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 27 日-2016 年 07 月 03 日　　2016 年第 27 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 21 个、中危漏洞 93 个、低危漏洞 4 个。漏洞平均分值为 5.81 分。本周收录的漏洞中，涉及 0day 漏洞 10 个（占 8%）。其中互联网上出现“MileSight camera 默认 SSH root 用户漏洞、MileSight camera 权限控制页面非授权访问漏洞”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 518 个，与上周（1091 个）环比下降 53%。

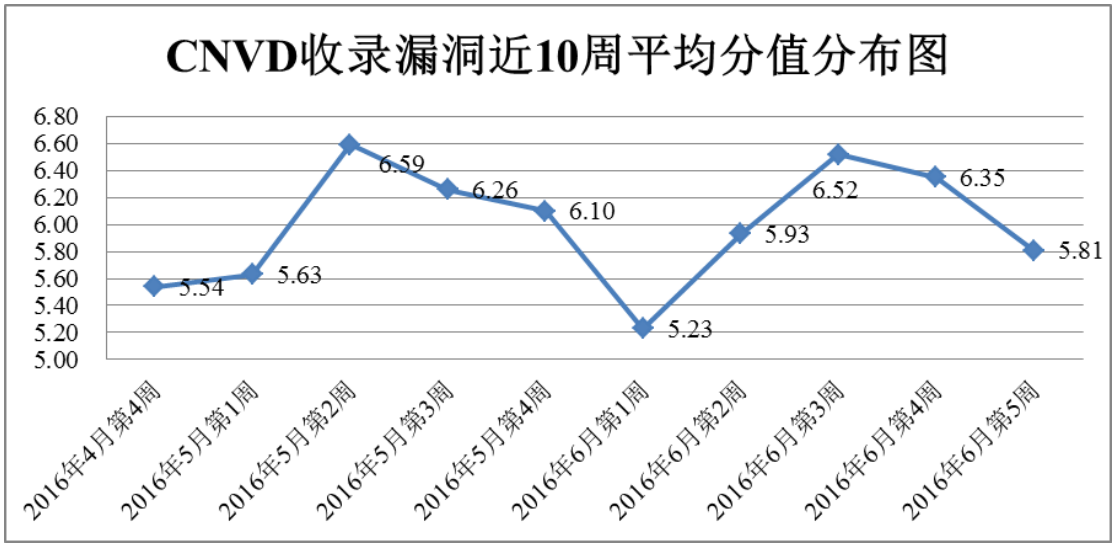

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 6 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 118 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、腾讯玄武实验室、福建六壬网安股份有限公司及其他个人白帽子向 CNVD 提交了 518 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
天融信	183	0
安天实验室	162	0
启明星辰	101	0
恒安嘉新	87	11
中国电信集团系统集成有限责任公司	33	0
H3C	8	0
乌云	377	377
漏洞盒子	40	40
西安四叶草信息技术有限公司	77	77
腾讯玄武实验室	5	5
福建六壬网安股份有限公司	4	4
CNCERT 广西分中心	1	1
个人	3	3
报送总计	1081	518
录入总计	118（去重）	518

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 75 个，web 应用漏洞 13 个，网络设备漏洞 12 个， 安全产品漏洞 10 个，操作系统漏洞 8 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	75
web 应用漏洞	13
网络设备漏洞	12
安全产品漏洞	10

操作系统漏洞	8

表 2 漏洞按影响类型统计表

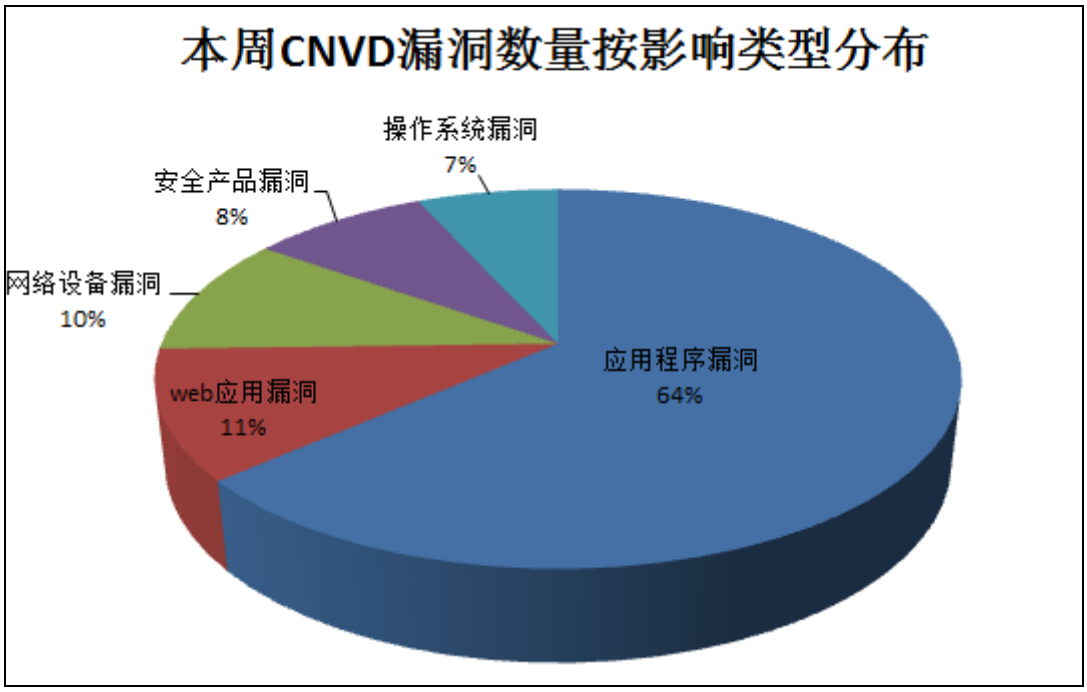

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Pidgin、WordPress、phpMyAdmin 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	Pidgin	16	14%
2	WordPress	11	9%
3	phpMyAdmin	10	8%
4	Symantec	8	7%
5	Linux	8	7%
6	PHP	7	6%
7	Open-Xchange	6	5%
8	MileSight	5	4%
9	IBM	4	3%
10	其他	43	37%

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 个电信行业漏洞，1 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，“Unitronics VisiLogic OPLC IDE 栈缓冲区溢出漏洞”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/

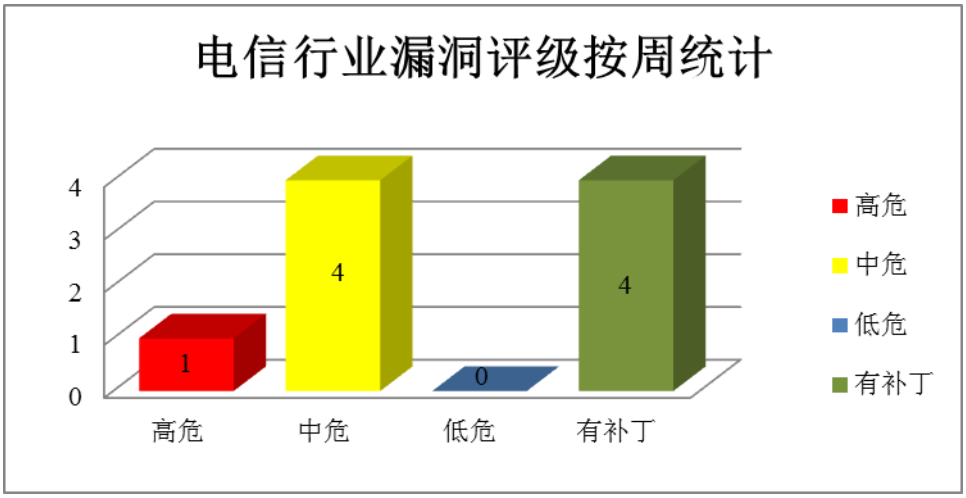

图 3 电信行业漏洞统计

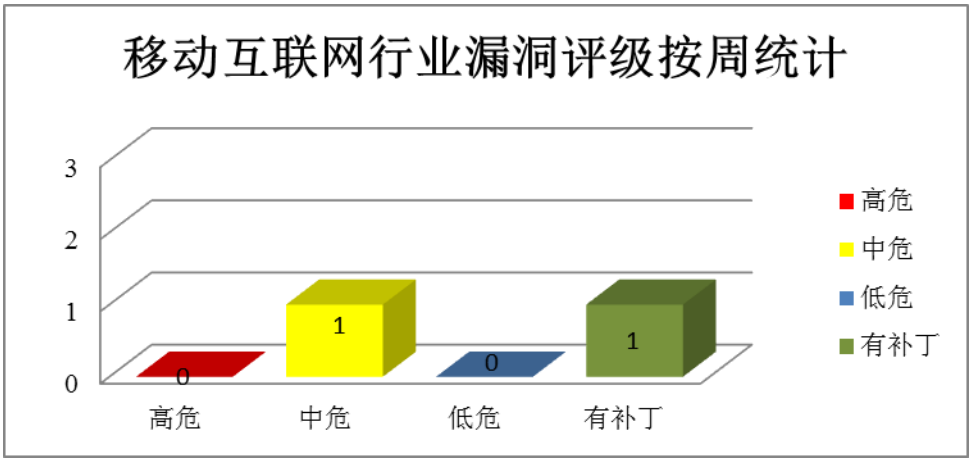

图 4 移动互联网行业漏洞统计

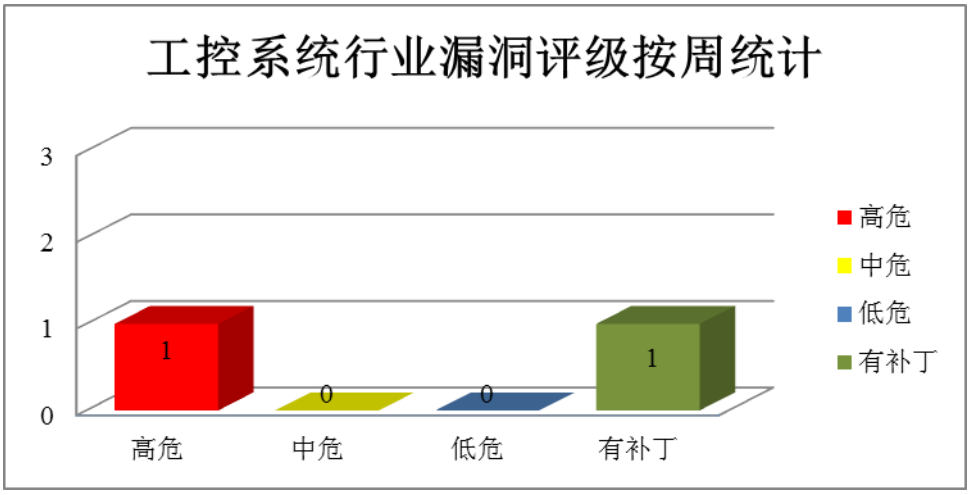

图 5 工控系统行业漏洞统计

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、 Pidgin 产品安全漏洞

Pidgin 是一款跨平台的实时通信客户端。本周，该产品被披露存在缓冲区溢出和拒绝服务漏洞，攻击者可利用漏洞进行跨站脚本攻击和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Pidgin MXIT 协议缓冲区溢出漏洞（CNVD-2016-04339、CNVD-2016-04340、CNVD-2016-04347）、Pidgin MXIT 协议拒绝服务漏洞、Pidgin MXIT 协议拒绝服务漏洞（CNVD-2016-04334、CNVD-2016-04335、CNVD-2016-04336、CNVD-2016-04337）等。其中，“Pidgin MXIT 协议缓冲区溢出漏洞（CNVD-2016-04347）”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-2016-04339
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04340
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04347
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04315
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04334
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04335
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04336
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04337

2、WordPress 产品安全漏洞

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，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泄露、进行跨站攻

击、执行未授权操作和发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：WordPress 信息泄露漏洞（CNVD-2016-04364）、WordPress 跨站脚本漏洞（CNVD-2016-04365、CNVD-2016-04366）、WordPress 重定向绕过漏洞、WordPress 拒绝服务漏洞（CNVD-2016-04363）、WordPress Collne Welcart e-Commerce 插件跨站脚本漏洞、WordPress 未授权操作漏洞、WordPress 密码更改漏洞等。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-2016-04364
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04365
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04366
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04367
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04363
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04349
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04319
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04314

3、phpMyAdmin 产品安全漏洞

phpMyAdmin 是 phpMyAdmin 团队开发的一套免费的、基于 Web 的 MySQL 数据库管理工具。本周，该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、进行跨站脚本攻击、执行任意代码和发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：phpMyAdmin 跨站请求伪造漏洞、phpMyAdmin 任意代码执行漏洞、phpMyAdmin 跨站脚本漏洞（CNVD-2016-04396、CNVD-2016-04395、CNVD-2016-04394）、phpMyAdmin SQL 注入漏洞、phpMyAdmin 表结构页跨站脚本漏洞、phpMyAdmin 拒绝服务漏洞等。其中，“phpMyAdmin 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-2016-04398
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04397
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04396
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04395
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04394
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04311
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04310
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04307

4、Symantec 产品安全漏洞

Symantec Endpoint Protection（SEP）是美国赛门铁克（Symantec）公司的一套防

病毒软件。SEP Manager 和 Client 是其中的管理端和客户端软件。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和实施跨站脚本攻击等。

CNVD 收录的相关漏洞包括：Symantec Endpoint Protection Manager 和 Client 服务器端请求伪造漏洞、Symantec Endpoint Protection Manager 跨站脚本漏洞（CNVD-2016-04421）、Symantec Endpoint Protection Manager 跨站请求伪造漏洞、Symantec Endpoint Protection Manager 和 Client 开放重定向漏洞、Symantec Endpoint Protection Manager 和 Client 设计漏洞、Symantec Endpoint Protection Manager 和 Client 信息泄露漏洞、Symantec Endpoint Protection Manager 和 Client 目录遍历漏洞、Symantec Endpoint Protection Client 竞争条件漏洞。其中，“Symantec Endpoint Protection Manager 跨站请求伪造漏洞”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-2016-04422

http://www.cnvd.org.cn/flaw/show/CNVD-2016-04421

http://www.cnvd.org.cn/flaw/show/CNVD-2016-04420

http://www.cnvd.org.cn/flaw/show/CNVD-2016-04419

http://www.cnvd.org.cn/flaw/show/CNVD-2016-04418

http://www.cnvd.org.cn/flaw/show/CNVD-2016-04416

http://www.cnvd.org.cn/flaw/show/CNVD-2016-04415

http://www.cnvd.org.cn/flaw/show/CNVD-2016-04417

5、Netgear 设备 web 界面登录密码泄露漏洞

Netgear 是全球领先的企业网络解决方案，及数字家庭网络应用倡导者。本周，Netgear 被披露存在密码泄露漏洞。允许攻击者利用漏洞获取管理界面登录密码。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-2016-04399

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-2016-04313	Trend Micro Deep Discovery hotfix_upload.cgi 文档名称远程代码执行漏洞	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://esupport.trendmicro.com/solution/en-US/1114281.aspx
CNVD-2016-04321	Unitronics VisiLogic OPLC IDE 栈缓冲区溢出漏洞	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://unitronicsplc.com/software-visilogic/
CNVD-2016-04327	RTMPDump librtmp 远程代码执行漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页：https://rtmpdump.mplayerhq.hu/
CNVD-2016-04344	7zip NArchive::NHfs::CHandler::ExtractZlibFile 方法堆缓冲区溢出漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页：http://www.7-zip.org/
CNVD-2016-04375	libarchive 整数溢出漏洞	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.libarchive.org/
CNVD-2016-04392	Linux kernel 缓冲区溢出漏洞（CNVD-2016-04392）	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.kernel.org/
CNVD-2016-04391	Linux kernel powerpc 系统拒绝服务漏洞	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.kernel.org/
CNVD-2016-04387	Linux kernel nfsd 权限获取漏洞	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：https://git.kernel.org/linus/4ac7249ea5a0ceef9f8269f63f33cc873c3fac61
CNVD-2016-04397	phpMyAdmin 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://www.phpmyadmin.net/security/PMASA-2016-27/
CNVD-2016-04320	Pidgin MXIT 协议缓冲区溢出漏洞	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://pidgin.im/news/security/?id=93

表 4 部分重要高危漏洞列表

小结：本周，Pidgin 产品被披露存在缓冲区溢出和拒绝服务漏洞，攻击者可利用漏洞进行跨站脚本攻击和发起拒绝服务攻击。此外，WordPress、phpMyAdmin、Symantec 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、执行任意代码、造成缓冲区溢出或发起拒绝服务攻击等。另外， Netgear 被披露存在密码泄露漏洞。允许攻击者利用漏洞获取管理界面登录密码。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. Godless 类恶意 APP 可 Root 90%安卓设备

最近，趋势科技的研究人员报告发现了一类恶意应用，并统称为 Godless。它们能 root 掉近 90%的安卓手机。Godless 恶意应用里包含了一些开源或者泄漏的安卓 root 工具，足可以秒杀安卓 5.1 或之前的版本。根据研究人员表示，一旦受害者的设备上安装了 Godless 恶意应用，它就会使用一个叫作“android-rooting-tools”的漏洞框架来获取受害者设备的 root 权限。有了 root 权限，恶意 Godless 应用在接受了远程服务器的指令后，就可以在受害者设备上静默下载安装其他应用。受害用户可能会安装上并不需要的应用，也可能会收到烦人的广告。更糟糕的是，这些恶意应用可能会在设备上安装后门监控用户。因此，为了避免遭受类似恶意应用的侵害，安卓用户应该规避使用第三方应用商店。而我们即使在谷歌官方应用商店下载应用时，也要仔细检查下开发者的信息。

参考链接：http://www.freebuf.com/news/107835.html

2. Swagger 曝远程代码执行漏洞，影响 Java、PHP、NodeJS 等众多开发语言

Swagger 规格被广泛的使用在 Html、PHP、Java 和 Ruby 等流行语言开发的应用中，其最近被曝出远程代码执行漏洞，潜在影响到了 Java、PHP、NodeJS 和 Ruby 等流行语言开发的应用。这个漏洞的 CVE 编号为 CVE-2016-5641。该漏洞属于参数注入漏洞，能够在 Swagger JSON 文件中嵌入恶意代码。如凡是使用 Swagger API 的应用程序都会受到影响。Rapid7 社区的安全研究人员目前公开了该漏洞的技术细节和修补方案。

参考链接：http://www.freebuf.com/news/107790.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