

信息安全漏洞周报

2016 年 12 月 26 日-2017 年 01 月 01 日

2017 年第 1 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 171 个，其中高危漏洞 48 个、中危漏洞 117 个、低危漏洞 6 个。漏洞平均分为 5.91。本周收录的漏洞中，涉及 0day 漏洞 40 个（占 23%）。其中互联网上出现“NETGEAR WNR2000 路由器访问控制漏洞、Horos 远程内存破坏漏洞”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 547 个，与上周（729 个）环比下降 25%。

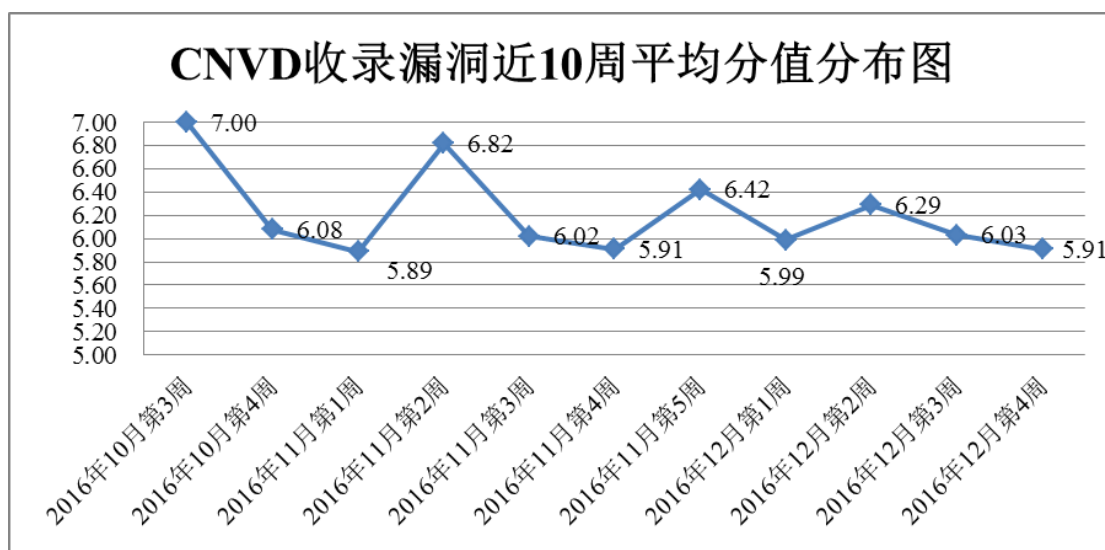


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 12 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 171 个漏洞。报送情况如表 1 所示。其中，启明星辰、安天实验室、蓝盾信息安全技术股份有限公司、华为技术有限公司等单位报送数量较多。360 网神、漏洞盒子、上海零盾网

络科技有限公司、新疆天山智汇信息科技有限公司、腾讯玄武实验室及其他个人白帽子向 CNVD 提交了 547 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	355	355
启明星辰	200	0
安天实验室	152	0
蓝盾信息安全技术股份有限公司	139	0
华为技术有限公司	80	0
天融信	69	0
绿盟科技	66	19
H3C	46	0
恒安嘉新	41	0
中国电信集团系统集成有限责任公司	36	0
北京数字观星科技有限公司	5	0
南京铤迅信息技术股份有限公司	2	2
漏洞盒子	17	17
上海零盾网络科技有限公司	1	1
新疆天山智汇信息科技有限公司	1	1
腾讯玄武实验室	1	1
CNCERT 山西分中心	4	4
CNCERT 陕西分中心	4	4
CNCERT 湖南分中心	3	3
CNCERT 江西分中心	2	2
CNCERT 宁夏分中心	1	1

CNCERT 福建分中心	1	1
个人	136	136
报送总计	1362	547
录入总计	171（去重）	547

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 171 个漏洞。其中应用程序漏洞 120 个， web 应用漏洞 25 个，网络设备漏洞 19 个，安全产品漏洞 4 个，操作系统漏洞 3 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	120
web 应用漏洞	25
网络设备漏洞	19
安全产品漏洞	4
操作系统漏洞	3

表 2 漏洞按影响类型统计表

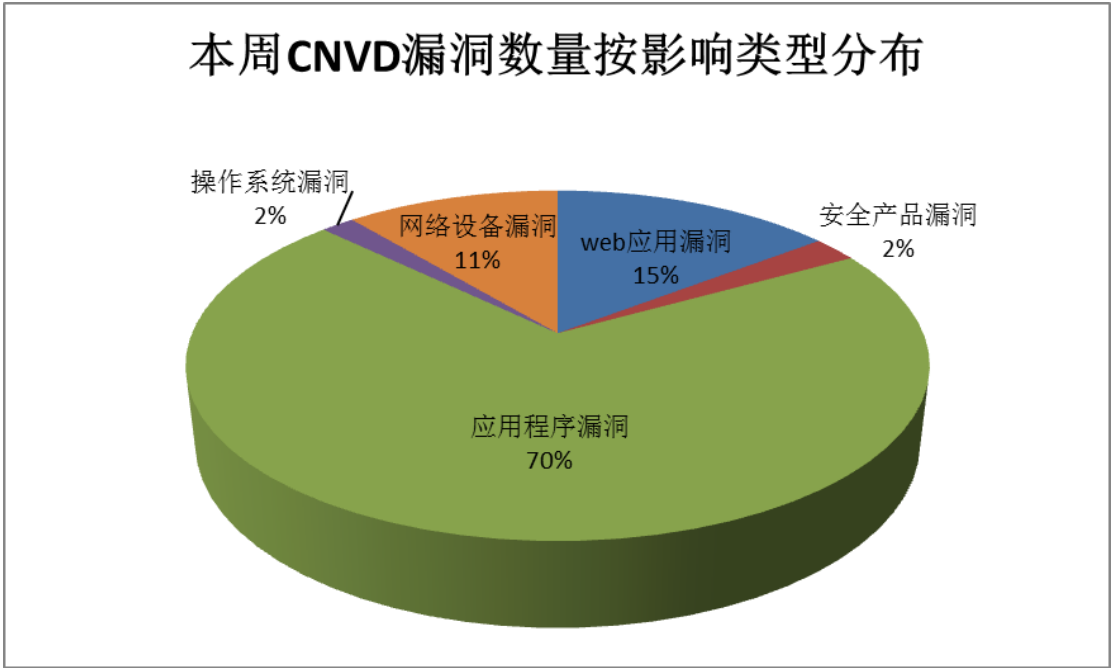


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 IBM、w3m、SAP 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	IBM	17	10%
2	w3m	10	6%
3	SAP	8	5%
4	HP	6	4%
5	phpMyAdmin	6	4%
6	Apache	5	3%
7	Samsung	5	3%
8	ZyXEL	4	2%
9	Huawei	3	1%
10	其他	107	62%

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 11 个电信行业漏洞，2 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，“BlackBerry Good Enterprise Mobility Server 任意命令执行漏洞”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/>

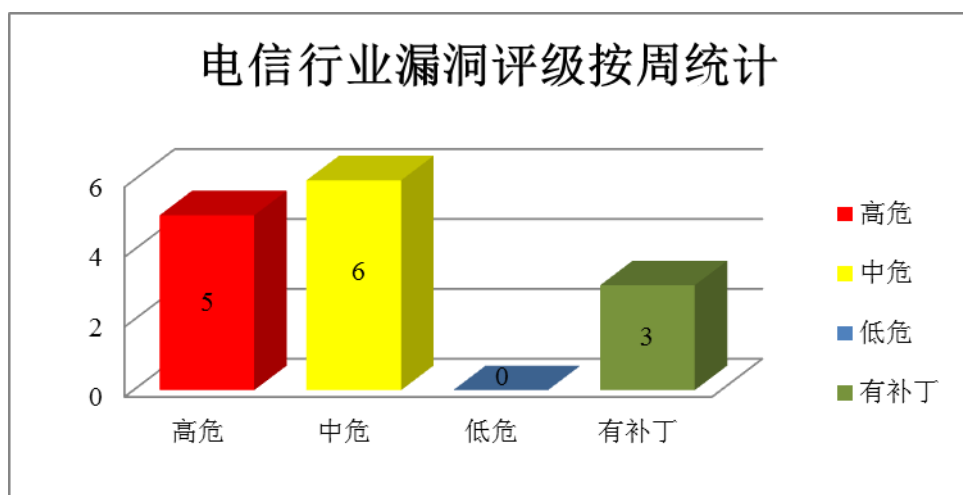


图 3 电信行业漏洞统计

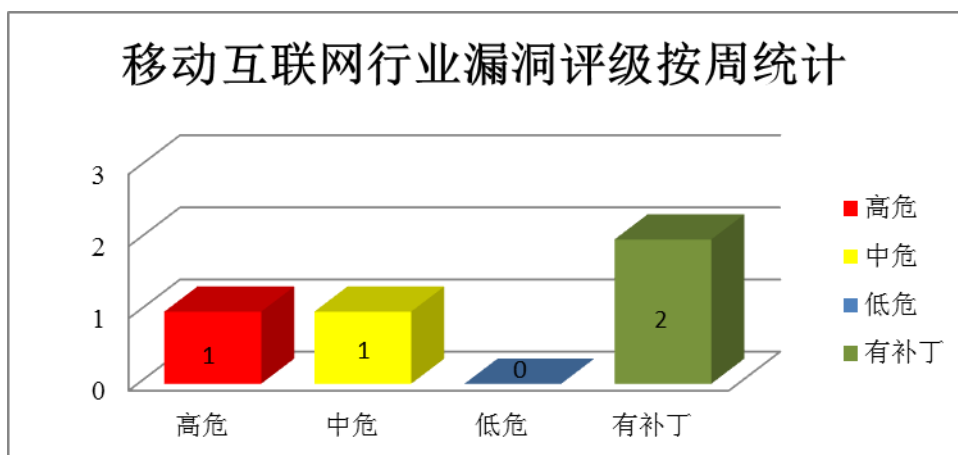


图 4 移动互联网行业漏洞统计

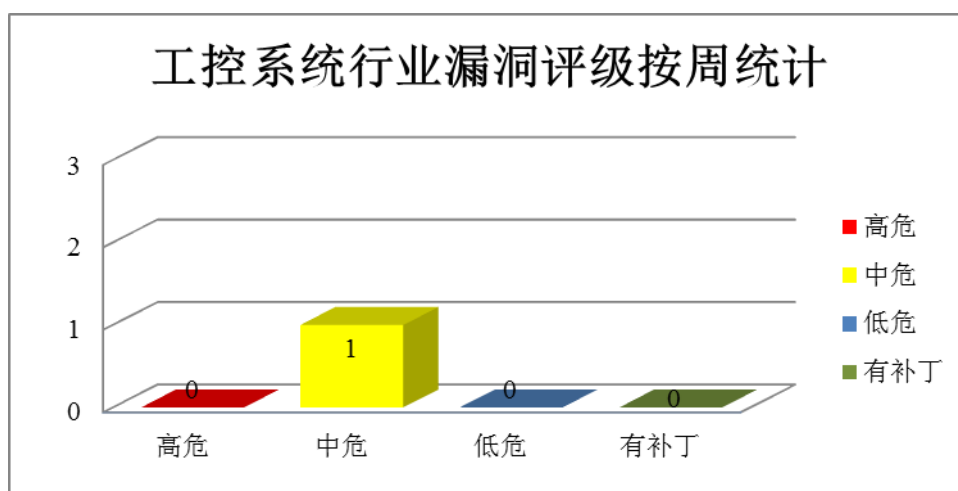


图 5 工控系统行业漏洞统计

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、PHPMailer 产品安全漏洞

PHPMailer 是一个用于发送电子邮件的 PHP 函数包。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：PHPMailer 远程代码执行漏洞。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-2016-13107>

2、IBM 产品安全漏洞

IBM Rational CLM、Rational Team Concert (RTC) 和 Rational Engineering Lifecycle Manager (RELM) 都是美国 IBM 公司的协作化生命周期管理解决方案；Rational DOORS Next Generation (RDNG) 是需求管理解决方案。IBM Tivoli Storage Manage

r Operations Center 是一套下一代简化备份管理的解决方案。IBM AIX 是一套 UNIX 操作系统。IBM Security Access Manager (ISAM) 是一款安全访问管理器；IBM Security Access Manager for Web 是一套通过一个模块式软件包提供移动访问安全防护的解决方案。本周，上述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、绕过安全限制、提升权限或进行跨站脚本攻击等。

CNVD 收录的相关漏洞包括：多款 IBM Rational 产品跨站脚本漏洞（CNVD-2016-13286、CNVD-2016-13288）、多款 IBM Rational 产品信息泄露漏洞、IBM Tivoli Storage Manager Operations Center 跨站脚本漏洞、IBM Tivoli Storage Manager Operations Center 安全绕过漏洞、IBM Tivoli Storage Manager Operations Center 跨站请求伪造漏洞、IBM AIX 本地权限提升漏洞（CNVD-2016-13013）、多款 IBM Security Access Manager 产品 SQL 注入漏洞等。其中，“IBM Tivoli Storage Manager Operations Center 跨站请求伪造漏洞、IBM AIX 本地权限提升漏洞（CNVD-2016-13013）、多款 IBM Security Access Manager 产品 SQL 注入漏洞”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-2016-13286>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-13288>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-13290>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-13226>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-13224>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-13275>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-13013>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-13272>

3、SAP 产品安全漏洞

SAP Download Manager 是德国思爱普（SAP）公司的开发的一套用于下载软件包和支持注释的 Java 应用程序。SAP HANA 是一套高性能的实时数据分析平台。SAP NetWeaver 是一套面向服务的集成化应用平台。SAP BusinessObjects 产品组合提供多种商务智能软件、信息管理软件、企业绩效管理解决方案、监管、风险与合规性解决方案。本周，上述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、绕过安全限制或执行任意命令等。

CNVD 收录的相关漏洞包括：SAP Download Manager 信息泄露漏洞（CNVD-2016-13117）、SAP HANA 信息泄露漏洞（CNVD-2016-12983、NVD-2016-13026）、SAP HANA 远程安全绕过漏洞、SAP HANA Cockpit 跨站脚本漏洞、SAP NetWeaver 安全绕过漏洞（CNVD-2016-13027）、SAP BusinessObjects 信息泄露漏洞、SAP BusinessObjects BI Platform 远程命令执行漏洞等。其中，“SAP BusinessObjects BI Platform 远程命

令执行漏洞”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-2016-13117>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12983>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12987>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12989>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-13026>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-13027>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-13028>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-13030>

4、HPE 产品安全漏洞

HPE Systems Insight Manager (SIM) 是美国惠普企业公司的一套面向惠普服务器、存储设备的管理软件。HPE Version Control Repository Manager (VCRM) 是一个用于存储支持 ProLiant 服务器的软件和固件的库。本周，上述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、上传任意文件或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：HPE Systems Insight Manager 拒绝服务漏洞 (CNVD-2016-13228、CNVD-2016-13230)、HPE Systems Insight Manager 跨站脚本漏洞、HP EHPE Version Control Repository Manager 文件上传漏洞、HPE Version Control Repository Manager 信息泄露漏洞、HPE Version Control Repository Manager 跨站请求伪造漏洞。其中，“HPE Systems Insight Manager 拒绝服务漏洞 (CNVD-2016-13230)、HP E Systems Insight Manager 跨站脚本漏洞”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-2016-13228>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-13229>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-13230>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-13009>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-13008>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-13007>

5、ZyXEL P660HN-T v2 路由器未经身份验证的远程命令执行漏洞

ZyXEL P660HN-T v2 是一款合勤科技生产的路由器。本周，ZyXEL 被披露存在远程命令执行漏洞。攻击者可利用漏洞远程执行任意代码。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-2016-13300>

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-2016-13000	OsiriX DICOM Viewer 远程内存破坏漏洞	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://www.osirix-viewer.com/
CNVD-2016-13001	Orthanc DICOM Server 远程内存破坏漏洞	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://www.orthanc-server.com/download.php
CNVD-2016-13012	Samsung Note Telecom 拒绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： http://security.samsungmobile.com/smrupdate.html#SMR-DEC-2016
CNVD-2016-13018	Apport 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，详情请关注厂商主页： https://wiki.ubuntu.com/Apport
CNVD-2016-13017	Apport 路径遍历漏洞	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://wiki.ubuntu.com/Apport
CNVD-2016-13031	CodeBlocks DLL 劫持漏洞	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://www.codeblocks.org/
CNVD-2016-13110	OmniView 信息泄露漏洞	高	用户可联系供应商获得补丁信息： https://ics-cert.us-cert.gov/advisories/ICSA-16-350-02
CNVD-2016-13111	OmniView 信息泄露漏洞（CNVD-2016-13111）	高	用户可联系供应商获得补丁信息： https://ics-cert.us-cert.gov/advisories/ICSA-16-350-02
CNVD-2016-13278	Cloud Foundry 权限提升漏洞	高	用户可联系供应商获得补丁信息： https://www.cloudfoundry.org/
CNVD-2016-13271	Symantec Norton Download Manager 远程代码执行漏洞	高	用户可联系供应商获得补丁信息： https://www.symantec.com/

表 4 部分重要高危漏洞列表

小结：本周，PHPMailer 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，IBM、SAP、HPE 等多款产品被披露存在多个安全漏洞，攻击者利用漏洞可泄露敏感信息、绕过安全限制或发起拒绝服务攻击等。另外，ZyXEL 被披露存在远程命令执行漏洞。攻击者可利用漏洞远程执行任意代码。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. 思科 CloudCenter Orchestrator 系统曝提权漏洞

思科提醒用户 Cisco CloudCenter Orchestrator 系统存在提权漏洞——CVE-2016-9223，可能已经被用于网络攻击。Cisco CloudCenter Orchestrator（简称 CCO，之前叫 CiQr）的 Docker Engine 存在漏洞，未经认证的攻击者也能通过高权限远程安装 Docker 容器。此漏洞是由于一个错误的配置引起的，导致的结果就是管理 Docker Engine 的端口可以不通过 CloudCenter Orchestrator 系统就对 Docker Engine 访问。攻击者可以通过加载 Docker 容器来利用此漏洞。造成的次要影响是这个漏洞可能会让攻击者得到 CloudCenter Orchestrator 的 root 权限。

参考链接：<http://www.freebuf.com/vuls/123888.html>

2. PHP7 曝出三个高危 0-day 漏洞，还有一个仍未修复

PHP7 出现三个高危 0-day 漏洞，可允许攻击者完全控制 PHP 网站。三个漏洞编号分别为 CVE-2016-7479、CVE-2016-7480 和 CVE-2016-7478，其利用方式与 Check Point 八月份详细报道的 CVE-2015-6832 漏洞类似。前两个漏洞如遭利用，将允许攻击者完全控制目标服务器，攻击者可以传播恶意程序、盗取或篡改客户数据等。如果第三个漏洞被利用，则可造成 DoS 攻击，可使目标网站资源系统耗尽并最终关闭。PHP 安全团队已在 10 月 13 日和 12 月 1 日发布了针对其中两个漏洞的补丁，但还有一个仍未修复。为保证 Web 服务器安全，用户应将服务器 PHP 版本升至最新。

参考链接：<http://www.freebuf.com/news/124159.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