国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2016 年 05 月 30 日-2016 年 06 月 05 日　　2016 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 114 个，其中高危漏洞 12 个、中危漏洞 90 个、低危漏洞 12 个。漏洞平均分值为 5.23 分。本周收录的漏洞中，涉及 0day 漏洞 7 个（占 6%）。其中互联网上出现“PowerFolder 远程代码执行漏洞”等零日代码攻击漏洞，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 1263 个，与上周（1210 个）环比增长 4%。

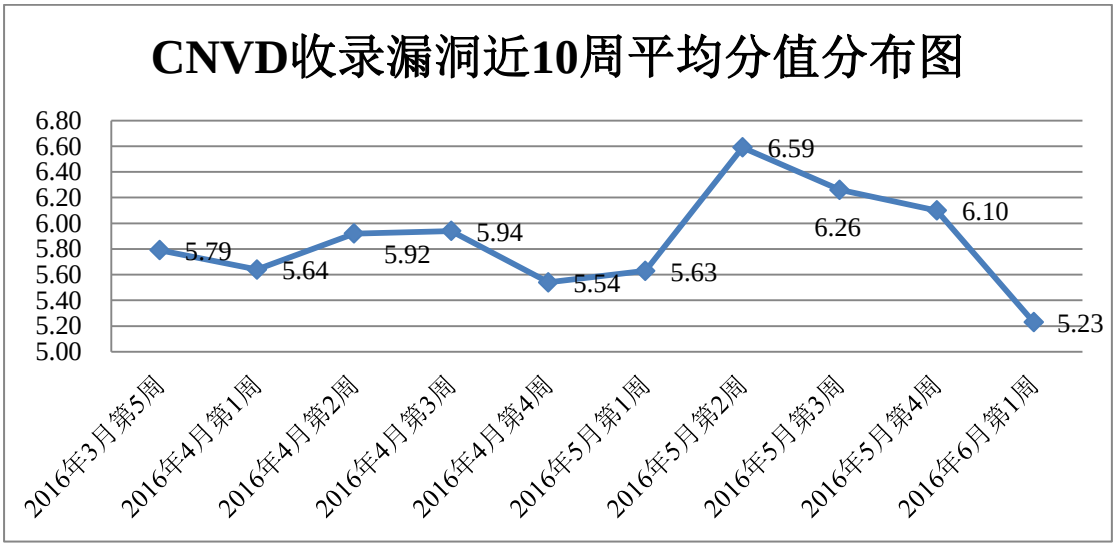

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 9 家成员单位、合作伙伴及个人报送了本周收录的全部 114 个漏洞。报送情况如表 1 所示。其中，安天实验室、恒安嘉新、启明星辰、绿盟科技等单位报送数量较多。补天平台、乌云、漏洞盒子、西安四叶草信息技术有限公司、深圳市深信服电子

科技有限公司、福建六壬网安股份有限公司、汉柏科技有限公司、山东安云信息技术有限公司、北京国舜科技股份有限公司、赛尔网络有限公司及白帽子向 CNVD 提交了 1263 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)	613	613
安天实验室	124	124
恒安嘉新	82	17
启明星辰	96	0
绿盟科技	93	0
杭州安恒信息技术有限公司	78	0
天融信	58	0
中国电信集团系统集成有限责任公司	45	1
H3C	12	0
乌云	406	406
漏洞盒子	54	54
西安四叶草信息技术有限公司	11	11
深圳市深信服电子科技有限公司	6	6
福建六壬网安股份有限公司	2	2
汉柏科技有限公司	2	2
山东安云信息技术有限公司	1	1
北京国舜科技股份有限公司	1	1
赛尔网络有限公司	1	1
CNCERT 江西分中心	6	6
CNCERT 上海分中心	3	3

CNCERT 宁夏分中心	1	1
个人	14	14
报送总计	1709	1263
录入总计	114（去重）	1263

表 1 成员单位上报漏洞统计表

本周漏洞按类型和厂商统计

本周，CNVD 收录了 114 个漏洞。其中应用程序漏洞 89 个，Web 应用漏洞 20 个，网络设备漏洞 2 个，安全产品漏洞 2 个，操作系统漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	89
web 应用漏洞	20
网络设备漏洞	2
安全产品漏洞	2
操作系统漏洞	1

表 2 漏洞按影响类型统计表

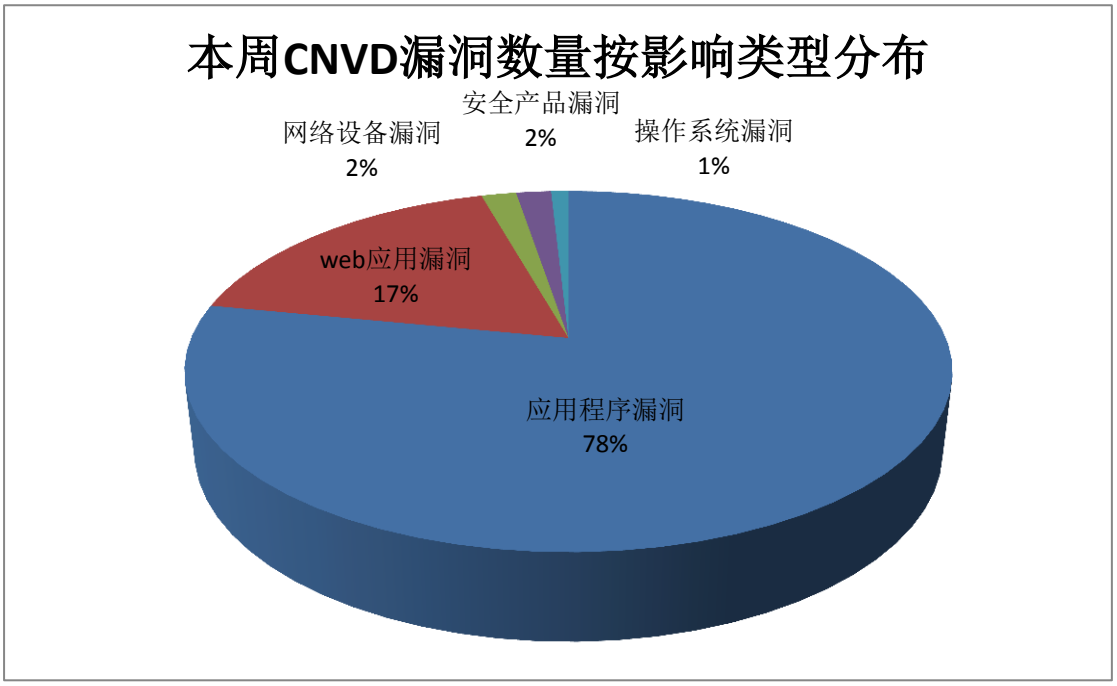

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 HP、Cybozu、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	HP	13	11%
2	Cybozu	12	11%
3	IBM	10	9%
4	Google	7	6%
5	Pulse Secure, LLC	7	6%
6	PHP	5	4%
7	ABB	4	4%
8	Cisco	3	3%
9	Teampass	3	3%
10	其他	50	43%

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 个电信行业漏洞，2 个移动互联网行业漏洞，6 个工控系统行业漏洞（如下图所示）。其中，“ESC 8832 未授权访问漏洞、ESC 8832 未授权操作漏洞”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/

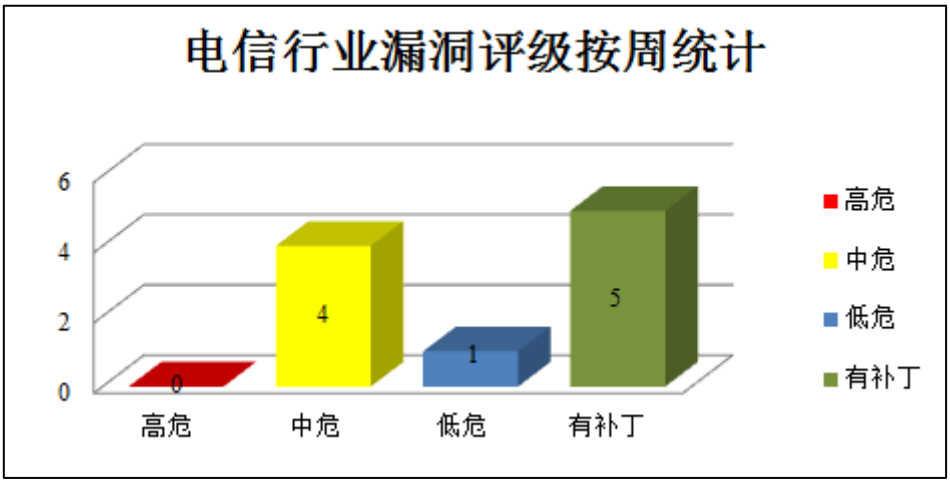

图 3 电信行业漏洞统计

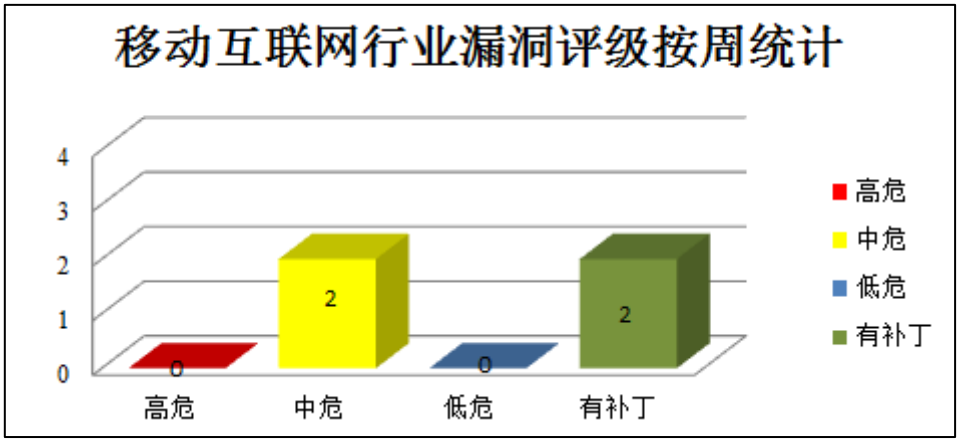

图 4 移动互联网行业漏洞统计

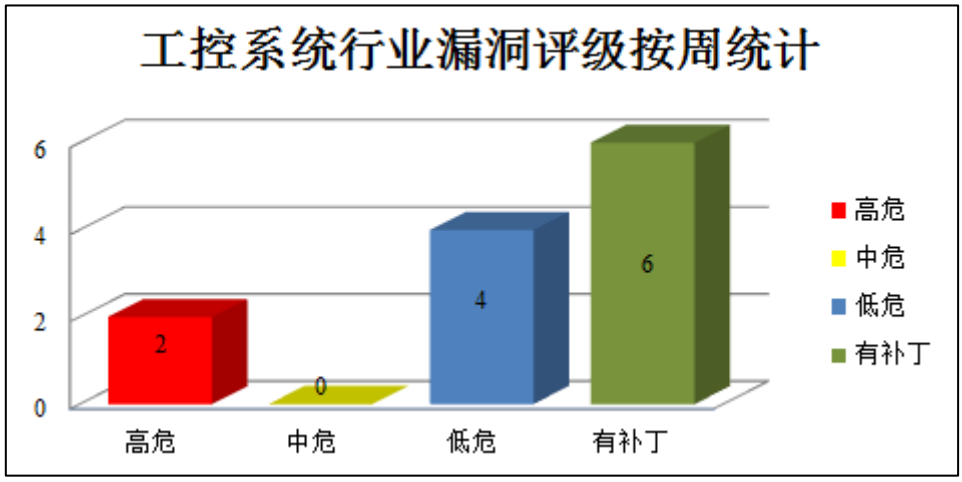

图 5 工控系统行业漏洞统计

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、 Apache 产品安全漏洞

Apache Struts 是一款用于创建企业级 Java Web 应用的开源框架。Apache PDFBox 是美国阿帕奇（Apache）软件基金会的一个开源的、基于 Java 并提供创建新的 PDF 文档、修改现有的 PDF 文档等功能的工具库。Apache Qpid Java Broker 是美国阿帕奇（Apache）软件基金会开发的一款使用 Java 语言编写的用于路由和转发邮件的消息中间件。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞执行任意代码或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Apache Struts2 远程代码执行漏洞（CNVD-2016-03754）、Apache PDFBox XML 外部实体漏洞、Apache Qpid Java Broker 拒绝服务漏洞、Apache Qpid Java Broker 身份验证绕过漏洞。其中，“Apache Struts2 远程代码执行漏洞（CNVD-2016-03754）”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-2016-03754

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03706

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03707

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03710

2、IBM 产品安全漏洞

IBM TRIRIGA Application Platform 是美国 IBM 公司的一套用于部署 TRIRIGA 应用的技术平台。IBM WebSphereeXtreme Scale 是美国 IBM 公司的一套分布式高速缓存解决方案。IBM UrbanCode Deploy（UCD）是美国 IBM 公司的一套应用自动化部署工具。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敏感信息和进行跨站脚本和跨站请求伪造攻击等。

CNVD 收录的相关漏洞包括：IBM TRIRIGA Application Platform 跨站脚本漏洞（CNVD-2016-03776）、IBM TRIRIGA Application Platform 跨站请求伪造漏洞（CNVD-2016-03775）、IBM TRIRIGA Application Platform HTTP 请求转发漏洞、IBM WebSphereeXtreme Scale HTTP 响应拆分漏洞、IBM WebSphereeXtreme Scale 信息泄露漏洞（CNVD-2016-03730）、IBM WebSphereDataPower XC10 缓冲区溢出漏洞、IBM UrbanCode Deploy 工件下载漏洞、IBM UrbanCode Deploy 信息泄露漏洞（CNVD-2016-03733）。其中，“IBM TRIRIGA Application Platform 跨站请求伪造漏洞（CNVD-2016-03775）”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-2016-03776

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03775

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03785

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03727

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03730

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03731

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03732

http://www.cnvd.org.cn/flaw/show/CNVD-2016-03733

3、Cybozu 产品安全漏洞

CybozuGaroon 是日本才望子（Cybozu）公司的一套门户型 OA 办公系统。本周，该产品被披露存在多安全绕过、信息泄露、目录遍历、拒绝服务和跨站脚本漏洞，攻击者可利用漏洞获取敏感信息、执行未授权操作、进行跨站脚本和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：CybozuGaroon 安全绕过漏洞、CybozuGaroon 安全绕过漏洞（CNVD-2016-03725）、CybozuGaroon 目录遍历漏洞（CNVD-2016-03722、CNVD-2016-03721）、CybozuGaroon 跨站脚本漏洞、CybozuGaroon 跨站脚本漏洞（CNVD-2

016-03716）、CybozuGaroon 拒绝服务漏洞、CybozuGaroon 信息泄露漏洞。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-2016-03723
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03725
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03722
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03721
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03715
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03716
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03719
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03717

4、Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司开发的一款 Web 浏览器。Blink 是美国谷歌（Google）公司和挪威欧朋（Opera Software）公司共同开发的一套浏览器排版引擎（渲染引擎）。Google V8 是其中的一套开源 JavaScript 引擎。本周，上述产品被披露存在同源策略绕过和缓冲区溢出漏洞，攻击者可利用漏洞绕过同源策略，影响保密性、完整性和可用性。

CNVD 收录的相关漏洞包括：Google Chrome 同源策略绕过漏洞（CNVD-2016-03778、CNVD-2016-03781、CNVD-2016-03783）、Google Chrome Blink 同源策略绕过漏洞（CNVD-2016-03780、CNVD-2016-03782）、Google Chrome V8 缓冲区溢出漏洞、Google Chrome V8 堆缓冲区溢出漏洞。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-2016-03778
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03781
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03783
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03780
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03782
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03784
http://www.cnvd.org.cn/flaw/show/CNVD-2016-03786

5、PowerFolder 远程代码执行漏洞

PowerFolder 是文件同步和协作中主要的内部解决方案。本周，PowerFolder 被披露存在远程代码执行漏洞。该漏洞源于允许反序列化不可信的数据，攻击者可利用漏洞执行任意代码。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-2016-03700

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-2016-03676	MEDHOST Perioperative Information Management System 未授权操作漏洞	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：http://www.medhost.com/
CNVD-2016-03675	ESC 8832 未授权操作漏洞	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：http://www.envirosys.com/
CNVD-2016-03674	ESC 8832 未授权访问漏洞	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：http://www.envirosys.com/
CNVD-2016-03673	多款 Black Box AlertWerksServSensor 产品信息泄露漏洞	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://www.blackbox.com/
CNVD-2016-03671	TYPO3 CMS 访问检查漏洞	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://typo3.org/teams/security/security-bulletins/typo3-core/typo3-core-sa-2016-013/
CNVD-2016-03689	pgpdump 资源管理错误漏洞	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：http://www.pgpdump.net/
CNVD-2016-03688	Pulse Connect Secure 拒绝服务漏洞	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://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA40206
CNVD-2016-03704	SAP NetWeaver AS JAVA 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：http://go.sap.com/
CNVD-2016-03697	Linknat SQL 注入漏洞	高	用户可联系供应商获得补丁信息：http://www.linknat.com/
CNVD-2016-03754	Apache Struts2 远程代码执行漏洞(CNVD-2016-03754)	高	关闭动态调用方法或升级至新版本修复该漏洞，软件更新地址：https://cwiki.apache.org/confluence/display/WW/Migration+Guide

表 4 部分重要高危漏洞列表

小结：本周 Apache 产品被披露存在多个安全漏洞，攻击者可利用漏洞执行任意代码或发起拒绝服务攻击等。此外，IBM、Cybozu、Google 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、执行未授权操作、执行任意代码或发起拒绝服务攻击等。在本周高危漏洞列表中，值得注意的是 ESC8832 工业控制数据采集系统被披露存在权限绕过漏洞，该系统有可能通过前端 Web 服务暴露在互联网上，构成安全威胁。

本周漏洞要闻速递

1.“SandJacking”攻击：在未越狱的 iOS 设备上安装恶意应用

在 HITB 2016 会议中，Mi3 Security 公司的安全研究员 ChilikTamir 发表了一个关于“SandJacking”攻击的演讲，利用一个未打补丁的 iOS 漏洞在未越狱的 iOS 设备上使用恶意版本替换合法的应用程序，获取设备的敏感信息。值得注意的是，该恶意应用只能为攻击者提供应用沙箱的访问权限。这意味着攻击者需要为每个目标应用程序创建恶意版本。但是 Tamir 认为如果考虑自动化的话这将不会成为阻碍攻击者的难题。该 SandJacking 漏洞在 2015 年 12 月被研究人员发现，并在 1 月报告给苹果，苹果已经确认了该漏洞，但是还没有发布补丁。该漏洞修复后，Tamir 会发布利用该漏洞利用工具。

参考链接：http://www.freebuf.com/vuls/105727.html

2.Forbidden attack：7 万台 web 服务器陷入被攻击的险境

最近，根据某国际安全小组的研究表明，金融巨头 Visa 旗下部分受 HTTPS 保护的网站最近被发现了一种漏洞。该漏洞源于不正确的传输层安全协议，在数据被加密时，错误重用了相同的加密随机数。它的存在可以让黑客注入恶意代码，访客浏览器将会访问到恶意内容。

参考链接：http://www.freebuf.com/vuls/105644.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