国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2017 年 09 月 04 日-2017 年 09 月 10 日 **2017 年第 37 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 335 个，其中高危漏洞 94 个、中危漏洞 213 个、低危漏洞 28 个。漏洞平均分值为 5.73。本周收录的漏洞中，涉及 0day 漏洞 124 个（占 37%），其中互联网上出现“HelpDEZk SQL 注入漏洞、WordPress FormCraft Basic 插件 SQL 注入漏洞”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 1326 个，与上周（1641 个）环比减少 19%。

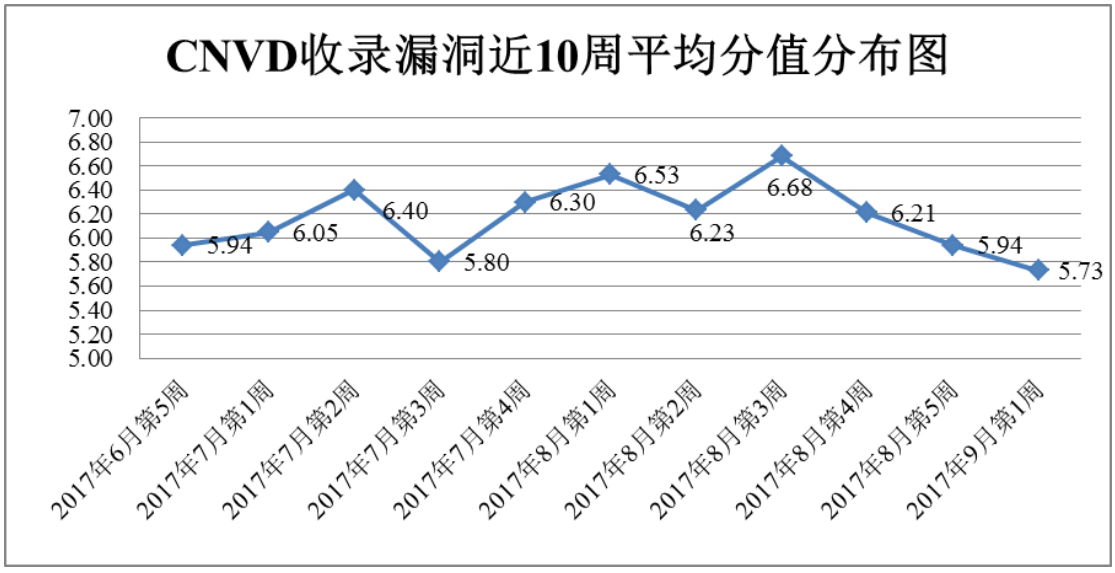

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 17 家成员单位、企业用户及个人用户报送了本周收录的全部 335 个漏洞。报送情况如表 1 所示。其中，H3C、安天实验室、恒安嘉新、中国电信集团系统集成有限责任公司、华为技术有限公司等单位报送数量较多。四川虹微技术有限公司（子午攻

防实验室）、深圳市鼎安天下信息科技有限公司、江苏同袍信息科技有限公司、上海犇众信息技术有限公司、山石网科通信技术有限公司、江苏省信息安全测评中心、北京安码科技有限公司、广州万方计算机科技有限公司、中新网络信息安全股份有限公司、北京市电子产品质量检测中心、广州软云计算机科技有限公司及其他个人白帽子向 CNVD 提交了 1326 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	264	0
安天实验室	225	0
360 网神	198	198
恒安嘉新	155	0
漏洞盒子	130	130
中国电信集团系统集成有限责任公司	118	36
华为技术有限公司	111	0
天融信	83	0
杭州安恒信息技术有限公司	53	0
绿盟科技	23	0
北京数字观星科技有限公司	22	0
厦门服云信息科技有限公司	16	0
启明星辰	7	7
东软	7	7
北京知道创宇信息技术有限公司	7	7
广西鑫瀚科技有限公司	2	2
深圳市腾讯计算机系统有限公司（玄武实验室）	1	1
四川虹微技术有限公司（子午攻防实验室）	243	243
深圳市鼎安天下信息科技	14	14

有限公司		
江苏同袍信息科技有限公司	6	6
上海犇众信息技术有限公司	5	5
山石网科通信技术有限公司	4	4
江苏省信息安全测评中心	3	3
北京安码科技有限公司	2	2
广州万方计算机科技有限公司	2	2
中新网络信息安全股份有限公司	2	2
北京市电子产品质量检测中心	1	1
广州软云计算机科技有限公司	1	1
CNCERT 广东分中心	2	2
个人	653	653
报送总计	2360	1326
录入总计	335（去重）	1326

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 335 个漏洞。其中应用程序漏洞 222 个，web 应用漏洞 85 个，网络设备漏洞 14 个，操作系统漏洞 11 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	222
web 应用漏洞	85
网络设备漏洞	14
操作系统漏洞	11
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

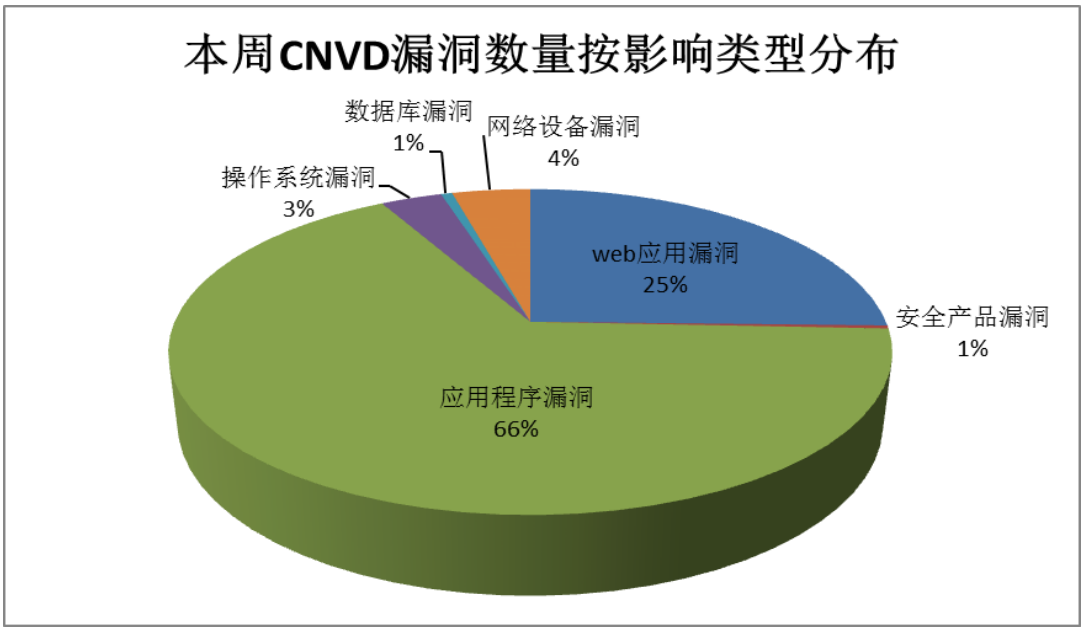

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 IBM、ImageMagick、JasPer 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	27	8%
2	ImageMagick	15	4%
3	JasPer	10	3%
4	Google	9	3%
5	Adobe	8	2%
6	Smiths Medical	8	2%
7	WordPress	7	2%
8	libfpx	7	2%
9	Wireshark	5	1%
10	其他	239	73%

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 15 个电信行业漏洞，43 个移动互联网行业漏洞，10 个工控系统行业漏洞（如下图所示）。其中，“ZyXEL PK5001Z 设备 ROOT 访问漏洞、多款 Huawei 产品 OSPF 协议 MaxAge LSA 拒绝服务漏洞、i-SENS SmartLog Diabetes Management Software 代码执行漏洞、Google Android Qualcomm 组件缓冲区溢出漏洞（CNV

D-2017-25678、CNVD-2017-25679）”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/

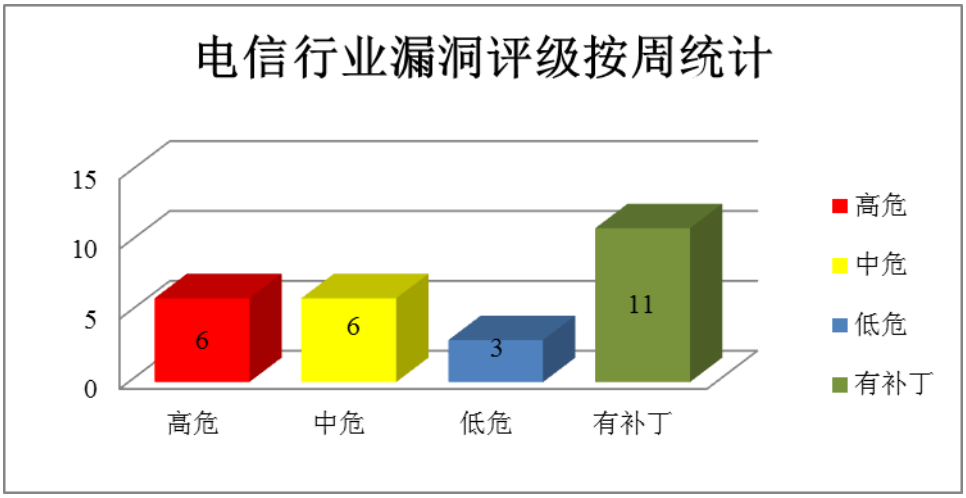

图 3 电信行业漏洞统计

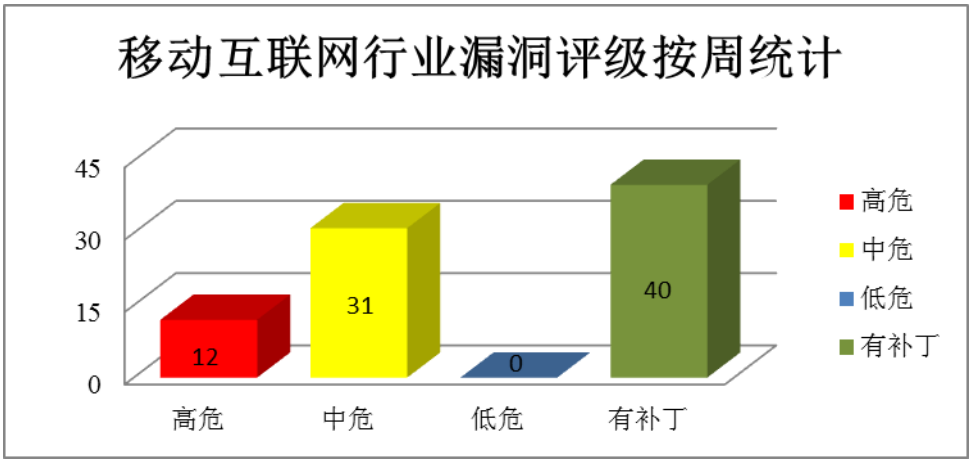

图 4 移动互联网行业漏洞统计

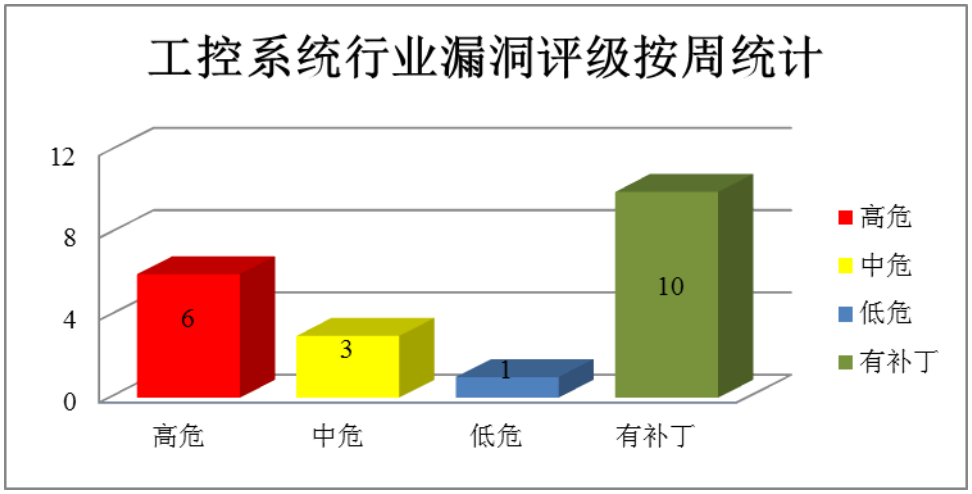

图 5 工控系统行业漏洞统计

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、Apache 产品安全漏洞

Struts2 是 Apache 软件基金会负责维护的一个基于 MVC 设计模式的 Web 应用框架开源项目。本周，该产品被披露存在 S2-052、S2-053 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：Apache Struts2 REST 插件远程代码执行漏洞、Apache Struts2 S2-053 远程代码执行漏洞。其中“Apache Struts2 REST 插件远程代码执行漏洞”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-2017-25267
http://www.cnvd.org.cn/flaw/show/CNVD-2017-25632

2、Google 产品安全漏洞

Android 是美国谷歌公司和开放手持设备联盟共同开发的一套以 Linux 为基础的开源操作系统。Qualcomm closed-source components 是其中的一个美国高通公司开发的闭源组件。本周，上述产品被披露存在缓冲区溢出漏洞，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：Google Android Qualcomm 组件缓冲区溢出漏洞（CNVD-2017-25677、CNVD-2017-25678、CNVD-2017-25679、CNVD-2017-25680、CNVD-2017-25681、CNVD-2017-25682、CNVD-2017-25683、CNVD-2017-25684）。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-2017-25677
http://www.cnvd.org.cn/flaw/show/CNVD-2017-25678
http://www.cnvd.org.cn/flaw/show/CNVD-2017-25679
http://www.cnvd.org.cn/flaw/show/CNVD-2017-25680
http://www.cnvd.org.cn/flaw/show/CNVD-2017-25681
http://www.cnvd.org.cn/flaw/show/CNVD-2017-25682
http://www.cnvd.org.cn/flaw/show/CNVD-2017-25683
http://www.cnvd.org.cn/flaw/show/CNVD-2017-25684

3、Adobe 产品安全漏洞

Adobe Reader/Acrobat 是一款流行的处理 PDF 文件的应用程序。本周，该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代码。

CNVD 收录的相关漏洞包括：Adobe Acrobat/Reader 内存破坏漏洞（CNVD-2017-25776、CNVD-2017-25777、CNVD-2017-25778、CNVD-2017-25779、CNVD-2017-25780、CNVD-2017-25781、CNVD-2017-25782、CNVD-2017-25783）。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-2017-25776
http://www.cnvd.org.cn/flaw/show/CNVD-2017-25777
http://www.cnvd.org.cn/flaw/show/CNVD-2017-25778
http://www.cnvd.org.cn/flaw/show/CNVD-2017-25779
http://www.cnvd.org.cn/flaw/show/CNVD-2017-25780
http://www.cnvd.org.cn/flaw/show/CNVD-2017-25781
http://www.cnvd.org.cn/flaw/show/CNVD-2017-25782
http://www.cnvd.org.cn/flaw/show/CNVD-2017-25783

4、Smiths Medical 产品安全漏洞

Medfusion 4000 Wireless Syringe Infusion Pump 是用于在急性护理环境中提供小剂量药物的注射器输液泵。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制、读取内存数据或执行任意代码等。

CNVD 收录的相关漏洞包括：Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump 缓冲区溢出漏洞、Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump 密码泄露漏洞、Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump 内存读取漏洞、Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump 身份验证绕过漏洞、Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump 硬编码漏洞、Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump 硬编码漏洞（CNVD-2017-25719）、Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump 硬编码密码漏洞、Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump 中间人攻击漏洞。除“Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump 密码泄露漏洞、Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump 内存读取漏洞、Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump 硬编码密码漏洞”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-2017-25723
http://www.cnvd.org.cn/flaw/show/CNVD-2017-25716
http://www.cnvd.org.cn/flaw/show/CNVD-2017-25722
http://www.cnvd.org.cn/flaw/show/CNVD-2017-25720
http://www.cnvd.org.cn/flaw/show/CNVD-2017-25721

http://www.cnvd.org.cn/flaw/show/CNVD-2017-25719

http://www.cnvd.org.cn/flaw/show/CNVD-2017-25718

http://www.cnvd.org.cn/flaw/show/CNVD-2017-25717

5、National Instruments LabVIEW 内存破坏漏洞

National Instruments LabVIEW 是美国国家仪器公司的一套系统设计平台。本周，National Instruments 被披露存在内存破坏漏洞，攻击者可利用漏洞造成拒绝服务。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-2017-25456

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-2017-24528	PHP msgfmt_parse_message 堆栈缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://bugs.php.net/bug.php?id=73473
CNVD-2017-24530	Lhaz Self-extracting archive 文件不可信搜索路径漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://chitora.com/jvn21369452.html
CNVD-2017-24536	LogicalDoc Community Edition XXE 漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：http://blog.logicaldoc.com/
CNVD-2017-24570	TYPO3 Faceted Search Extension SQL 注入漏洞	高	用户可联系供应商获得补丁信息：https://typo3.com/
CNVD-2017-24566	TYPO3 Content Rating Extbase Extension SQL 注入漏洞	高	用户可联系供应商获得补丁信息：https://typo3.com/
CNVD-2017-24615	Atutor SQL 注入漏洞（CNVD-2017-24615）	高	用户可联系供应商获得补丁信息：http://www.atutor.ca/atutor/
CNVD-2017-25068	Ruby UTF-8 解析器拒绝服务漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://bugs.ruby-lang.org/issues/13742
CNVD-2017-25425	WordPress Task Manager Pro 存在多个漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://wpvulndb.com/plugins/task-manager-pro
CNVD-2017-25520	Lhaz+不可信搜索路径漏洞漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://chitora.com/jvn21369452.html
CNVD-2017-25531	Lhaz 安装程序不可信搜索路径漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://chitora.com/jvn21369452.html

表 4 部分重要高危漏洞列表

小结：本周，Apache 被披露存在 S2-052、S2-053 远程代码执行漏洞，攻击者可利用漏洞执行任意代码。此外， Adobe、Google、Smiths Medical 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制、读取内存数据、执行任意代码或发起拒绝服务攻击等。另外，National Instruments 被披露存在内存破坏漏洞，攻击者可利用漏洞造成拒绝服务。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. Apache Struts2（S2-052）漏洞

Apache Struts2 是 Apache 基金会发布的一款实现了 MVC 模式的中间件软件，广泛应用于 Web 开发和大型网站建设。Apache Struts 2.5 - Struts 2.5.12 版本的 REST 插件存在远程代码执行漏洞（CVE-2017-9805）。当 Struts2 通过 REST 插件使用 XStream 的实例 xstreamhandler 处理反序列化 XML 有效载荷时没有进行任何过滤，导致远程攻击者可以利用该漏洞构造恶意的 XML 内容，进而获取业务数据或服务器权限，执行任意代码。

参考链接：http://www.freebuf.com/news/146828.html

2. 华为、三星等手机 Bootloader 被曝存在多个高危漏洞

California 大学的研究团队发现主流手机平台的 bootloader 中存在代码执行和 DOS 的安全漏洞。研究人员用 BootStomp 发现了 6 个新发现的漏洞，其中 5 个分别被厂商确认。还有一个之前报告过的安全缺陷。这些漏洞中有的允许攻击者作为 bootloader 的一部分执行二进制代码，攻击者也可以进行永久的 DOS 攻击。研究人员开发的工具 Boot Stomp 能识别出两个 bootloader 的漏洞，攻击者可以在 root 权限下利用这两个漏洞解锁设备并打破信任链。

参考链接：http://www.freebuf.com/news/146858.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