

信息安全漏洞周报

2013 年 08 月 26 日-2013 年 09 月 01 日

2013 年第 35 期

本周漏洞基本情况

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 147 个，其中高危漏洞 50 个、中危漏洞 78 个、低危漏洞 19 个。上述漏洞中，可利用来实施远程攻击的漏洞有 132 个。本周收录的漏洞中，已有 100 个漏洞由厂商提供了修补方案，建议用户及时下载补丁更新程序，避免遭受网络攻击。本周互联网上出现“StarUML WinGraphviz.dll ActiveX 控件缓冲区溢出漏洞”、“RubyGems Sounder 'sound.rb' 远程命令注入漏洞”等的零日攻击代码，请使用相关产品的用户注意加强防范。

成员单位报送漏洞统计

本周，共 6 家成员单位及个人报送了本周收录的全部 147 个漏洞。各单位报送情况如表 1 所示。其中，安天实验室、天融信、启明星辰等单位报送数量较多。此外，知道创宇公司、High-TechBridgeSecurity Research Lab、网神信息技术（北京）股份有限公司、北京网御星云信息技术有限公司以及个人报送者向 CNVD 提交了 8 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
安天实验室	94	0
天融信	82	0
启明星辰	71	0
绿盟科技	43	0
恒安嘉新	42	0
知道创宇	1	1
High-Tech Bridge	1	1

网神信息技术（北京）股份有限公司	1	1
北京网御星云信息技术有限公司	2	2
个人	3	3
报送总计	340	8
录入总计	147（去重）	8

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Plone、IBM、McAfee、Cisco 等多家厂商的产品，部分漏洞数量按厂商统计如表 2 所示。

序号	厂商（产品）	漏洞数量	所占比例
1	Plone	13	9%
2	IBM	11	7%
3	McAfee	11	7%
4	Cisco	8	5%
5	FFmpeg	5	3%
6	wordpress	5	3%
7	Google	4	3%
8	Linux	4	3%
9	Drupal	3	2%
10	Samsung	2	1%
11	其它	81	57%

表 2 漏洞产品涉及厂商分布统计表

漏洞按影响类型统计

本周，CNVD 收录了 147 个漏洞。其中应用程序漏洞 98 个，WEB 应用漏洞 35 个，操作系统漏洞 5 个，数据库漏洞 1 个，网络设备漏洞 8 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	98
WEB 应用漏洞	35
网络设备漏洞	8
操作系统漏洞	5
安全产品漏洞	0
数据库漏洞	1

表 3 漏洞按影响类型统计表

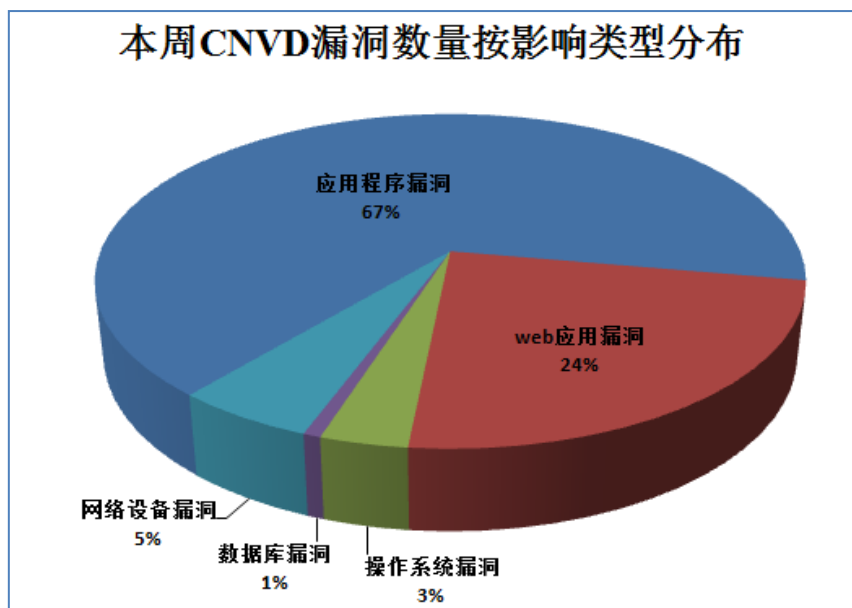


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 13 个电信行业漏洞和 1 个移动互联网行业漏洞（如下列表所示）。其中，“Belkin F5D7234-4 G Wireless Router 输入验证漏洞、Cisco Unified Communications Manager 拒绝服务漏洞（CNVD-2013-12598）、Cisco Unified Communications Manager 拒绝服务漏洞（CNVD-2013-12599）、Cisco Unified Communications Manager 'SIP'拒绝服务漏洞、IBM WebSphere DataPower SOA Appliance Kerberos AAA 策略安全绕过漏洞、Cisco Unified Communications Manager 缓冲区溢出漏洞”的综合评级均为“高危”。相关厂商已经发布了漏洞修复程序。本周，CNVD 未收录工控系统漏洞。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2013-12686	IBM DB2 和 DB2 Connect 存在多个未授权访问漏洞	中危	有补丁
电信	CNVD-2013-12629	IBM WebSphere Commerce 工具页跨站脚本漏洞	中危	有补丁
电信	CNVD-2013-12670	Belkin F5D7234-4 G Wireless Router 输入验证漏洞	高危	无补丁
电信	CNVD-2013-12598	Cisco Unified Communications Manager 拒绝服务漏洞（CNVD-2013-12598）	高危	有补丁
电信	CNVD-2013-12599	Cisco Unified Communications Manager 拒绝服务漏洞（CNVD-2013-12599）	高危	有补丁
电信	CNVD-2013-12600	Cisco Unified Communications Manager 'SIP'拒绝服务漏洞	高危	有补丁
电信	CNVD-2013-12606	Sitecom N300/N600 WPA2/管理密码生成算法漏洞	中危	有补丁

		洞		
电信	CNVD-2013-12607	Sitecom N300/N600 未文档化 Telnet 服务漏洞	中危	有补丁
电信	CNVD-2013-12608	Sitecom N300/N600 内置账户漏洞	中危	有补丁
电信	CNVD-2013-12616	IBM WebSphere DataPower SOA Appliance Kerberos AAA 策略安全绕过漏洞	高危	有补丁
电信	CNVD-2013-12586	多个 NetGear ProSafe 交换机信息泄露漏洞	中危	无补丁
电信	CNVD-2013-12564	Cisco Unified Communications Manager 缓冲区溢 出漏洞	高危	有补丁
电信	CNVD-2013-12566	多个 NetGear ProSafe 交换机远程拒绝服务漏洞	中危	无补丁
移动互 联网	CNVD-2013-12623	Google Android PRNG 熵漏洞	低危	有补丁

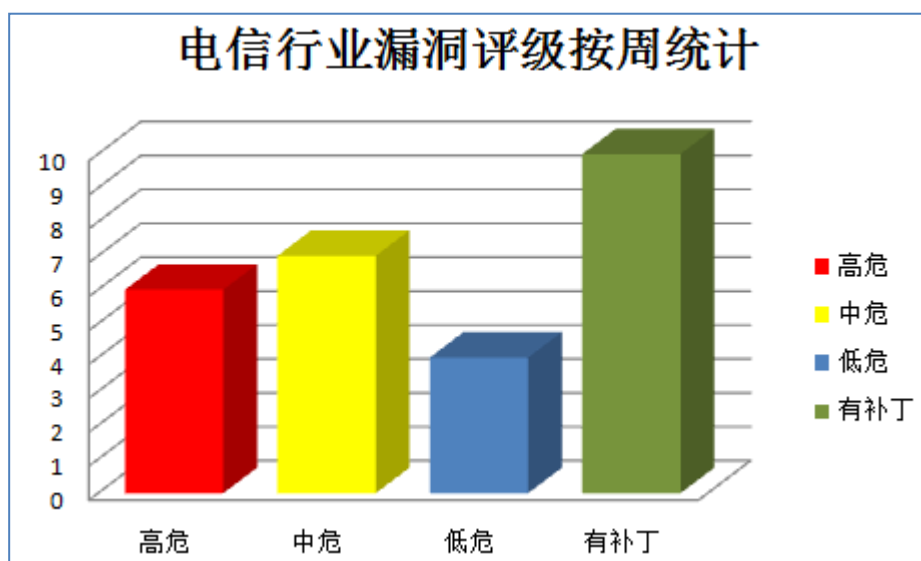


图 2 电信行业漏洞统计

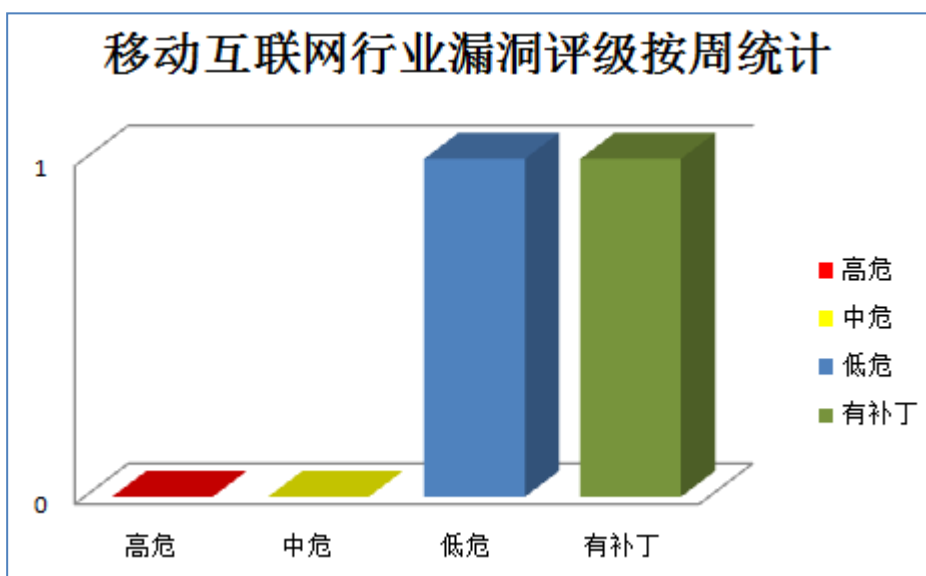


图 3 移动互联网行业漏洞统计

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

Google Chrome 是一款开源的 WEB 浏览器；Android 是基于 Linux 开放性内核的操作系统；Google Caja 是 Google 公司 Ben Laurie 发起了一个 Caja 项目，旨在制订一个 JavaScript 语言的子集和最佳编程指导方针，约束 JavaScript 程序员编写的代码。本周，上述产品被披露存在多个安全漏洞，远程攻击者利用漏洞可获得敏感信息，导致应用程序崩溃，执行任意代码。

CNVD 收录的相关漏洞包括：Google Caja V8 JavaScript VM 存在未明远程代码执行漏洞、Google Chrome GraphicsLayer::setContentTo 函数内存错误引用漏洞、Google Chrome Inspector HTML 导入处理拒绝服务漏洞、Google Android PRNG 熵漏洞。其中，“Google Caja V8 JavaScript VM 存在未明远程代码执行漏洞、Google Chrome GraphicsLayer::setContentTo 函数内存错误引用漏洞”的综合评级均为“高危”。厂商已发布了“Google Caja V8 JavaScript VM 存在未明远程代码执行漏洞、Google Android PRNG 熵漏洞”的修补程序。CNVD 提醒用户尽快下载补丁更新，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-2013-12701>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12617>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12618>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12623>

2、IBM 产品安全漏洞

IBM WebSphere DataPower SOA Appliances 是 IBM 针对面向服务架构(SOA)这一整体方法中的重要元素；IBM Optim Performance Manager 是一款基于网络开发的数据库性能监控工具；IBM DB2 Universal Database Server 是一款大型的商业关系数据库；Compute Grid 是 IBM WebSphere Extended Deployment V6.1 中推出的一项功能，提供了最完整的企业 Java 批处理编程解决方案；IBM WebSphere Commerce 是一款商务应用开发软件；IBM iNotes 是一个 Web 解决方案；IBM Cognos 是一款集成商业智能（BI）和计划的解决方案。本周，上述产品被披露存在多个安全漏洞，远程攻击者利用漏洞可获得敏感信息，执行未授权的访问。

CNVD 收录的相关漏洞包括：IBM WebSphere DataPower SOA Appliance Kerberos AAA 策略安全绕过漏洞、IBM Optim Performance Manager 目录遍历漏洞、IBM DB2 和 DB2 Connect 存在多个未授权访问漏洞、IBM WebSphere Extended Deployment Compute Grid 信息泄露漏洞、IBM WebSphere Commerce 工具页跨站脚本漏洞、IBM Lotus iNotes 存在多个未明跨站脚本漏洞、IBM Cognos Business Intelligence 访问绕过漏洞、IBM Cognos Business Intelligence 访问绕过漏洞等。其中，“IBM WebSphere DataPower SOA

Appliance Kerberos AAA 策略安全绕过漏洞”的综合评级为“高危”。厂商已发布了上述漏洞的修补程序。CNVD 提醒相关用户尽快下载补丁更新，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-2013-12616>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12672>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12686>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12628>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12629>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12630>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12633>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12681>

3、McAfee 产品安全漏洞

McAfee Network Data Loss Prevention 是一款数据防泄漏解决方案。本周，该产品被披露存在多个安全漏洞。攻击者利用漏洞可获得敏感信息，执行未授权的操作。

CNVD 收录的相关漏洞包括：McAfee Network Data Loss Prevention 单用户模式未验证本地访问漏洞、McAfee Network Data Loss Prevention 存在未明跨站脚本漏洞、McAfee Network Data Loss Prevention 存在未明跨站请求伪造漏洞、McAfee Network Data Loss Prevention Cookie HttpOnly 标记漏洞、McAfee Network Data Loss Prevention MYSQL 未验证本地访问漏洞、McAfee Network Data Loss Prevention SSH 密钥本地泄漏漏洞、McAfee Network Data Loss Prevention 会话并发漏洞、McAfee Network Data Loss Prevention 明文密码本地泄漏漏洞等。厂商已发布上述漏洞的修补程序。CNVD 提醒相关用户尽快下载补丁更新，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-2013-12658>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12659>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12660>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12661>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12666>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12667>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12668>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12665>

4、Red Hat 产品安全漏洞

Red Hat CloudForms 是红帽子推出的混合云管理软件；Red Hat Enterprise Virtualization Manager 是一款虚拟化解决方案应用。本周，该产品被披露存在多个漏洞，攻击者利用漏洞可获取权限，执行任意 Ruby 代码。

CNVD 收录的相关漏洞包括：Red Hat Enterprise Virtualization Manager 本地权限提

升漏洞（CNVD-2013-12687）、Red Hat CloudForms Management Engine 存在未明代码执行漏洞。上述漏洞的综合评级均为“高危”。厂商已发布了上述漏洞的修补程序。CNVD 提醒相关用户尽快下载补丁更新，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-2013-12677>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12687>

5、RubyGems Sounder 'sound.rb'远程命令注入漏洞

Sounder 是 Mac OSX afplay 命令的 ruby gem API。本周，该产品被披露存在一个综合评级为“高危”的命令注入漏洞。攻击者可以利用漏洞可执行任意命令。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-2013-12698>

更多高危漏洞如表 3 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-2013-12673	TYPO3 Slideshow Extension 存在未明 SQL 注入漏洞	高	暂无
CNVD-2013-12679	IncrediMail 'INCREDISPOOLERLib.Pop'控件缓冲区溢出漏洞	高	用户可联系供应商获得补丁信息： http://www.incredimail.com/english/home.aspx
CNVD-2013-12682	Software Toolbox TOP Server 远程拒绝服务漏洞	高	暂无
CNVD-2013-12680	Cisco Prime Central for HCS Assurance 远程拒绝服务漏洞（CNVD-2013-12680）	高	用户可参考如下供应商提供的安全公告获得补丁信息： http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130821-hcm
CNVD-2013-12684	Samsung DVR Cookie 身份验证绕过漏洞	高	暂无
CNVD-2013-12625	Rygel SQLite 字符串排序函数内存破坏漏洞	高	Rygel 0.19.5 已经修复此漏洞，建议用户下载更新： https://wiki.gnome.org/Rygel
CNVD-2013-12698	RubyGems Sounder 'sound.rb'远程命令注入漏洞	高	暂无
CNVD-2013-12626	Rygel 字符串排序函数内存破坏漏洞	高	Rygel 0.18.4 已经修复此漏洞，建议用户下载更新： https://wiki.gnome.org/Rygel

CNVD-2013-12702	B2BBuilder SQL 注入漏洞	高	暂无
CNVD-2013-12627	mooSocial 存在多个输入验证漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，Google、Red Hat、McAfee 和 IBM 的多款产品被披露存在多个漏洞，攻击者利用漏洞可获得敏感信息，执行未授权的操作，导致应用程序崩溃执行任意代码。此外，Sounde 程序被披露存在一个高危零日漏洞，建议相关用户应随时关注厂商主页，及时获取修复补丁或解决方案。

本周重要漏洞修补信息

CNVD 整理和发布以下重要安全修补信息。

1、Linux 发布升级程序，修补 Kernel 产品安全漏洞

Linux Kernel 是 Linux 操作系统的内核。本周，Linux 发布升级程序，修补 Kernel 产品存在的漏洞，攻击者可以利用漏洞造成内核崩溃。CNVD 已收录相关补丁，请广大用户及时下载更新，避免引发漏洞相关的安全事件。

补丁下载链接：<http://www.cnvd.org.cn/patchInfo/show/39159>

<http://www.cnvd.org.cn/patchInfo/show/39163>

<http://www.cnvd.org.cn/patchInfo/show/39171>

<http://www.cnvd.org.cn/patchInfo/show/39220>

本周要闻速递

1. 苹果 ios6 漏洞致程序闪退或崩溃

8 月 31 日消息，苹果 ios 和 MacOS 系统被发现一个远程拒绝服务漏洞，发送一段阿拉伯字符串到 ios 或 mac 用户的聊天软件或短信，将导致应用闪退甚至程序崩溃。用户通过聊天软件、邮件、短信、微博等接收该字符串时，会出现程序闪退。目前，只有 ios6 和 OSx10.8 系统受到该漏洞影响，ios5 等低版本不受影响，ios7 和 osX10.9 中该漏洞也已修复。目前针对该漏洞的补丁还未出，部分应用已经做出紧急应对处理，比如拦截导致问题的字符串，以及提出临时解决方案等。

参考链接：<http://news.zol.com.cn/article/143093.html>

2. OS X 重大安全漏洞

苹果 Mac OS X 中一个地址不明的安全漏洞被发现，恶意入侵者可通过修改用户的时钟，利用时间戳设置来绕开系统的常规授权验证方式，从而获得读取计算机所有文件的最高权限。该漏洞一直没有被修复，受影响的系统有 OS X 10.7~10.8.4，苹果目前并没有做出回应。该安全漏洞已经存在了将近半年的时间，安全漏洞测试工具 Metasploit 的开发人员现在创建了新的模块，从而可以更容易地发现 Mac 上的漏洞。该漏洞以 Unix 的“sudo”指令为基础，将允许或拒绝用户当前权限级别的操作。拥有最高级别权限的用户将可以访问其它用户的文件，尽管这些用户设置了密码保护。

参考链接：<http://www.kankanews.com/ICkengine/archives/36539.shtml>

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

国家互联网应急中心是国家计算机网络应急技术处理协调中心的简称（英文简称为 CNCERT 或 CNCERT/CC），成立于 1999 年 9 月，是一个非政府非盈利的网络安全技术协调组织，主要任务是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展中国互联网上网络安全事件的预防、发现、预警和协调处置等工作，以维护中国公共互联网环境的安全、保障基础信息网络和网上重要信息系统的安全运行。目前，CNCERT 在我国大陆 31 个省、自治区、直辖市设有分中心。

同时，CNCERT 积极开展国际合作，是中国处理网络安全事件的对外窗口。CNCERT 是国际著名网络安全合作组织 FIRST 正式成员，也是 APCERT 的发起人之一，致力于构建跨境网络安全事件的快速响应和协调处置机制。截止 2012 年，CNCERT 与 51 个国家和地区的 91 个组织建立了“CNCERT 国际合作伙伴”关系。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82990999