

信息安全漏洞周报

2013 年 09 月 16 日-2013 年 09 月 22 日

2013 年第 38 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 165 个，其中高危漏洞 84 个、中危漏洞 76 个、低危漏洞 5 个。上述漏洞中，可利用来实施远程攻击的漏洞有 151 个。本周收录的漏洞中，已有 136 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“Mitsubishi MC-WorX 'IcoLaunch.dll' ActiveX 控件远程代码执行漏洞”、“PHPLinks 存在多个跨站脚本漏洞”等零日攻击代码，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 165 个漏洞。各单位报送情况如表 1 所示。其中，天融信、启明星辰、安天实验室、恒安嘉新等单位报送数量较多。此外，知道创宇公司、High-TechBridgeSecurityResearch Lab 以及个人报送者向 CNVD 提交了 4 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
天融信	157	0
启明星辰	65	0
安天实验室	40	0
恒安嘉新	30	0
绿盟科技	27	0
知道创宇	2	1
High-Tech Bridge Security Research Lab	1	1

个人	2	2
报送总计	324	4
录入总计	165（去重）	4

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Microsoft、Mozilla、FFmpeg 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	Microsoft	33	20%
2	Mozilla	19	12%
3	FFmpeg	13	8%
4	Cisco	11	7%
5	Apple	11	7%
6	wordpress	6	4%
7	HP	5	3%
8	Moodle	4	2%
9	Drupal	3	2%
10	Linux	2	1%
11	其它	58	34%

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 165 个漏洞。其中应用程序漏洞 118 个，WEB 应用漏洞 22 个，操作系统漏洞 16 个，网络设备漏洞 7 个，安全产品漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	118
WEB 应用漏洞	22
网络设备漏洞	7
操作系统漏洞	16
安全产品漏洞	2
数据库漏洞	0

表 3 漏洞按影响类型统计表

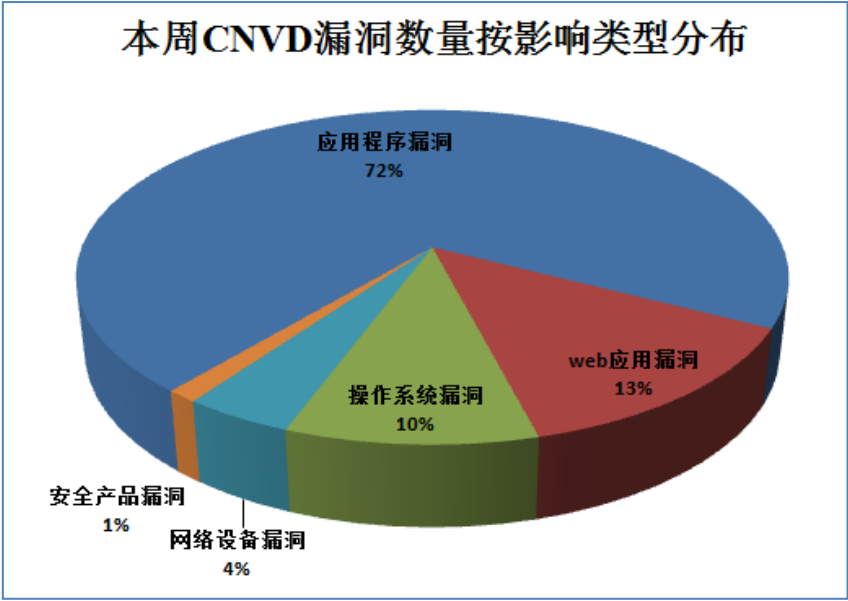


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 8 个电信行业漏洞、3 个工控系统行业漏洞和 1 个移动互联网行业漏洞（如下列表所示）。其中，“Juniper Junos J-Web 任意命令执行漏洞、WellinTech KingView ActiveX 存在多个任意文件覆盖漏洞、Mitsubishi MC-WorX 'IcoLaunch.dll' ActiveX 控件远程代码执行漏洞、Siemens SCALANCE X-200 系列交换机会话劫持漏洞、安卓下 Mozilla Firefox 共享文件库加载本地文件包含漏洞、Juniper Networks 多个 Junos 服务存在未明拒绝服务漏洞”的综合评级均为“高危”。相关厂商已经发布了漏洞修复程序。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2013-13104	ONO Hitron CDE-30364 存在多个跨站请求伪造漏洞	中危	无补丁
电信	CNVD-2013-13027	Siemens SCALANCE X-200 系列交换机会话劫持漏洞	高危	有补丁
电信	CNVD-2013-13033	NetVanta 3430 WEB 接口默认管理账户漏洞	中危	无补丁
电信	CNVD-2013-13041	Junos Pulse Secure Access Service 登录页面跨站脚本漏洞	中危	有补丁
电信	CNVD-2013-13042	Juniper Networks 多个 Junos 服务存在未明拒绝服务漏洞	高危	有补丁
电信	CNVD-2013-13050	Cisco Prime LAN Management Solution 跨帧脚本漏洞	中危	有补丁

电信	CNVD-2013-13052	多个 Cisco 产品 ActiveMQ 组件拒绝服务漏洞	中危	有补丁
电信	CNVD-2013-13089	Juniper Junos J-Web 任意命令执行漏洞	高危	有补丁
工控系统	CNVD-2013-13162	WellinTech KingView ActiveX 存在多个任意文件覆盖漏洞	高危	无补丁
工控系统	CNVD-2013-13110	Mitsubishi MC-WorX 'IcoLaunch.dll' ActiveX 控件远程代码执行漏洞	高危	无补丁
工控系统	CNVD-2013-13027	Siemens SCALANCE X-200 系列交换机会话劫持漏洞	高危	有补丁
移动互联网	CNVD-2013-13136	安卓下 Mozilla Firefox 共享文库加载本地文件包含漏洞	高危	有补丁

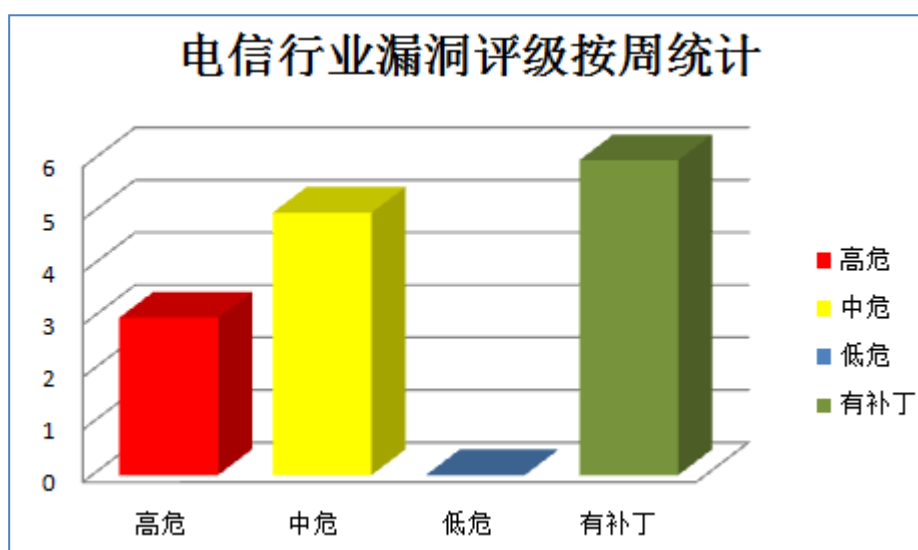


图 2 电信行业漏洞统计

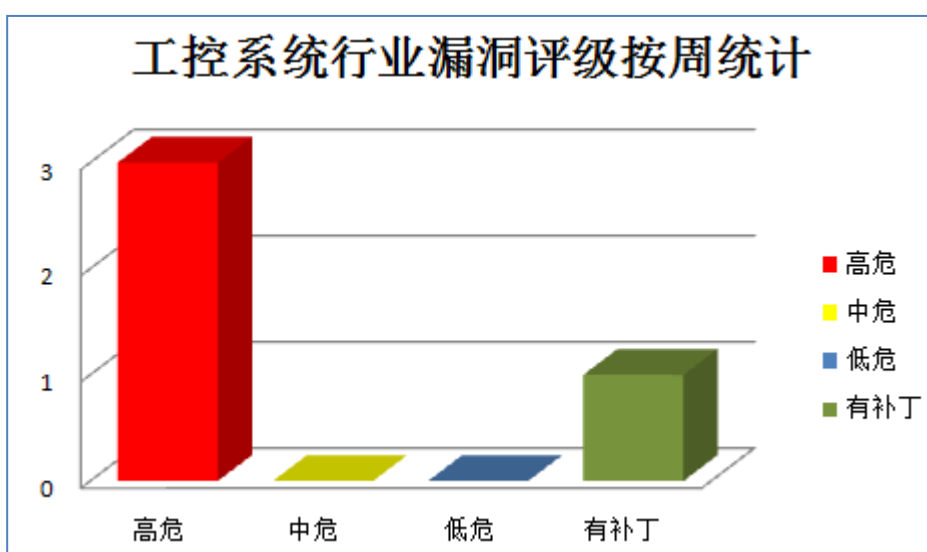


图 3 工控系统行业漏洞统计

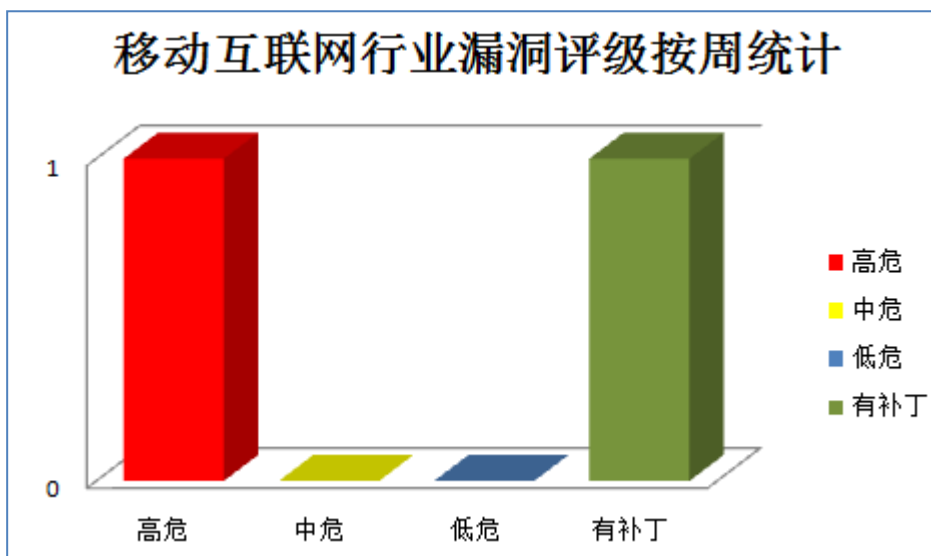


图 4 移动互联网行业漏洞统计

本周重要漏洞信息

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、Microsoft 产品安全漏洞

Microsoft Internet Explorer 是一款 WEB 浏览器。本周，该产品被披露存在多个漏洞，攻击者利用漏洞可执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft IE MSHTML 内存破坏远程代码执行漏洞、Microsoft Internet Explorer 内存破坏漏洞（CNVD-2013-13096）。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-2013-13095>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13096>

2、Mozilla 产品安全漏洞

Mozilla Firefox/SeaMonkey/Thunderbird 是 Mozilla 所发布的 WEB 浏览器/新闻组客户端/邮件客户端。本周，上述产品被披露存在多个安全漏洞。攻击者利用漏洞可使应用程序崩溃，执行任意代码。

CNVD 收录的相关漏洞包括：Mozilla 多个产品 JS_GetGlobalForScopeChain 内存错误引用漏洞、Mozilla 多个产品 nsGfxScrollFrameInner::IsLTR()函数内存破坏漏洞、Mozilla 多个产品 mozilla::layout::ScrollbarActivity 函数内存错误引用漏洞、Mozilla 多个产品 nsFloatManager::GetFlowArea()函数缓冲区溢出漏洞、Mozilla 多个产品 Select 元素处理内存错误引用漏洞、Mozilla 多个产品动画管理样式表克隆内存错误引用漏洞、Mozilla 多个产品 HTML5 Tree Builder template 元素处理任意代码执行漏洞、Mozilla 多个产品存在多个未明内存破坏漏洞（CNVD-2013-13148）等。上述漏洞的综合评级均为“高危”。

厂商已经发布了上述漏洞的修补程序。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-2013-13131>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13133>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13134>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13135>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13143>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13145>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13147>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13148>

3、Apple 产品安全漏洞

Apple Mac OS X 是一款苹果公司开发的操作系统。本周，该产品被披露存在多个安全漏洞。攻击者利用漏洞可绕过安全限制，获取敏感信息，使应用程序崩溃，执行任意代码。

CNVD 收录的相关漏洞包括：Apple Mac OS X 撤消 SSL 证书验证安全绕过漏洞、Apple Mac OS X Server 存在多个跨站脚本漏洞、Apple Mac OS X 内存破坏漏洞（CNVD-2013-12996）、Apple Mac OS X 锁屏安全绕过漏洞、Apple Mac OS X Unicode 字符串拒绝服务漏洞、Apple Mac OS X 'IGMP'拒绝服务漏洞、Apple Mac OS X PDF 文件缓冲区溢出漏洞、Apple MAC OS X ImageIO 缓冲区溢出漏洞（CNVD-2013-13009）等。其中，“Apple Mac OS X 撤消 SSL 证书验证安全绕过漏洞”的综合评级为“高危”。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安全事件。

参考链接：<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13011>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13156>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12996>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12998>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12999>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13000>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13006>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13009>

4、Cisco 产品安全漏洞

Cisco Unified Computing System 通过将统一计算、网络、存储访问和虚拟化整合到一个系统中，简化 IT 管理并提高灵活性；Cisco NX-OS 软件是一个数据中心级的操作系统；Cisco Open Network Environment Platform 思科开放式网络环境，是全面而广泛的网络可编程性的实现方法。本周，上述产品被披露存在多个安全漏洞。攻击者利用漏洞

可查看修改数据，使应用程序崩溃。

CNVD 收录的相关漏洞包括：Cisco Unified Computing System 私钥泄露漏洞、Cisco Unified Computing System 畸形联系地址处理本地拒绝服务漏洞、Cisco Unified Computing System 证书校验安全绕过漏洞(CNVD-2013-13155)、Cisco Unified Computing System 证书校验安全绕过漏洞、Cisco NX-OS software BGP 正则表达式拒绝服务漏洞、Cisco Open Network Environment Platform 拒绝服务漏洞、多个 Cisco Unified MeetingPlace 产品跨站请求伪造漏洞。厂商已经发布了除“多个 Cisco Unified MeetingPlace 产品跨站请求伪造漏洞”外，其余漏洞的修补程序。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-2013-13153>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13154>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13155>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13157>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13158>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13097>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13001>

5、Mitsubishi MC-WorX 'IcoLaunch.dll' ActiveX 控件远程代码执行漏洞

Mitsubishi MC-WorkX 是工厂自动化应用工具。本周，该产品被披露存在一个综合评级为“高危”的远程代码执行漏洞。Mitsubishi MC-WorkX LaunchCtl ActiveX 控件(IcoLaunch.dll)提供不安全的"FileName"属性，远程攻击者利用漏洞可构建恶意 WEB 页，诱使用户解析，执行任意程序。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-2013-13110>

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-2013-13128	Zyware Health Monitoring System 存在多个漏洞	高	暂无
CNVD-2013-13129	Western Digital Arkeia 未验证固件上传漏洞	高	Western Digital Arkeia Appliance v10.1.10 已经修改该漏洞，建议用户下载更新： http://www.arkeia.com
CNVD-2013-13151	FFmpeg 'libavcodec'越界内存访问漏洞	高	用户可参考如下厂商提供的安全公告获得补丁信息： http://git.videolan.org/?p=ffmpeg.git ;

			a=commit;h=39ed5442620a7a0fd2328b7d4aefc6ae152c5441
CNVD-2013-13159	OpenEMR 任意文件上传漏洞	高	OpenEMR 4.1.2 已经修改该漏洞，建议用户下载使用： http://www.open-emr.org
CNVD-2013-13162	WellinTech KingView ActiveX 存在多个任意文件覆盖漏洞	高	暂无
CNVD-2013-13100	Uploadify 'uploadify.php'存在多个输入验证漏洞	高	暂无
CNVD-2013-13105	MPlayer Server 应答任意远程文件覆盖漏洞	高	MPlayer 1.1.1 已经修改该漏洞，建议用户下载更新： http://www.mplayerhq.hu/design7/news.html
CNVD-2013-13102	Practico CMS 'uid' SQL 注入漏洞	高	暂无
CNVD-2013-13107	Moodle 查询字符串 SQL 注入漏洞	高	Moodle 2.5.2, 2.4.6 和 2.3.9 已经修改该漏洞，建议用户下载更新： http://www.moodle.org
CNVD-2013-13110	Mitsubishi MC-WorkX 'IcoLaunch.dll' ActiveX 控件远程代码执行漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，Microsoft IE、Apple Mac OS X、Mozilla 和 Cisco 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，使应用程序崩溃，执行任意代码。Mitsubishi MC-WorkX 自动化应用工具被披露存在一个高危零日漏洞需要引起重视，建议相关用户随时关注厂商主页，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获得敏感信息、提升权限或使系统崩溃。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/39616>

<http://www.cnvd.org.cn/patchInfo/show/39580>



本周要闻速递

1. iOS 7 再曝安全漏洞可绕过锁屏打电话

9月22日消息，在iOS 7正式发布仅一天后，就有用户发现了其中存在的一个锁屏漏洞。而现在，第二个锁屏漏洞再次被媒体曝光，它可以绕过锁屏界面直接拨打电话。该漏洞的具体操作方式是，在一部由密码锁定的iPhone当中进入紧急通话界面，输入一个号码，然后重复按下绿色的“呼叫”按键。最后这个按键会呈现卡住的状态，然后手机崩溃，屏幕变成白苹果 logo+黑色界面，但这个号码实际上已经拨出去了。经过测试，这个漏洞在安装了iOS 7的iPhone 5和4S上都存在。

参考链接：<http://digi.it.sohu.com/20130922/n386950954.shtml>

2. 微软IE浏览器存高危“中秋节漏洞” 尚无补丁

9月22日消息，据经济之声《天下财经》报道，微软最新发布的安全公告显示，IE浏览器存在一个高危漏洞，现在已经被命名为IE“中秋节漏洞”，它很容易遭到黑客攻击，被远程控制。截至目前，这一漏洞已经成为今年发现的威胁级别最高、影响用户数量最多的漏洞，但是，微软还没有推出可以修复这个漏洞的正式补丁。

参考链接：http://finance.cnr.cn/txcj/201309/t20130922_513651899.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