国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2016 年 07 月 11 日-2016 年 07 月 17 日 **2016 年第 29 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 201 个，其中高危漏洞 103 个、中危漏洞 83 个、低危漏洞 15 个。漏洞平均分值为 6.84 分。本周收录的漏洞中，涉及 0day 漏洞 23 个（占 11%）。其中互联网上出现“WECON LeviStudio 堆缓冲区溢出漏洞、Apache struts2 devMode 远程代码执行漏洞”等零日漏洞，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 419 个，与上周（457 个）环比下降 8%。

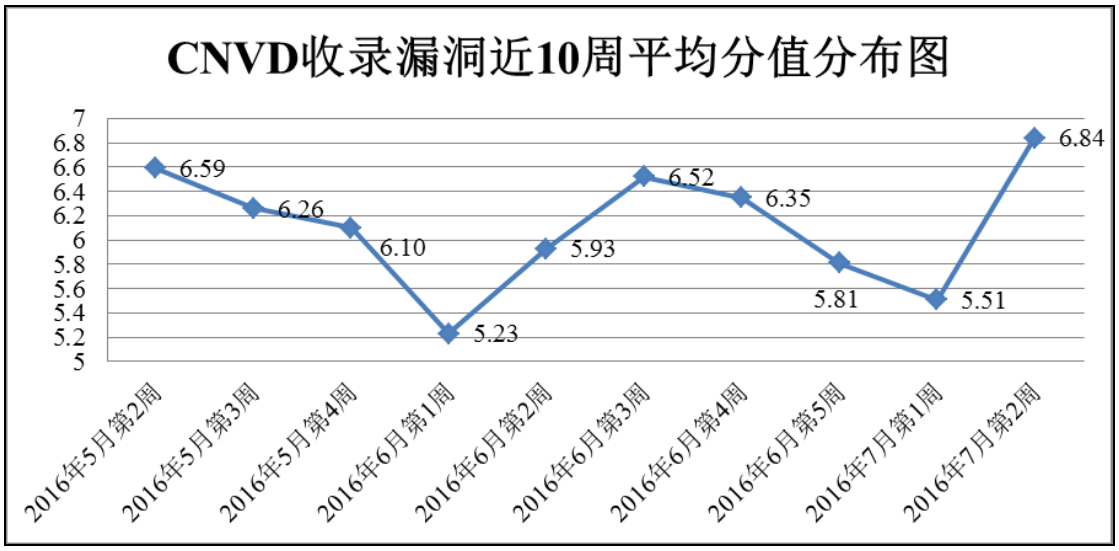

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 8 家成员单位、合作伙伴及企业用户、个人用户报送了本周收录的全部 201 个漏洞。报送情况如表 1 所示。其中，奇虎(补天平台)、启明星辰、天融信、安天实验室等单位报送数量较多。补天平台、乌云、漏洞盒子、深圳市深信服电子科技有限公司、腾讯玄武实验室及其他个人白帽子向 CNVD 提交了 419 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)	337	337
启明星辰	275	0
天融信	255	0
安天实验室	218	0
恒安嘉新	111	21
H3C	74	0
中国电信集团系统集成有限责任公司	40	0
乌云	585	0
漏洞盒子	16	16
深圳市深信服电子科技有限公司	5	5
腾讯玄武实验室	13	13
CNCERT 江西分中心	6	6
CNCERT 宁夏分中心	6	6
个人	15	15
报送总计	1956	419
录入总计	201（去重）	419

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 201 个漏洞。其中操作系统漏洞 102 个，应用程序漏洞 88 个，web 应用漏洞 9 个，网络设备漏洞 13 个， 安全产品漏洞 1 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	102
应用程序漏洞	88
web 应用漏洞	9

网络设备漏洞	1
安全产品漏洞	1

表 2 漏洞按影响类型统计表

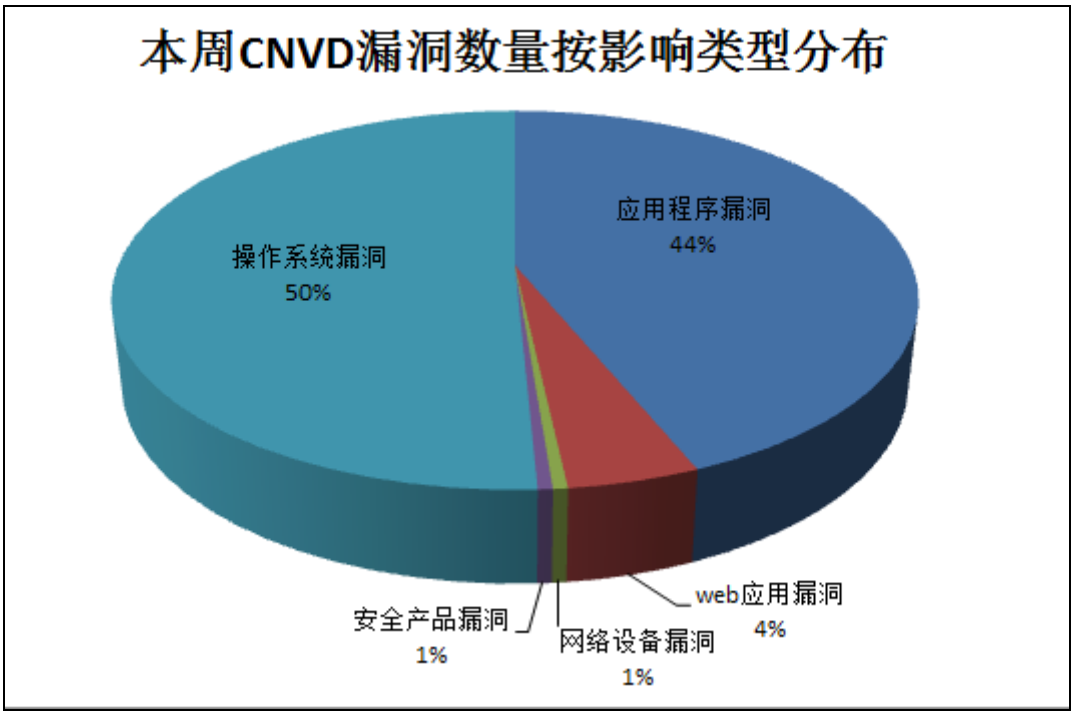

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Adobe、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	Google	98	49%
2	Adobe	21	10%
3	IBM	18	9%
4	Microsoft	16	8%
5	SELTECO	5	2%
6	Pivotal	4	2%
7	Red Hat	2	1%
8	CloudBees	2	1%
9	Pulp	2	1%
10	其他	33	17%

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 1 个电信行业漏洞，99 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，“Android MediaTek Wi-Fi 提权漏洞、Android Qualcomm 组件堆缓冲区溢出漏洞、Android NVIDIA 驱动器权限提升漏洞、Android NFC 权限提升漏洞、Android Sockets 权限提升漏洞、Android Framework APIs 权限提升漏洞、Android libpng 权限提升漏洞、Android ChooserTarget 服务权限提升漏洞、Android sof 权限提升漏洞、Android 内核权限提升漏洞等”的综合评级为“高危”。详情请参照 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/

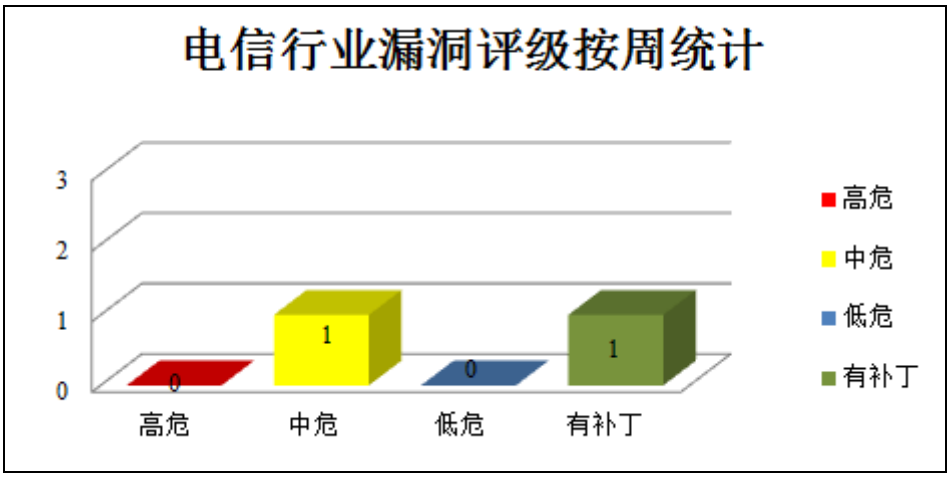

图 3 电信行业漏洞统计

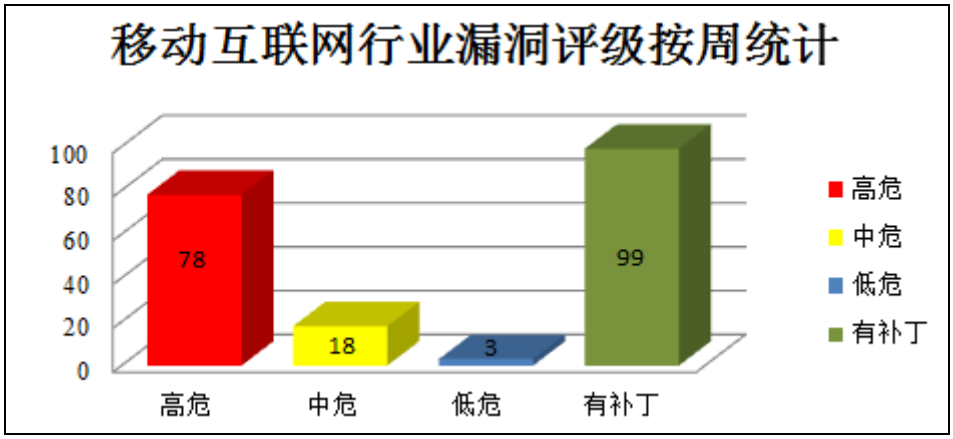

图 4 移动互联网行业漏洞统计

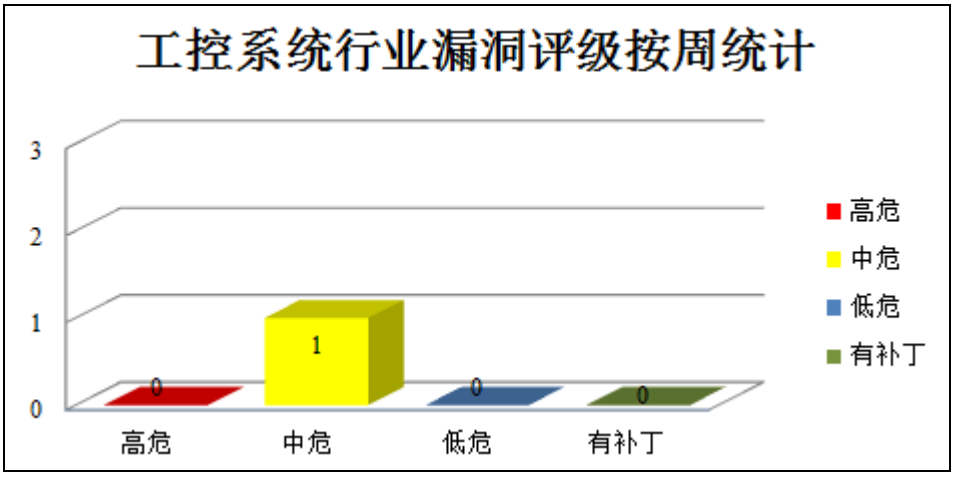

图 5 工控系统行业漏洞统计

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、Microsoft 产品安全漏洞

7 月 12 日，微软发布了 2016 年 7 月份的月度例行安全公告，共含 11 项更新，修复了 Microsoft Windows、Internet Explorer、Edge、Office、Office Service、.NET Framework、Adobe Flash Player 和 Web Apps 中存在的 40 个安全漏洞。其中，6 项远程代码更新的综合评级为最高级“严重”级别。利用上述漏洞，攻击者可提升权限，远程执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft 脚本引擎内存破坏漏洞（CNVD-2016-04792）、Microsoft Windows Win32k 权限提升漏洞（CNVD-2016-04745、CNVD-2016-04746）、Microsoft Windows 打印后台处理程序远程执行代码漏洞、Microsoft Internet Explorer 内存破坏漏洞（CNVD-2016-04805、CNVD-2016-04806、CNVD-2016-04844、CNVD-2016-04843）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/webinfo/show/3890

2、Google 产品安全漏洞

Android on Nexus 5 是美国谷歌（Google）公司和开放手持设备联盟（简称 OHA）共同开发的一套运行于 Nexus 5（智能手机）中并以 Linux 为基础的开源操作系统。Qualcomm 是使用在其中的一个美国高通（Qualcomm）公司的设备专用的高通组件。本周，上述产品被披露存在提权漏洞，攻击者可利用漏洞获取特权。

CNVD 收录的相关漏洞包括：Android Qualcomm 组件提权漏洞（CNVD-2016-04846、CNVD-2016-04847、CNVD-2016-04848、CNVD-2016-04849、CNVD-2016-04850、CNVD-2016-04851、CNVD-2016-04852、CNVD-2016-04853）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-2016-04846
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04847
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04848
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04849
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04850
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04851
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04852
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04853

3、Adobe 产品安全漏洞

Adobe Reader 等都是美国奥多比（Adobe）公司的产品。Adobe Reader 是一款免费的 PDF 文件阅读器；Acrobat 是一款 PDF 文件编辑和转换工具；Acrobat Reader DC 是一套用于查看、打印和批注 PDF 的工具。Classic 和 Continuous 是 Acrobat Reader DC 产品下载中心所提供的两种更新机制。Adobe Flash Player 是美国奥多比（Adobe）公司的一款跨平台、基于浏览器的多媒体播放器产品。本周，上述产品被披露存在内存破坏漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：多款 Adobe 产品内存破坏漏洞（CNVD-2016-04794、CNVD-2016-04796、CNVD-2016-04797、CNVD-2016-04798、CNVD-2016-04799、CNVD-2016-04800、CNVD-2016-04801）、Adobe Flash Player 内存破坏漏洞（CNVD-2016-04757）等。其中，“Adobe Flash Player 内存破坏漏洞（CNVD-2016-04757）”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-2016-04794
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04796
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04797
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04798
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04799
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04800
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04801
http://www.cnvd.org.cn/flaw/show/CNVD-2016-04757

4、IBM 产品安全漏洞

IBM Security Identity Manager（ISIM）是美国 IBM 公司的一套身份管理和治理解决方案。IBM Jazz Reporting Service 是 IBM Rational Reporting for Development Intelligence 的可选组件。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

权限、泄露敏感信息和实施跨站脚本攻击等。

CNVD 收录的相关漏洞包括：IBM Security Identity Manager 权限获取漏洞、IBM Security Identity Manager 信息泄露漏洞、IBM Security Identity Manager 用户伪造漏洞、IBM Security Identity Manager 设计漏洞、IBM Jazz Reporting Service (JRS)跨站请求伪造漏洞、IBM Jazz Reporting Service (JRS)跨站脚本漏洞（CNVD-2016-04651、CNVD-2016-04650）、IBM Jazz Reporting Service (JRS)跨站脚本漏洞等。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-2016-04750

http://www.cnvd.org.cn/flaw/show/CNVD-2016-04752

http://www.cnvd.org.cn/flaw/show/CNVD-2016-04753

http://www.cnvd.org.cn/flaw/show/CNVD-2016-04754

http://www.cnvd.org.cn/flaw/show/CNVD-2016-04652

http://www.cnvd.org.cn/flaw/show/CNVD-2016-04651

http://www.cnvd.org.cn/flaw/show/CNVD-2016-04650

http://www.cnvd.org.cn/flaw/show/CNVD-2016-04648

5、Apache struts2 devMode 远程代码执行漏洞

Apache Struts 是美国阿帕奇（Apache）软件基金会负责维护的一个开源项目，是一套用于创建企业级 Java Web 应用的开源 MVC 框架。本周，Apache 被披露存在远程代码执行漏洞。允许攻击者利用漏洞远程执行任意命令。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-2016-04656

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-2016-04735	Symantec CIDS Driver PE 文件内存破坏漏洞	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.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20160707_01
CNVD-2016-04742	Spring Boot 框架 SPEL 表达式注入漏洞	高	厂商已发布了升级程序修复该漏洞，CNVD 建议用户将程序升级至 Spring Boot 1.3.1 及以上版本：https://github.com/spring-projects/spring-boot/commit/edb16a13ee33e62b

			046730a47843cb5dc92054e6
CNVD-2016-04665	Android NFC 权限提升漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://source.android.com/security/bulletin/2016-07-01.html
CNVD-2016-04666	Android socket 权限提升漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://source.android.com/security/bulletin/2016-07-01.html
CNVD-2016-04667	Android Kernel Video Driver 权限提升漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://source.android.com/security/bulletin/2016-07-01.html
CNVD-2016-04668	Android Kernel File System 权限提升漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://source.android.com/security/bulletin/2016-07-01.html
CNVD-2016-04662	Android MediaTek 视频驱动提权漏洞	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://source.android.com/security/bulletin/2016-07-01.html
CNVD-2016-04663	Android Qualcomm Wi-Fi 驱动提权漏洞	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://source.android.com/security/bulletin/2016-07-01.html
CNVD-2016-04675	Android Framework APIs 权限提升漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://source.android.com/security/bulletin/2016-07-01.html
CNVD-2016-04677	Android libpng 权限提升漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://source.android.com/security/bulletin/2016-07-01.html

表 4 部分重要高危漏洞列表

小结：7 月 12 日，微软发布了 2016 年 7 月份的月度例行安全公告，共含 11 项更新，修复了 Microsoft Windows、Internet Explorer、Edge、Office、Office Service、.NET Framework、Adobe Flash Player 和 Web Apps 中存在的 40 个安全漏洞。其中，6 项远程代码更新的综合评级为最高级“严重”级别。利用上述漏洞，攻击者可提升权限，远程执行任意代码。此外，Google、Adobe、IBM 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、实施跨站脚本攻击、执行任意代码或发起拒绝服务攻击等。另外，Apache 被披露存在远程代码执行漏洞。允许攻击者利用漏洞远程执行任意命令。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. 1.4 亿小米手机受远程执行代码漏洞影响

小米智能手机正面临一个新型的远程执行代码（RCE）漏洞威胁，该漏洞存在于旧版 MIUI 分析套件中，被 MIUI 的多个应用程式使用，攻击者可利用该漏洞获取对手机的完全控制权。小米方面早些时候释出 MIUI 7.2 全球稳定版意图修补该漏洞，并呼吁用户尽快更新。

参考链接：http://www.freebuf.com/news/108995.html

2. 宝马车载娱乐系统 ConnectedDrive 曝远程操控 0day 漏洞

ConnectedDrives 是宝马车载信息娱乐系统，该系统可以通过移动 APP 来管理车辆。Vulnerability 实验室的安全研究员 BenjaminKunz Mejri 在向宝马官方提交漏洞五个月后（官方还是没打补丁），昨日公布了 ConnectedDrive 的两个 Web 0day 漏洞。第一个是会话劫持漏洞，Mejri 表示他这种攻击可以绕过 VIN 会话验证，然后使用另一个 VIN 接入访问以编辑其他用户的汽车设置，恶意用户可以借此获取另一用户的 VIN（车辆识别号）。第二个漏洞出现在门户页面上重置密码处，也就是 passwordResetOk.html 文件。远程操作的黑客可以将自己的 payload 以 GET 方式发送过去，注入到该客户端 WEB 界面中。

参考链接：http://www.freebuf.com/vuls/108841.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