国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2017 年 07 月 24 日-2017 年 07 月 30 日 **2017 年第 31 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 276 个，其中高危漏洞 102 个、中危漏洞 163 个、低危漏洞 11 个。漏洞平均分值为 6.30。本周收录的漏洞中，涉及 0day 漏洞 37 个（占 13%），其中互联网上出现“WebsiteBaker 任意 PHP 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 2841 个。

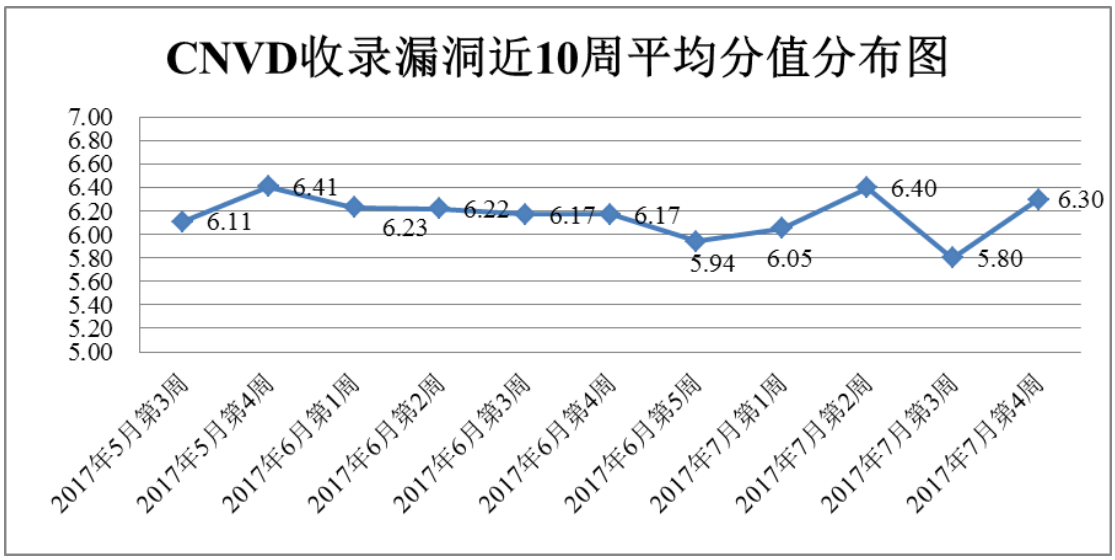

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 18 家成员单位、企业用户及个人用户报送了本周收录的全部 276 个漏洞。报送情况如表 1 所示。其中，H3C、天融信、恒安嘉新、安天实验室、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、南京联成科技发展股份有限公司、安徽新华博信息技术股份有限公司、中新网络信息安全股份有限公司、山

石网科通信技术有限公司、江苏同袍信息科技有限公司、山东安云信息技术有限公司、深圳鼎安天下信息科技有限公司、网信智安、君立华域、六壬网安、广州神月信息安全技术有限公司、江西安服信息产业有限公司、上海观安信息技术有限公司、中电长城网际系统应用有限公司、北京安码科技有限公司、中国航天科工集团第四研究院软件评测中心（北京）、上海犇众信息技术有限公司及其他个人白帽子向 CNVD 提交了 2841 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	1238	1238
漏洞盒子	261	261
H3C	259	0
天融信	189	1
恒安嘉新	172	0
安天实验室	107	0
中国电信集团系统集成有限责任公司	84	12
启明星辰	84	10
绿盟科技	63	0
华为技术有限公司	60	0
杭州安恒信息技术有限公司	55	0
厦门服云信息科技有限公司	23	0
南京铱迅信息技术股份有限公司	14	14
深圳市深信服电子科技有限公司	7	7
北京数字观星科技有限公司	5	0
知道创宇	4	4
广西鑫瀚科技有限公司	3	3
深圳市腾讯计算机系统有限公司（玄武实验室）	2	2

南京联成科技发展股份有限公司	36	36
安徽新华博信息技术股份有限公司	25	25
中新网络信息安全股份有限公司	19	19
山石网科通信技术有限公司	19	19
江苏同袍信息科技有限公司	11	11
山东安云信息技术有限公司	8	8
深圳鼎安天下信息科技有限公司	8	8
网信智安	7	7
君立华域	6	6
六壬网安	5	5
广州神月信息安全技术有限公司	4	4
江西安服信息产业有限公司	2	2
上海观安信息技术有限公司	2	2
中电长城网际系统应用有限公司	2	2
北京安码科技有限公司	1	1
中国航天科工集团第四研究院软件评测中心（北京）	1	1
上海犇众信息技术有限公司	1	1
CNCERT 广东分中心	3	3
吉林分中心	2	2
个人	1127	1127
报送总计	3919	2841
录入总计	276（去重）	2841

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 276 个漏洞。其中应用程序漏洞 118 个，操作系统漏洞 113 个，数据库漏洞 18 个，网络设备漏洞 12 个，web 应用漏洞 11 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	118
操作系统漏洞	113
数据库漏洞	18
网络设备漏洞	12
web 应用漏洞	11
安全产品漏洞	4

表 2 漏洞按影响类型统计表

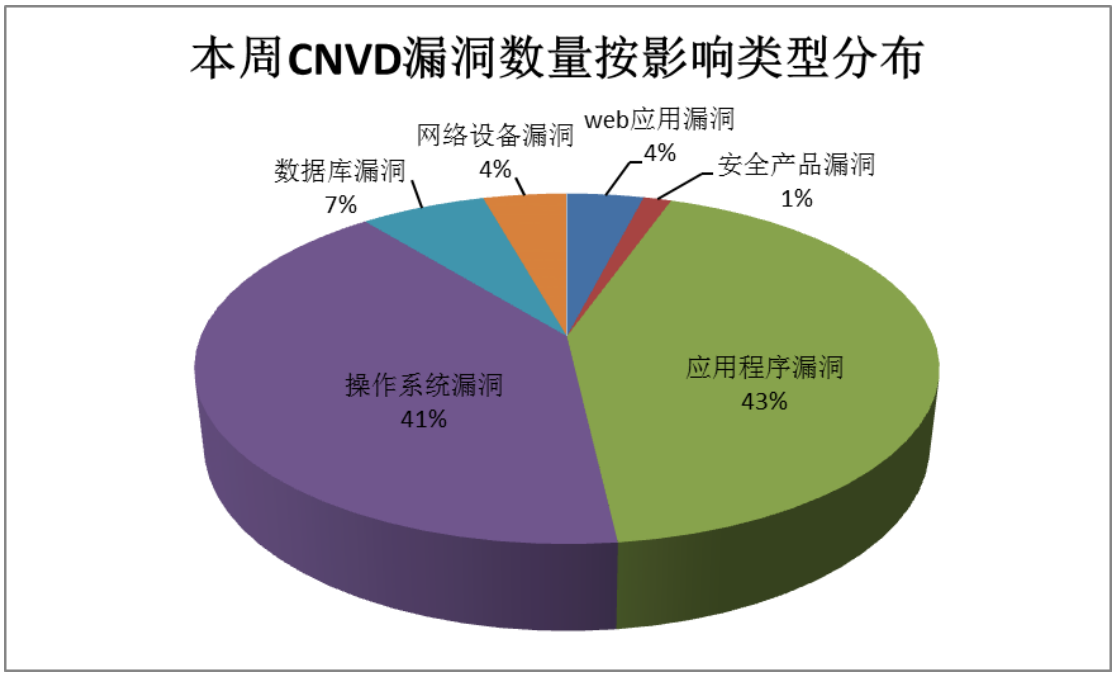

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Apple、Google、Microsoft 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	64	23%
2	Google	34	12%
3	Microsoft	18	7%
4	Oracle	17	6%
5	ImageMagick	15	5%
6	Cisco	10	4%

7	FreeRADIUS	10	4%
8	Exiv2	5	2%
9	Linux	4	1%
10	其他	99	36%

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 20 个电信行业漏洞，83 个移动互联网行业漏洞，3 个工控系统行业漏洞（如下图所示）。其中，“Google Android 竞争条件漏洞、Google Android Secure Display 竞争条件漏洞、多款 Apple 产品 Contacts 缓冲区溢出漏洞、Lenovo VIBE nac_server 组件本地提权漏洞、Google Android 整数溢出漏洞（CNVD-2017-16015）”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/

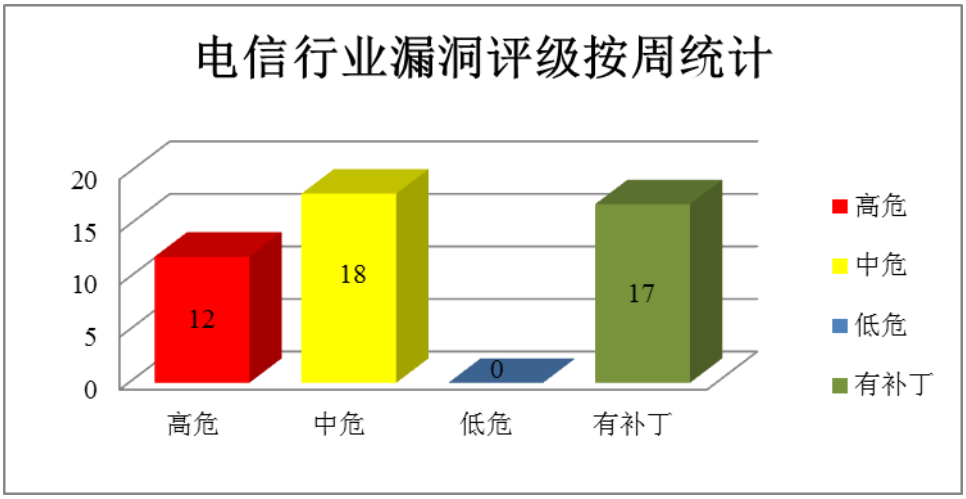

图 3 电信行业漏洞统计

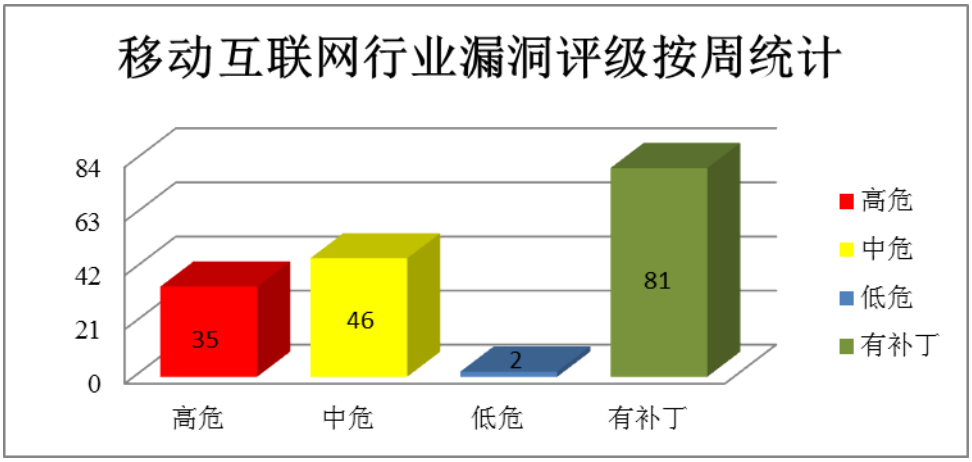

图 4 移动互联网行业漏洞统计

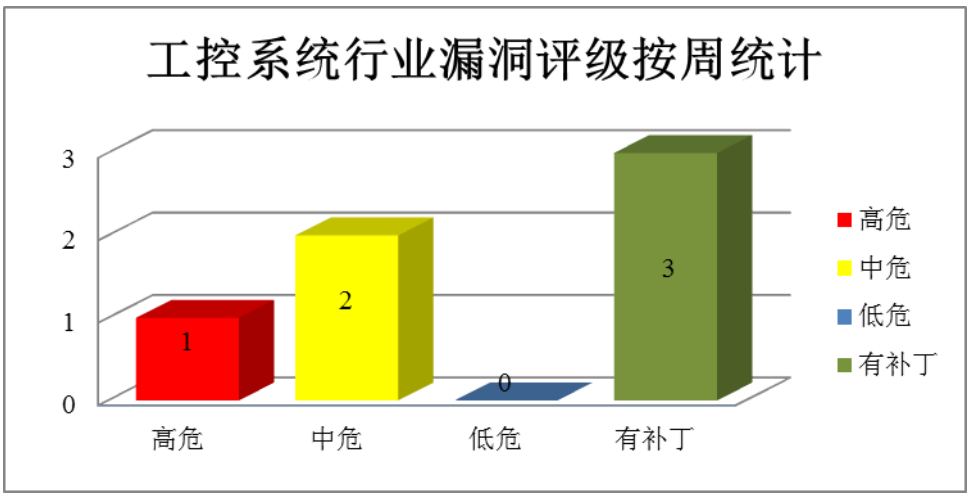

图 5 工控系统行业漏洞统计

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 是为专移动设备所开发的一套操作系统；Safari 是一款 Web 浏览器，是 Mac OS X 和 iOS 操作系统附带的默认浏览器。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。Kernel 是其中的一个内核组件。本周，上述产品被披露存在内存破坏漏洞等，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：多款 Apple 产品 WebKit 内存破坏漏洞（CNVD-2017-16610、CNVD-2017-16611、CNVD-2017-16615、CNVD-2017-16619）、多款 Apple 产品 Kernel 内存破坏漏洞（CNVD-2017-16869、CNVD-2017-16870、CNVD-2017-16871、CNVD-2017-16872）。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-2017-16610
http://www.cnvd.org.cn/flaw/show/CNVD-2017-16611
http://www.cnvd.org.cn/flaw/show/CNVD-2017-16615
http://www.cnvd.org.cn/flaw/show/CNVD-2017-16619
http://www.cnvd.org.cn/flaw/show/CNVD-2017-16869
http://www.cnvd.org.cn/flaw/show/CNVD-2017-16870
http://www.cnvd.org.cn/flaw/show/CNVD-2017-16871
http://www.cnvd.org.cn/flaw/show/CNVD-2017-16872

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。Media framework 是其中的一个用于多媒体开发框架。本周，该产品被披露存在远程代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Google Android media framework 远程代码执行漏洞（CNVD-2017-15961、CNVD-2017-15962、CNVD-2017-15963、CNVD-2017-15964、CNVD-2017-15965、CNVD-2017-15966、CNVD-2017-15967、CNVD-2017-15968）。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-2017-15961
http://www.cnvd.org.cn/flaw/show/CNVD-2017-15962
http://www.cnvd.org.cn/flaw/show/CNVD-2017-15963
http://www.cnvd.org.cn/flaw/show/CNVD-2017-15964
http://www.cnvd.org.cn/flaw/show/CNVD-2017-15965
http://www.cnvd.org.cn/flaw/show/CNVD-2017-15966
http://www.cnvd.org.cn/flaw/show/CNVD-2017-15967
http://www.cnvd.org.cn/flaw/show/CNVD-2017-15968

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。Explorer 是其中的一个 Windows 操作系统附带的默认浏览器。Microsoft Office 是一套基于 Windows 操作系统的办公软件套装。Microsoft Edge 是其中的一款系统附带的 Web 浏览器。本周，上述产品被披露存在内存破坏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 Office 内存破坏漏洞（CNVD-2017-15998、CNVD-2017-15999）、Microsoft Office 远程代码执行漏洞（CNVD-2017-16982、CNVD-2017-16983）、Microsoft Windows PowerShell 远程代码执行漏洞、Microsoft Windows Search 远程代码执行漏洞、Microsoft Edge 远程内存破坏漏洞（CNVD-2017-16997）、M

icrosoft Windows Explorer 远程代码执行漏洞。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-2017-15998
http://www.cnvd.org.cn/flaw/show/CNVD-2017-15999
http://www.cnvd.org.cn/flaw/show/CNVD-2017-16982
http://www.cnvd.org.cn/flaw/show/CNVD-2017-16983
http://www.cnvd.org.cn/flaw/show/CNVD-2017-16989
http://www.cnvd.org.cn/flaw/show/CNVD-2017-16990
http://www.cnvd.org.cn/flaw/show/CNVD-2017-16997
http://www.cnvd.org.cn/flaw/show/CNVD-2017-17009

4、Oracle 产品安全漏洞

Oracle MySQL 是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。MySQL Server component 是其中的服务器组件。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：Oracle MySQL Server 拒绝服务漏洞（CNVD-2017-17010、CNVD-2017-17011、CNVD-2017-17012、CNVD-2017-17013、CNVD-2017-17017、CNVD-2017-17189、CNVD-2017-17190、CNVD-2017-17191）。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-2017-17010
http://www.cnvd.org.cn/flaw/show/CNVD-2017-17011
http://www.cnvd.org.cn/flaw/show/CNVD-2017-17012
http://www.cnvd.org.cn/flaw/show/CNVD-2017-17013
http://www.cnvd.org.cn/flaw/show/CNVD-2017-17017
http://www.cnvd.org.cn/flaw/show/CNVD-2017-17189
http://www.cnvd.org.cn/flaw/show/CNVD-2017-17190
http://www.cnvd.org.cn/flaw/show/CNVD-2017-17191

5、TP-Link PTWR841N V8 路由器配置服务逻辑漏洞

TP-Link PTWR841N V8 是一款无线路由器。本周，TP-Link 被披露存在逻辑漏洞，攻击者可利用漏洞修改路由器的设置，将流量重新路由到恶意服务器。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-2017-16354

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-2017-16035	Ocaml 提权漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://caml.inria.fr/mantis/view.php?id=7557
CNVD-2017-16247	nuevoMailer 'r'参数 SQL 注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.nuevomailer.com/
CNVD-2017-16344	Foscam IP Video Camera 栈缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：http://www.foscam.com/
CNVD-2017-16343	EMC VASA Provider Virtual Appliance 远程代码执行漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：http://www.securityfocus.com/bid/99169
CNVD-2017-16365	Drupal Services 模块 SQL 注入漏洞	高	用户可联系供应商获得补丁信息：https://www.drupal.org/
CNVD-2017-16369	Xen 'shadow/common.c'权限提升漏洞	高	用户可联系供应商获得补丁信息：http://www.xenproject.org/
CNVD-2017-16976	FreeRADIUS data2vp_wimax()写入溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://freeradius.org/security/fuzzer-2017.html
CNVD-2017-16971	FreeRADIUS 'rad_coalesce()'写入溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://freeradius.org/security/fuzzer-2017.html
CNVD-2017-16977	FreeRADIUS 拒绝服务漏洞（CNVD-2017-16977）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://freeradius.org/security/fuzzer-2017.html
CNVD-2017-17235	ImageMagick 'ReadOneJNGImage'函数 CPU 耗尽漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/ImageMagick/ImageMagick/issues/526

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等，攻击者可利用漏洞执行任意代码或发起拒绝服务攻击。此外，Google、Microsoft、Oracle 等多款产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码或发起拒绝服务攻击等。另外，TP-Link 被披露存在逻辑漏洞，攻击者可利用漏洞修改路由器的设置，将流量重新路由到恶意服务器。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. Uber SSO 系统存在身份认证绕过漏洞

Uber 近期部署在网站 auth.uber.com 上，基于 Uber 所有子域名 cookie 共享实现认证的单点登录系统（SSO）也存在安全问题，攻击者可通过入侵控制任意一个*.uber.com 子域名进行会话 cookie 窃取。因此，这两个问题的综合应用将造成对 Uber 整个 SSO 系统的身份认证绕过，实现对所有 Uber 子域名网站的访问控制，影响甚大。

参考链接：http://www.freebuf.com/news/141630.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