国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2017 年 05 月 29 日-2017 年 06 月 04 日 **2017 年第 23 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 157 个，其中高危漏洞 54 个、中危漏洞 95 个、低危漏洞 8 个。漏洞平均分值为 6.23。本周收录的漏洞中，涉及 0day 漏洞 16 个（占 10%），其中互联网上出现“CERIO DT-100G-N/DT-300N/CW-300N 存在多个漏洞、D-Link DIR-600M 身份验证绕过漏洞”等零日代码攻击漏洞。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 766 个，与上周（561）环比增长 37%。

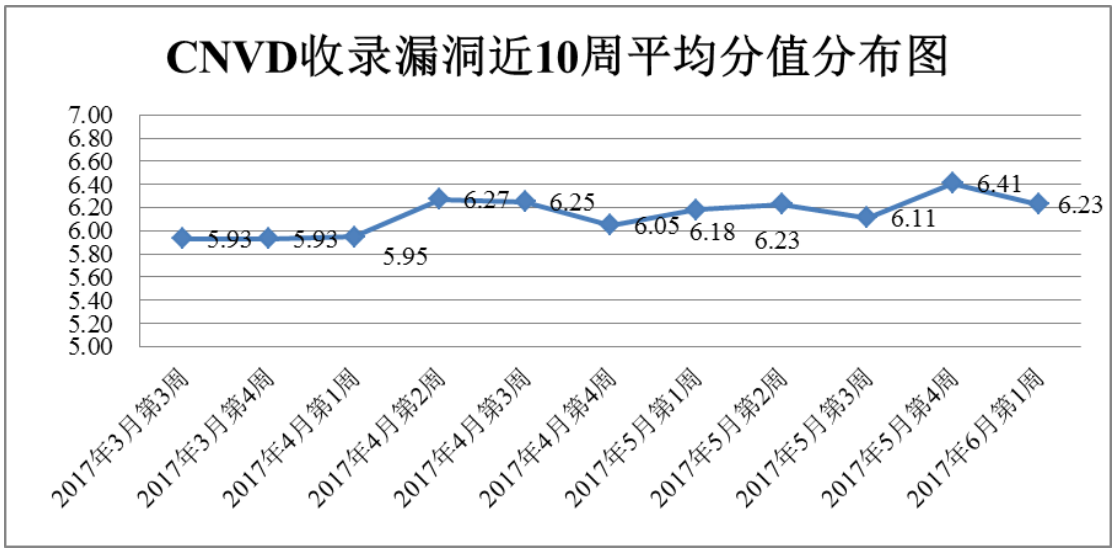

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 19 家成员单位、企业用户及个人用户报送了本周收录的全部 157 个漏洞。报送情况如表 1 所示。其中，启明星辰、华为技术有限公司、天融信、安天实验室、恒安嘉新等单位报送数量较多。360 网神、漏洞盒子、六壬网安、中新网络信息安全股份有

限公司、清远职业技术学院、河北网信智安信息技术有限公司、江西安服信息产业有限公司、杭州朔方信息技术有限公司、安徽新华博信息技术股份有限公司、广州软云计算机科技有限公司、江苏君立华域信息安全技术有限公司及其他个人白帽子向 CNVD 提交了 766 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	240	240
启明星辰	119	0
华为技术有限公司	86	0
天融信	74	2
安天实验室	70	0
恒安嘉新	67	0
东软	64	0
H3C	51	0
漏洞盒子	83	83
杭州安恒信息技术有限公司	28	0
厦门服云信息科技有限公司	17	1
中国电信集团系统集成有限责任公司	15	0
绿盟科技	9	0
北京数字观星科技有限公司	5	0
知道创宇	5	3
阿里云计算有限公司	3	0
广西鑫瀚科技有限公司	2	2
南京铱迅信息技术股份有限公司	1	1
西安四叶草信息技术有限公司	1	1

六壬网安	23	23
中新网络信息安全股份有限公司	22	22
清远职业技术学院	19	19
河北网信智安信息技术有限公司	6	6
江西安服信息产业有限公司	6	6
杭州朔方信息技术有限公司	4	4
安徽新华博信息技术股份有限公司	3	3
广州软云计算机科技有限公司	3	3
江苏君立华域信息安全技术有限公司	3	3
CNCERT 福建分中心	4	4
CNCERT 河北分中心	1	1
CNCERT 宁夏分中心	1	1
CNCERT 浙江分中心	1	1
个人	337	337
报送总计	1373	766
录入总计	157（去重）	766

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 157 个漏洞。其中应用程序漏洞 79 个，操作系统漏洞 49 个，web 应用漏洞 22 个，网络设备漏洞 5 个，数据库漏洞 1 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	79
操作系统漏洞	49
web 应用漏洞	22
网络设备漏洞	5
数据库漏洞	1

安全产品漏洞	1

表 2 漏洞按影响类型统计表

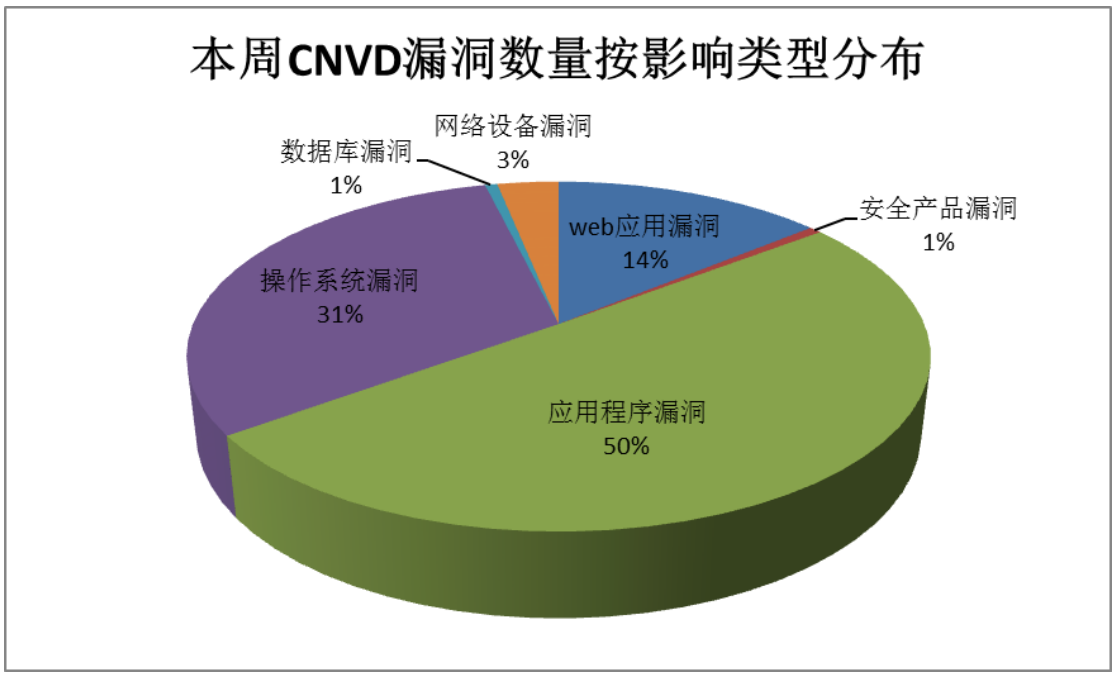

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Apple、Cisco、ImageWorsener 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	55	35%
2	Cisco	10	6%
3	ImageWorsener	9	6%
4	Oracle	9	6%
5	VirusTotal	4	2%
6	Atlassian	3	2%
7	IBM	3	2%
8	QPDF	3	2%
9	RoundCube	3	2%
10	其他	58	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 个电信行业漏洞，35 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，“Fortinet FortiWLC-SD 权限提升漏洞、Schneider Electric Wonderware InduSoft Web Studio 权限提升漏洞、Apple macOS Sierra iBooks 权限提升漏洞、多款 Apple 产品 Foundation 组件内存破坏漏洞、Apple macOS Sierra IOSurface 权限提升漏洞”等的综合评级为“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/

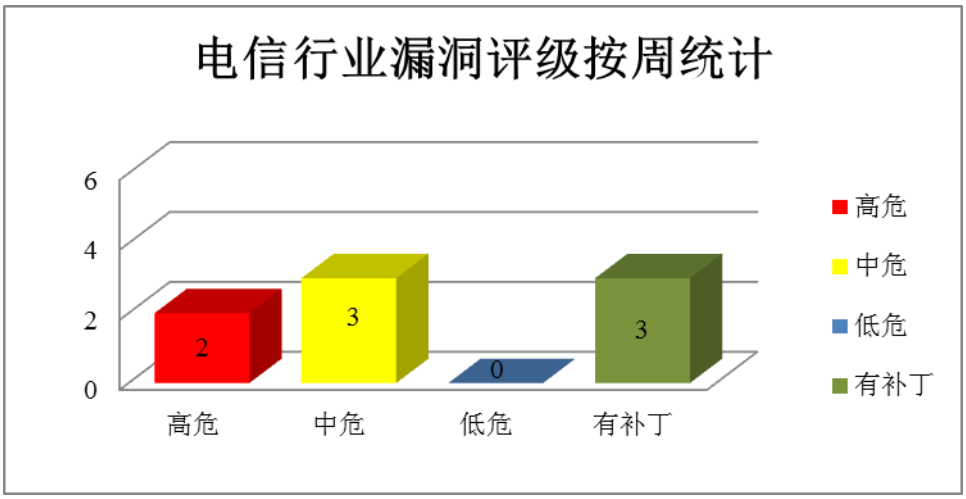

图 3 电信行业漏洞统计

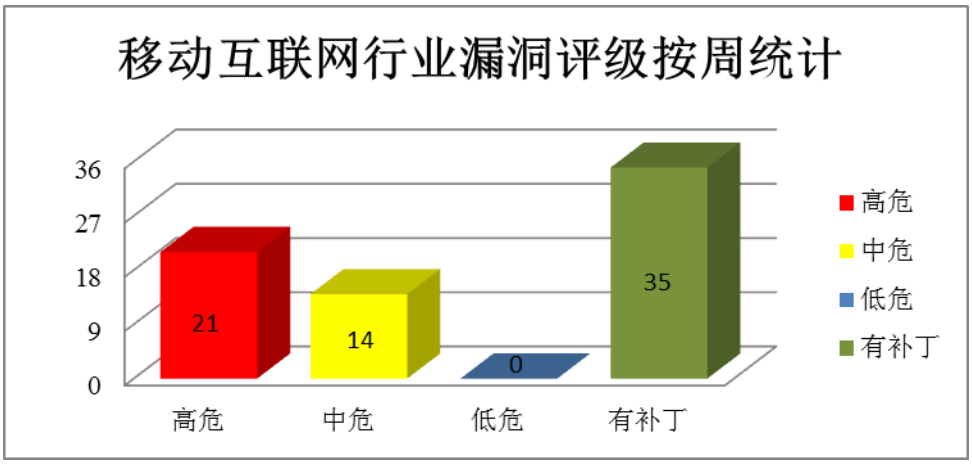

图 4 移动互联网行业漏洞统计

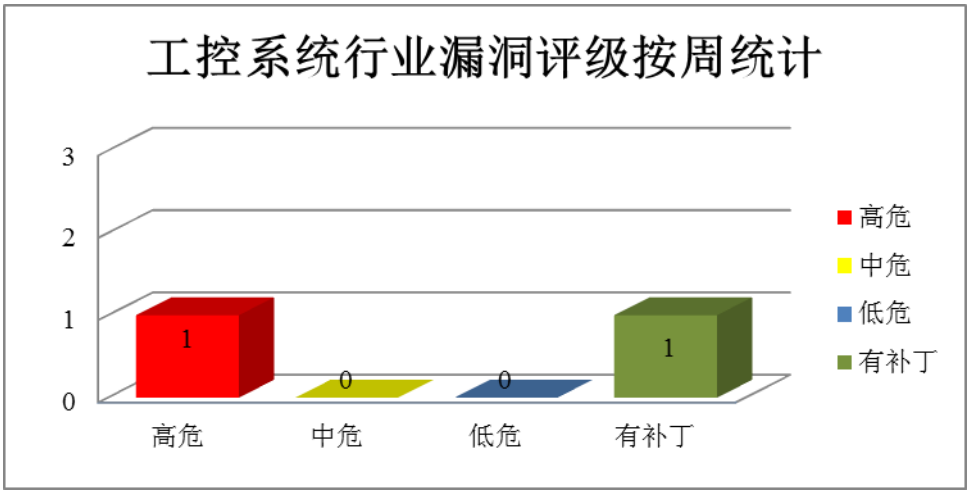

图 5 工控系统行业漏洞统计

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、Apple 产品安全漏洞

Apple iOS 是为移动设备所开发的一套操作系统；Safari 是一款 Web 浏览器；tvOS 是一套智能电视操作系统。WebKit 是 KDE 社区开发的一套开源 Web 浏览器引擎；watchOS 是一套智能手表操作系统；AVEVideoEncoder 是其中的一个视频编码器。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的代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：多款 Apple 产品 WebKit 组件内存破坏漏洞（CNVD-2017-07721、CNVD-2017-07722、CNVD-2017-07723、CNVD-2017-07724、CNVD-2017-07725）、多款 Apple 产品 AVEVideoEncoder 组件内存破坏漏洞（CNVD-2017-07726、CNVD-2017-07727、CNVD-2017-07728）。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-2017-07721

http://www.cnvd.org.cn/flaw/show/CNVD-2017-07722

http://www.cnvd.org.cn/flaw/show/CNVD-2017-07723

http://www.cnvd.org.cn/flaw/show/CNVD-2017-07724

http://www.cnvd.org.cn/flaw/show/CNVD-2017-07725

http://www.cnvd.org.cn/flaw/show/CNVD-2017-07726

http://www.cnvd.org.cn/flaw/show/CNVD-2017-07727

http://www.cnvd.org.cn/flaw/show/CNVD-2017-07728

2、Cisco 产品安全漏洞

Cisco Remote Expert Manager Software 是美国思科（Cisco）公司的的一款远程管理软件，Cisco Prime Collaboration 是综合性视频及声音服务保障及管理系统。本周，上述产品被披露存在目录遍历、拒绝服务和信息泄露漏洞，攻击者可利用漏洞泄露敏感信息或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco Prime Collaboration Provisioning 目录遍历漏洞、Cisco Prime Collaboration Provisioning 目录遍历任意文件删除漏洞、Cisco Remote Expert Manager 拒绝服务漏洞、Cisco Remote Expert Manager 临时文件信息泄露漏洞、Cisco Remote Expert Manager 信息泄露漏洞、Cisco Remote Expert Manager 信息泄露漏洞（CNVD-2017-08157、CNVD-2017-08155）、Cisco Remote Expert Manager 虚拟目标信息泄露漏洞。其中“Cisco Prime Collaboration Provisioning 目录遍历漏洞、Cisco Prime Collaboration Provisioning 目录遍历任意文件删除漏洞”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-2017-07745
http://www.cnvd.org.cn/flaw/show/CNVD-2017-08158
http://www.cnvd.org.cn/flaw/show/CNVD-2017-08151
http://www.cnvd.org.cn/flaw/show/CNVD-2017-08152
http://www.cnvd.org.cn/flaw/show/CNVD-2017-08156
http://www.cnvd.org.cn/flaw/show/CNVD-2017-08157
http://www.cnvd.org.cn/flaw/show/CNVD-2017-08155
http://www.cnvd.org.cn/flaw/show/CNVD-2017-08154

3、Oracle 产品安全漏洞

Oracle PeopleSoft Products 是美国甲骨文（Oracle）公司的一套企业人力资本管理解决方案。Oracle Hospitality Applications 是一套用于酒店管理的业务应用程序、服务器和存储解决方案。Oracle Utilities Applications 是一套为电气、燃气和水务等公司提供运营应用和云服务的解决方案。Oracle Communications Security Gateway 为语音和数据的传输提供安全保障。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞影响数据的完整性、保密性和可用性。

CNVD 收录的相关漏洞包括：Oracle Automatic Service Request 本地漏洞（CNVD-2017-08075）、Oracle Communications Security Gateway 远程漏洞、Oracle Hospitality OPERA 5 Property Services 远程漏洞（CNVD-2017-08076、CNVD-2017-08077）、Oracle PeopleSoft Enterprise SCM Service Procurement 远程漏洞、Oracle PeopleSoft Products PeopleSoft Enterprise SCM Purchasing 远程漏洞、Oracle Real-Time Scheduler 远程漏洞。其中“Oracle Automatic Service Request 本地漏洞（CNVD-2017-08075）”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-2017-08075

http://www.cnvd.org.cn/flaw/show/CNVD-2017-08111

http://www.cnvd.org.cn/flaw/show/CNVD-2017-08076

http://www.cnvd.org.cn/flaw/show/CNVD-2017-08077

http://www.cnvd.org.cn/flaw/show/CNVD-2017-08074

http://www.cnvd.org.cn/flaw/show/CNVD-2017-08113

http://www.cnvd.org.cn/flaw/show/CNVD-2017-08105

4、Trend Micro Deep Security 存在多个漏洞

Trend Micro Deep Security 是一种在虚拟、云计算和传统的数据中心环境之间统一安全性的服务器和应用程序防护软件。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞泄露敏感信息，提升权限或执行任意代码。

CNVD 收录的相关漏洞包括：Trend Micro Deep Security 存在多个漏洞。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-2017-07718

5、WordPress Powerplay Gallery 插件文件上传漏洞

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，WordPress 被披露存在文件上传漏洞，攻击者可利用漏洞创建任意目录。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-2017-07717

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-2017-07739	VMware Workstation Pro for Linux 和 VMware Workstation Player for Linux 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.vmware.com/security/advisories/VMSA-2017-0009.html
CNVD-2017-07752	Silicon Graphics LibTIFF 堆缓冲区溢出漏洞（CNVD-2017-07752）	高	暂无
CNVD-2017-07975	PHPCMS v9.6.3 存在文件包含漏洞	高	暂无
CNVD-2017-08070	Fortinet FortiWLC-SD 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：http://fortiguard.com/psirt/FG-IR-17-0

			97
CNVD-2017-08085	Sitecore CRM 代码执行漏洞	高	暂无
CNVD-2017-08087	SAP Business Intelligence SQL 注入漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://erpscan.com/press-center/blog/sap-cyber-threat-intelligence-report-january-2017/
CNVD-2017-08088	Magento CMS 'RetrieveImage.php'任意文件上传漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：http://www.magentocommerce.com
CNVD-2017-08106	Zimbra Collaboration Suite 存在未明权限提升漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories
CNVD-2017-08166	Schneider Electric Wonderware InduSoft Web Studio 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：http://www.indusoft.com/Products-Downloads
CNVD-2017-08169	Apache jUDDI 开放重定向漏洞	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://juddi.apache.org/security.html

表 4 部分重要高危漏洞列表

小结：本周，Apple 被披露存在内存破坏漏洞，攻击者可利用漏洞执行任意的代码或发起拒绝服务攻击。此外，Cisco 、Oracle、Trend Micro 等多款产品被披露存在多个漏洞，攻击者利用漏洞可执行任意代码、泄露敏感信息、提升权限或发起拒绝服务攻击等。另外，Wordpress 被披露存在文件上传漏洞，攻击者可利用漏洞创建任意目录。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. Oracle Responsys 本地文件包含漏洞

Oracle Responsys 云服务系统中存在一个本地文件包含漏洞（LFI）。由于当前很多商业销售、网络存储和社交关系公司都采用了 Oracle Responsys 的云解决方案，所以，该漏洞对多个知名公司服务造成影响，这些公司包括 Facebook、Linkedin、Dropbox 等。由于对代码和系统架构的审查和过滤不当，攻击者可通过目录遍历字符的注入从而获取到目标服务器相关信息。

参考链接：http://www.freebuf.com/vuls/135512.html

2. SELinux 用户执行 sudo 命令可获取 root 权限

该高危漏洞 CVE-2017-1000367 发生在 Linux 的 Sudo 命令中的 get_process_ttyn

ame() 函数中。攻击者可以利用这个漏洞，让普通用户在使用 Sudo 命令获得临时权限时执行一些操作，将他们的权限提升到 root 级别。在运用 SELinux 机制的系统上，Sudo 用户可以使用命令行的输出提升自己的用户权限，还可以在文件系统中覆盖文件系统中的文件（甚至覆盖由 root 用户所拥有的文件）。

参考链接：http://www.freebuf.com/vuls/136156.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