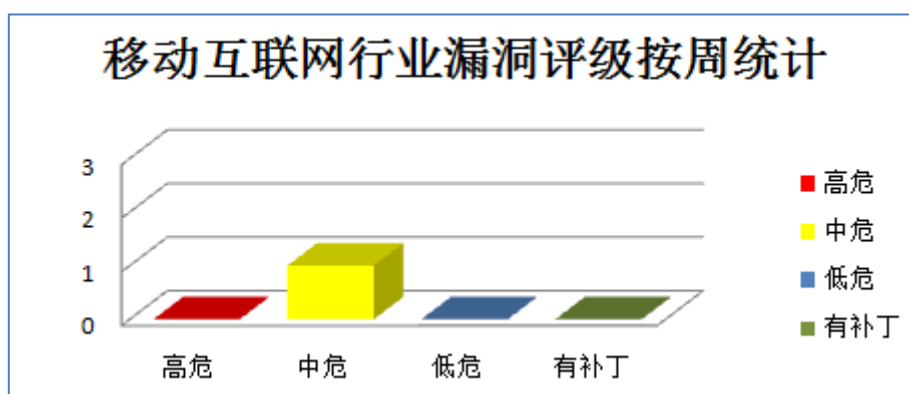


图 2 移动互联网行业漏洞统计

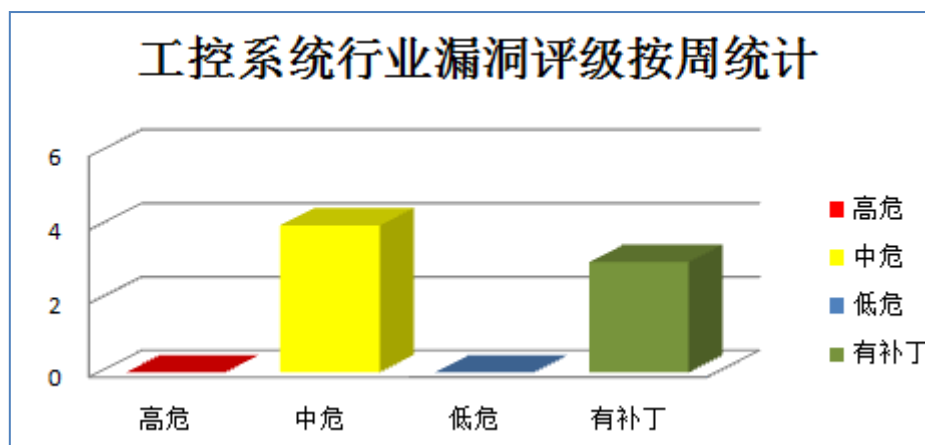


图 3 工控系统行业漏洞统计

本周重要漏洞信息

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、GNU 产品安全漏洞

GNU glibc 是一款 Linux 操作系统中 C 库的实现。本周，上述产品被披露存在缓冲区溢出和拒绝服务漏洞，攻击者可利用漏洞以当前用户权限执行任意代码，进而控制操作系统主机或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：GNU glibc 远程堆缓冲区溢出漏洞、GNU patch 'set_hunkmax()'函数拒绝服务漏洞。其中，“GNU glibc 远程堆缓冲区溢出漏洞”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 提醒用户尽快下载补丁更新，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-2015-00719>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00705>

2、Google 产品安全漏洞

Google Chrome 是一款流行的 WEB 浏览器。本周，上述产品被披露存在内存错误引用和拒绝服务漏洞，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：Google Chrome 拒绝服务漏洞（CNVD-2015-00667、CNVD-2015-00668、CNVD-2015-00669、CNVD-2015-00672）、Google Chrome DOM 内存错误引用代码执行漏洞、Google Chrome DOM 内存错误引用漏洞（CNVD-2015-00666、CNVD-2015-00701）、Google Chrome V8 内存破坏漏洞。上述漏洞的综合评级均为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户尽快下载补丁更新，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-2015-00667>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00668>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00669>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00672>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00665>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00666>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00701>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00664>

3、Apple 产品安全漏洞

Apple MAC OS X Yosemite 是苹果公司开发的最新操作系统。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞获取敏感信息、进行未授权操作、提升权限或执行任意代码。

CNVD 收录的相关漏洞包括：Apple MAC OS X Yosemite 信息泄露漏洞（CNVD-2015-00758、CNVD-2015-00759、CNVD-2015-00761）、Apple MAC OS X Yosemite 任意代码执行漏洞、Apple MAC OS X Yosemite 安全绕过漏洞、Apple Mac OS X XPC 类型混淆安全绕过漏洞、Apple Mac OS X IOBluetoothDevice 本地权限提升漏洞。其中，“Apple MAC OS X Yosemite 任意代码执行漏洞、Apple Mac OS X IOBluetooth

Device 本地权限提升漏洞”的综合评级均为“高危”。除“Apple Mac OS X IOBluetoothDevice 本地权限提升漏洞”外，厂商已经发布了其余漏洞的修补程序。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-2015-00758>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00759>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00761>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00727>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00760>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00639>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00636>

4、Oracle 产品安全漏洞

MySQL 是一款开源关系型数据库管理系统。本周，上述产品被披露存在未明漏洞，攻击者可利用漏洞影响系统的完整性、可用性和保密性。

CNVD 收录的相关漏洞包括：Oracle MySQL Server 存在未明漏洞（CNVD-2015-00627、CNVD-2015-00626、CNVD-2015-00625、CNVD-2015-00624、CNVD-2015-00623、CNVD-2015-00622、CNVD-2015-00621、CNVD-2015-00628）。其中“Oracle MySQL Server 存在未明漏洞（CNVD-2015-00623）”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-2015-00627>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00626>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00625>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00624>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00623>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00622>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00621>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00628>

5、JasPer 'jpc_dec_process_sot()'远程堆缓冲区溢出漏洞

JasPer 是一款图形处理工具，包括 JPEG-2000 Part-1 code 实现。本周，JasPer 'jpc_dec_process_sot()'被披露存在综合评级为“高危”的堆缓冲区溢出漏洞。攻击者可以利用漏洞在受影响应用程序的上下文中执行任意代码。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-2015-00638>

更多高危漏洞如表 3 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	漏洞名称	综合	修复方式
--------	------	----	------

号		评级	
CNVD-2015-00557	McAfee Data Loss Prevention Endpoint 权限提升漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://kc.mcafee.com/corporate/index?page=content&id=SB10097 https://kc.mcafee.com/corporate/index?page=content&id=SB10098
CNVD-2015-00559	McAfee Data Loss Prevention Endpoint SQL 注入漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://kc.mcafee.com/corporate/index?page=content&id=SB10097 https://kc.mcafee.com/corporate/index?page=content&id=SB10098
CNVD-2015-00608	Samba 权限提升漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://www.samba.org/
CNVD-2015-00611	PHP Calendar Extension 远程整数溢出漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： http://www.php.net
CNVD-2015-00613	Adobe Flash Player 内存破坏漏洞（CNVD-2015-00613）	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： http://helpx.adobe.com/security/products/flash-player/apsb15-02.html
CNVD-2015-00614	Libevent 存在多个堆缓冲区溢出漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： http://libevent.org/
CNVD-2015-00633	grep 'kwset.c'远程缓冲区溢出漏洞	高	用户可以联系供应商获得补丁信息： http://www.gnu.org/software/grep/
CNVD-2015-00632	Adobe Flash Player 存在未明漏洞（CNVD-2015-00632）	高	用户可以联系供应商获得补丁信息： http://www.adobe.com/
CNVD-2015-00642	Attachmate Reflection FTP 客户端栈缓冲区溢出漏洞	高	用户可联系供应商获得补丁信息： https://www.attachmate.com/
CNVD-2015-00655	ManageEngine ServiceDesk Plus 'CreateReportTable.jsp' SQL 注入漏洞	高	用户可以联系供应商获得补丁信息： http://www.manageengine.com/produ

			cts/service-desk/
--	--	--	-------------------

表 3 部分高危漏洞列表

小结：本周，GNU 产品被披露存在缓冲区溢出和拒绝服务漏洞，攻击者可利用漏洞以当前用户权限执行任意代码，进而控制操作系统主机或发起拒绝服务攻击。此外，Google、Apple、Oracle 多款产品被批露存在多个安全漏洞，允许攻击者利用漏洞获取敏感信息、提升权限、执行未授权操作或任意代码、还可发起拒绝服务攻击。另外，Jasper 'jpc_dec_process_sot()'被披露存在一个高危零日漏洞。攻击者可以利用漏洞在受影响应用程序的上下文中执行任意代码。建议相关用户应随时关注上述厂商主页，及时获取修复补丁或解决方案。

本周重要漏洞修补信息

CNVD 整理和发布以下重要安全修补信息。

1、Apache 修补 Qpid 产品漏洞

Apache Qpid(Open Source AMQP Messaging)是一个跨平台的企业通讯解决方案，实现了高级消息队列协议。

本周，Apache 修补了上述产品存在的安全绕过和拒绝服务漏洞，避免攻击者利用漏洞绕过安全限制执行未授权操作和发起拒绝服务攻击。CNVD 已收录相关补丁，请广大用户及时下载更新，避免引发漏洞相关的网络安全事件。

补丁下载链接：<http://www.cnvd.org.cn/patchInfo/show/54747>

<http://www.cnvd.org.cn/patchInfo/show/54745>

本周要闻速递

1. D-Link 路由器曝远程 DNS 劫持漏洞

安全研究人员发现 D-Link 路由器上存在高危 DNS 劫持漏洞。利用该漏洞，攻击者无需身份验证就可访问 D-Link 设备的 web 管理者界面，然后更改 DNS 设置，重定向用户到一个钓鱼网站，或者更改域名为提供恶意程序的地址。即使 web 管理者为暴露在网，攻击者也可以通过使用跨站请求伪造（CSRF）技术从本地网络访问路由器界面。研究者目前无法确定是不是所有的 D-Link 路由器都存在漏洞，但至少可以确定的是 D-Link 的 DSL-2740R ADSL 调制解调器/无线路由器上存在该漏洞。另外，所有使用 ZynOS 固件的路由器都是不安全的，品牌包括 D-Link（友讯）、TP-Link（深圳普联）、ZTE（中兴通讯）。

参考链接：<http://www.freebuf.com/news/57949.html>

2. “美国版微信” WhatsApp Web 存在两个安全漏洞

Indrajeet Bhuyan 今年 17 岁，是一名来自印度的安全研究人员。近日他发现了两个 WhatsApp Web 版的漏洞。一个是照片越权查看漏洞：正常情况下，如果我们设置了“仅联系人可见”的话，那其他非联系人列表里的人是无法查看我们的资料图片的。但是新版本的 WhatsApp Web 却不一样，无论你设不设置“仅联系人可见”，其他的联系人（包括联系人列表之外的用户）都能看到你 WhatsApp 上的图片。另外一个漏洞是照片同步漏洞：当用户在 WhatsApp 手机客户端上删除照片后，照片还能够通过 PC（Web）版获得。

参考链接：<http://www.freebuf.com/news/57926.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