

信息安全漏洞周报

2017 年 10 月 23 日-2017 年 10 月 29 日

2017 年第 44 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 482 个，其中高危漏洞 127 个、中危漏洞 326 个、低危漏洞 29 个。漏洞平均分为 5.82。本周收录的漏洞中，涉及 0day 漏洞 103 个（占 21%），其中互联网上出现“WordPress eventr SQL 注入漏洞、GNOME libgedit.a 文件拒绝服务漏洞”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 853 个，与上周（635 个）环比增长 34%。

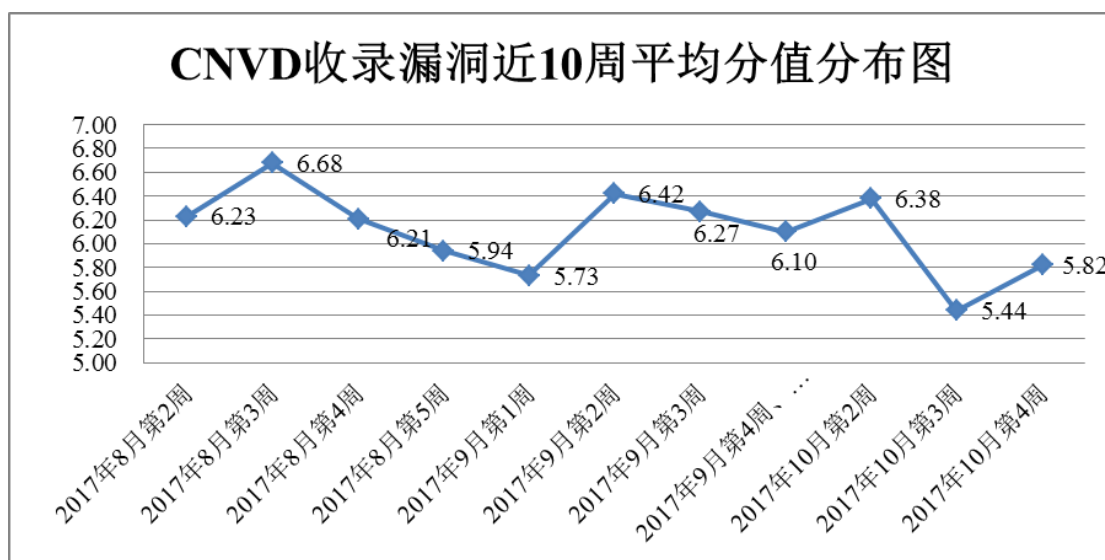


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，H3C、天融信、安天实验室、华为技术有限公司、恒安嘉新等单位报送数量较多。深圳市鼎安天下信息科技有限公司、四川虹微技术有限公司（子午攻防实验室）、中新网络信息安全股份有限公司、福建榕基软件股份有限公

司、广州万方计算机科技有限公司、江苏同袍信息科技有限公司及其他个人白帽子向 C NVD 提交了 853 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
H3C	284	0
天融信	284	4
安天实验室	226	0
漏洞盒子	191	191
360 网神	161	161
华为技术有限公司	139	0
恒安嘉新	98	0
杭州安恒信息技术有限公司	44	0
绿盟科技	34	0
中国电信集团系统集成有 限责任公司	29	0
启明星辰	8	8
知道创宇	2	0
北京无声信息技术有限公司	1	0
东软	1	1
北京安信天行科技有限公 司	1	1
深圳市深信服电子科技有 限公司	1	1
西安四叶草信息技术有限 公司	1	1
深圳市鼎安天下信息科技 有限公司	28	18
四川虹微技术有限公司 (子午攻防实验室)	18	11
中新网络信息安全股份有 限公司	5	3

福建榕基软件股份有限公司	1	3
广州万方计算机科技有限公司	1	1
江苏同袍信息科技有限公司	1	1
CNCERT 重庆分中心	10	10
CNCERT 吉林分中心	9	9
CNCERT 新疆分中心	7	7
CNCERT 福建分中心	5	5
CNCERT 广东分中心	3	3
CNCERT 浙江分中心	2	2
CNCERT 海南分中心	1	1
个人	411	411
报送总计	2007	853

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 482 个漏洞。其中应用程序漏洞 279 个，操作系统漏洞 90 个，web 应用漏洞 82 个，网络设备漏洞 28 个，数据库漏洞 2 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	279
操作系统漏洞	90
web 应用漏洞	82
网络设备漏洞	28
数据库漏洞	2
安全产品漏洞	1

表 2 漏洞按影响类型统计表

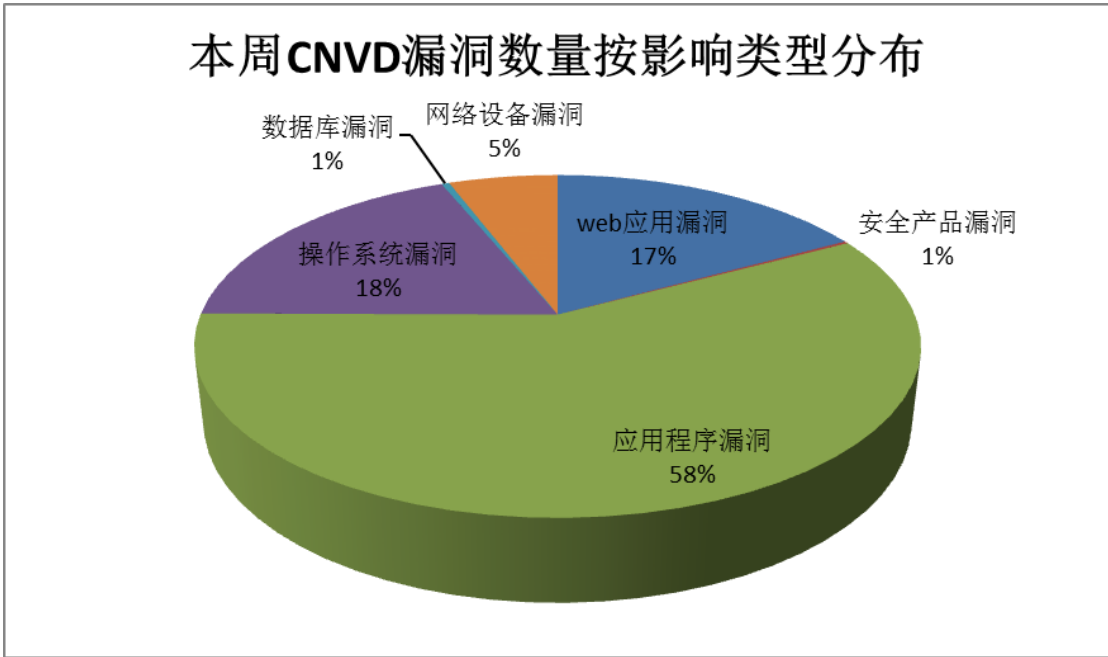


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、Google、WordPress 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	Oracle	94	20%
2	Google	92	19%
3	WordPress	53	11%
4	D-Link	17	4%
5	ImageMagick	10	2%
6	GraphicsMagick	8	2%
7	Juniper Networks	5	1%
8	SimpleSAMLphp	4	1%
9	TYPO3	4	1%
10	其他	195	39%

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 32 个电信行业漏洞，124 个移动互联网行业漏洞，5 个工控系统行业漏洞（如下图所示）。其中，“Korenix JetNet 中间人攻击漏洞、Korenix JetNet 未授权访问漏洞、Oracle WebLogic Server 存在未明漏洞（CNVD-2017-31499）、Spider

Control MicroBrowser 任意代码执行漏洞、Google Android Runtime 拒绝服务漏洞”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/>

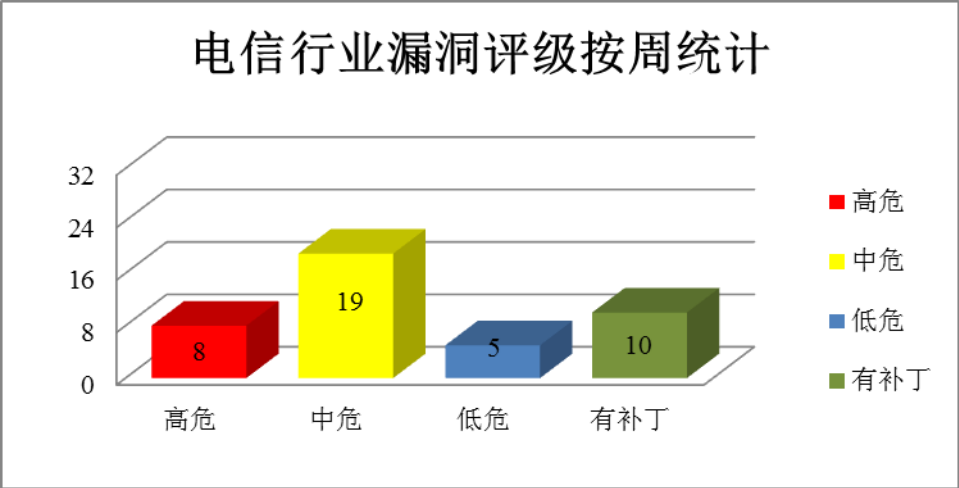


图 3 电信行业漏洞统计

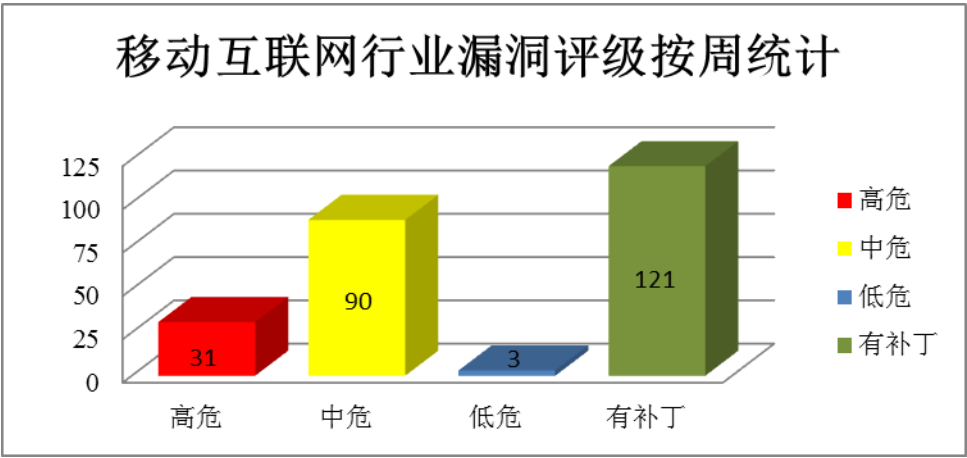


图 4 移动互联网行业漏洞统计

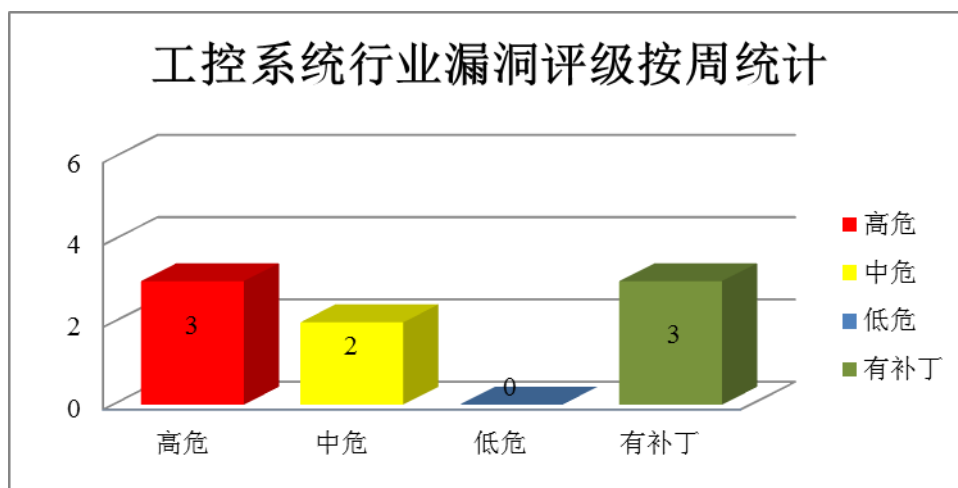


图 5 工控系统行业漏洞统计

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、Google 产品安全漏洞

Android 是美国谷歌公司开发的一套以 Linux 为基础的开源操作系统。Media framework(libhevc)是其中的一个用于多媒体开发的 hevc 解码库。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-2017-31360、CNVD-2017-31361、CNVD-2017-31362、CNVD-2017-31363、CNVD-2017-31364、CNVD-2017-31365、CNVD-2017-31366、CNVD-2017-31367）。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-2017-31360>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31361>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31362>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31363>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31364>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31365>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31366>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31367>

2、Oracle 产品安全漏洞

Oracle E-Business Suite 是美国甲骨文公司的一套全面集成式的全球业务管理软件。Oracle Knowledge Management 是其中的一个知识管理组件。Oracle Fusion Middleware 是一套面向企业和云环境的业务创新平台。Oracle WebLogic Server 是其中的一

个适用于云环境和传统环境的应用服务器组件。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保密性、完整性和可用性。

CNVD 收录的相关漏洞包括：Oracle Knowledge Management 组件存在未明漏洞、Oracle Knowledge Management 组件存在未明漏洞（CNVD-2017-31058、CNVD-2017-31059）、Oracle WebLogic Server 存在未明漏洞（CNVD-2017-31499、CNVD-2017-31500、CNVD-2017-31501、CNVD-2017-31502、CNVD-2017-31503）。除“Oracle WebLogic Server 存在未明漏洞（CNVD-2017-31500、CNVD-2017-31501、CNVD-2017-31502、CNVD-2017-31503）”外，其余漏洞的综合评级为“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-2017-31057>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31058>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31059>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31499>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31500>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31501>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31502>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31503>

3、D-Link 产品安全漏洞

D-Link DIR-850L REV.A 和 REV.B 都是友讯（D-Link）公司的无线路由器产品。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息、获取权限或执行任意代码。

CNVD 收录的相关漏洞包括：D-Link DIR-850L REV.A 和 REV.B DHCP 客户端远程代码执行漏洞、D-Link DIR-850L REV.A 跨站脚本漏洞、D-Link DIR-850L REV.A 跨站脚本漏洞（CNVD-2017-31794、CNVD-2017-31795、CNVD-2017-31796）、D-Link DIR-850L REV.B 密码泄露漏洞、D-Link DIR-850L REV.B 权限获取漏洞、D-Link DIR-850L REV.B 权限获取漏洞（CNVD-2017-31792）。其中，“D-Link DIR-850L REV.A 和 REV.B DHCP 客户端远程代码执行漏洞、D-Link DIR-850L REV.B 权限获取漏洞、D-Link DIR-850L REV.B 权限获取漏洞（CNVD-2017-31792）”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-2017-31797>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31793>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31794>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31795>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31796>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31791>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31788>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31792>

4、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，该产品被披露存在 SQL 注入漏洞，攻击者可利用漏洞执行任意 SQL 命令。

CNVD 收录的相关漏洞包括：WordPress eventr 'event'参数 SQL 注入漏洞、WordPress eventr SQL 注入漏洞、WordPress SQL 注入漏洞（CNVD-2017-31384）、WordPress Support Ticket System SQL 注入漏洞、WordPress surveys 'action'变量 SQL 注入漏洞、WordPress surveys SQL 注入漏洞、WordPress surveys 'survey_id'变量 SQL 注入漏洞、WordPress WatuPRO SQL 注入漏洞。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-2017-31217>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31216>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31384>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31428>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31185>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31186>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31184>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-31146>

5、Arris NVG599 AT&T U-verse ROOT 获取漏洞

Arris NVG599 是美国 Arris 集团公司的一款路由器产品。本周，Arris 被披露存在权限提升漏洞，远程攻击者可通过在 49955 端口上建立会话，并安装新软件利用该漏洞获取 root 权限。目前，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-2017-31553>

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-2017-31019	Red5 Media Server 代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： https://github.com/mbechler/marshalsec
CNVD-2017-31050	Pivotal Software Cloud Foundry 输入验证漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：

			https://www.cloudfoundry.org/cve-2016-8218/
CNVD-2017-31146	WordPress WatuPRO 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://github.com/wp-plugins/watu
CNVD-2017-31147	ImageMagick 拒绝服务漏洞（CNVD-2017-31147）	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.imagemagick.org
CNVD-2017-31284	SimpleSAMLphp PHP 会话固定漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://simplesamlphp.org/security/2017-05-01
CNVD-2017-31287	SimpleSAMLphp 不正确认证漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://simplesamlphp.org/security/2016-12-04
CNVD-2017-31336	YADIFA DNS 数据包解析器拒绝服务漏洞	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.yadifa.eu/
CNVD-2017-31575	Flets Install Tool 不可信搜索路径漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： http://flets-w.com/topics/inst_tool_vulnerability/
CNVD-2017-31585	Optimal Guard 安装程序不可信搜索路径漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://www.optim.co.jp/contents/23246
CNVD-2017-31675	libpgf 双重释放漏洞	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.libpgf.org

表 4 部分重要高危漏洞列表

小结：本周，Google 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。此外，Oracle、D-Link、Wordpress 等多款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等。另外，Arris 被披露存在权限提升漏洞，远程攻击者可通过在 49955 端口上建立会话，并安装新软件利用该漏洞获取 root 权限。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. 新型勒索软件 Bad Rabbit 在东欧诸国爆发

近日，据媒体报道，乌克兰的一些交通组织以及一些政府组织遭受了网络攻击，导致一些计算机文件被加密勒索。攻击者首先通过入侵新闻媒体类网站，随后利用这些新

闻类网站发起水坑攻击。当用户浏览这些网站时，用户浏览器就会弹出伪装的 Adobe flash player 升级的对话框，当用户点击了 install 按钮后，就会下载勒索软件。如果此时用户有高度的安全意识，不去运行下载的文件的话就可以免受勒索。但根据受害用户的数量来看，很多用户都运行了下载的假冒的升级程序。

参考链接：<http://www.freebuf.com/news/151827.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：010-82991537