

信息安全漏洞周报

2013 年 09 月 09 日-2013 年 09 月 15 日

2013 年第 37 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 133 个，其中高危漏洞 40 个、中危漏洞 79 个、低危漏洞 14 个。上述漏洞中，可利用来实施远程攻击的漏洞有 108 个。本周收录的漏洞中，已有 106 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“GOM Player '.wav'文件拒绝服务漏洞”、“Bo-Blog SQL 注入漏洞”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 7 家成员单位及个人报送了本周收录的全部 133 个漏洞。各单位报送情况如表 1 所示。其中，启明星辰、绿盟科技、安天实验室、天融信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 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
启明星辰	132	0
绿盟科技	90	0
天融信	84	0
安天实验室	71	0
恒安嘉新	51	0
东软	3	0
知道创宇	4	2

High-Tech Bridge Security Research Lab	1	1
个人	5	5
报送总计	441	8
录入总计	133（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 Microsoft、Adobe、Mediawiki 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	16	12%
2	Adobe	14	10%
3	Mediawiki	8	6%
4	IBM	8	6%
5	Open-Xchange	7	5%
6	Cisco	5	4%
7	WordPress	5	4%
8	Cogent Real-Time Systems	3	2%
9	Sophos	2	2%
10	TYPO3	2	2%
11	其它	63	47%

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 133 个漏洞。其中应用程序漏洞 95 个，WEB 应用漏洞 20 个，操作系统漏洞 13 个，网络设备漏洞 2 个，安全产品漏洞 3 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	95
WEB 应用漏洞	20
网络设备漏洞	2
操作系统漏洞	13
安全产品漏洞	3
数据库漏洞	0

表 3 漏洞按影响类型统计表

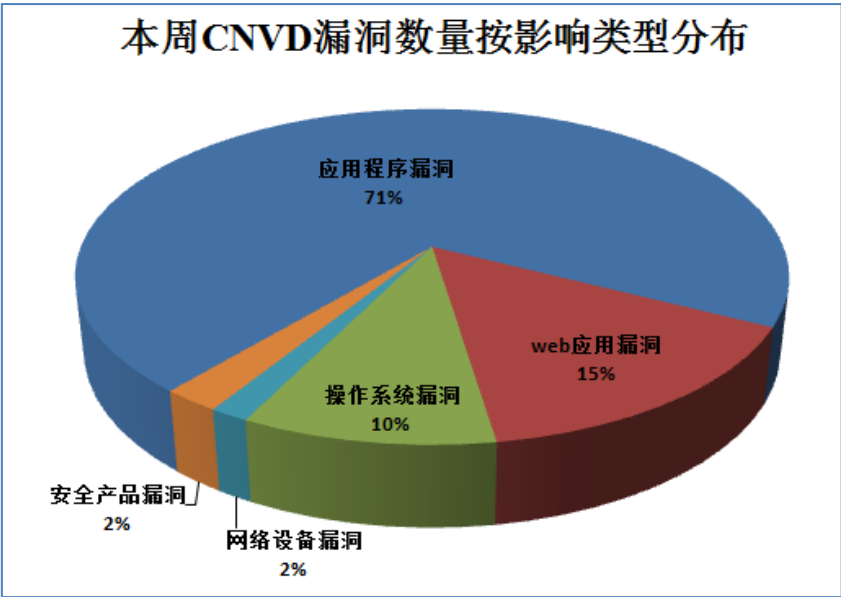


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 1 个电信行业漏洞和 3 个工控系统行业漏洞(如下列表所示)。其中，“D-Link DIR-505 路由器存在多个漏洞”的综合评级为“高危”。相关厂商已经发布了漏洞修复程序。本周，CNVD 未收录移动互联网行业漏洞。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2013-12987	D-Link DIR-505 路由器存在多个漏洞	高危	有补丁
工控系统	CNVD-2013-12943	Cogent DataHub 存在未明任意文件覆盖漏洞	中危	无补丁
工控系统	CNVD-2013-12944	Cogent DataHub 远程拒绝服务漏洞（CNVD-2013-12944）	中危	无补丁
工控系统	CNVD-2013-12945	Cogent DataHub 远程拒绝服务漏洞（CNVD-2013-12945）	中危	无补丁

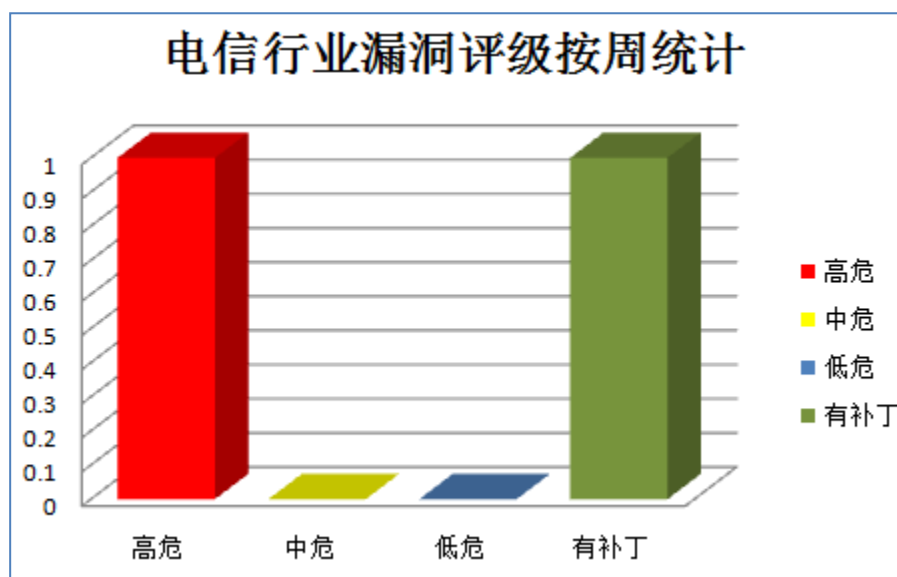


图 2 电信行业漏洞统计

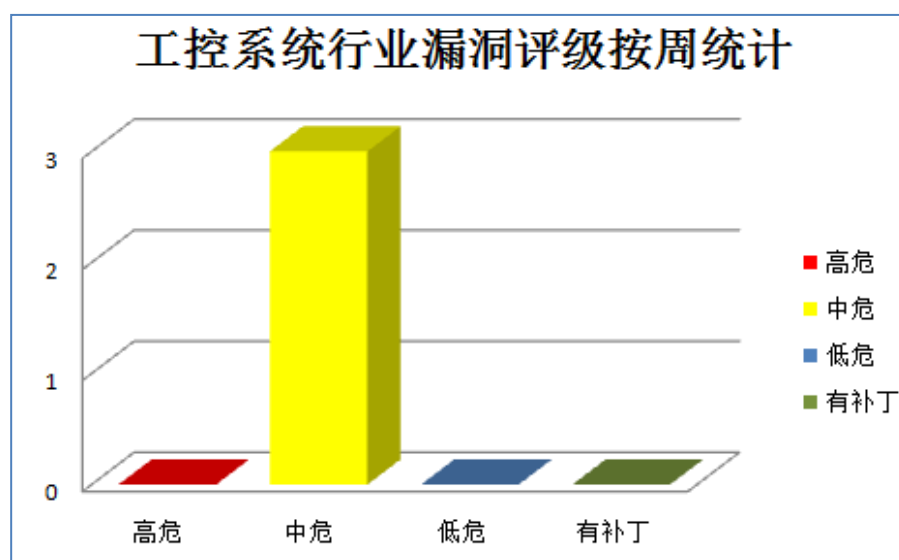


图 3 工控系统行业漏洞统计

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

本周，微软发布了 2013 年 9 月份的月度例行安全公告，共含 13 项更新，修复了 Microsoft Windows、Office、Internet Explorer、SharePoint Portal Server、SharePoint Server、Office Web Apps 和 FrontPage 软件中存在的 53 个安全漏洞。其中，MS13-067、MS13-068、MS13-069 和 MS13-070 项更新综合评级均为最高级“严重”级别，剩余 9 项更新综合评级均为“重要”级别。利用上述漏洞，攻击者可以执行任意代码，提升权限，进行拒绝服务攻击，获取敏感信息。

CNVD 收录的相关漏洞包括：Microsoft Windows Win32k.sys 内存对象处理存在未明本地权限提升漏洞（CNVD-2013-12947、CNVD-2013-12948、CNVD-2013-12949、CNVD-2013-12950、CNVD-2013-12951、CNVD-2013-12952、CNVD-2013-12953）、Microsoft Windows 特制 OLE 对象处理任意代码执行漏洞等。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 提醒广大 Microsoft 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-2013-12947>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12948>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12949>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12950>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12951>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12952>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12953>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12955>

2、Adobe 产品安全漏洞

本周,Adobe 发布了安全更新公告,用于修复 AdobeFlash Player、Shockwave Player、Acrobat、Reader 产品存在的 14 个安全漏洞,相关产品运行在 Windows、Macintosh、Android、Linux 多个平台。利用上述漏洞,攻击者可以在所受影响的系统上执行任意代码,控制系统或使系统崩溃。

CNVD 收录的相关漏洞包括：Adobe Shockwave Player 存在未明内存破坏漏洞（CNVD-2013-12991、CNVD-2013-12992）、Adobe Reader / Acrobat 存在未明整数溢出漏洞（CNVD-2013-12993、CNVD-2013-12994）、Adobe Reader / Acrobat 存在未明缓冲区溢出漏洞（CNVD-2013-12960、CNVD-2013-12963）、Adobe Reader / Acrobat 存在未明内存破坏漏洞（CNVD-2013-12961、CNVD-2013-12962）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 提醒广大 Adobe 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-2013-12991>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12992>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12993>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12994>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12960>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12961>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12962>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12963>

3、Cisco 产品安全漏洞

Cisco SocialMiner 是一款社交网络监控软件；Cisco Unified IP Phone 8945 Series 是 IP 电话终端设备，提供语音、视频等功能。Cisco Adaptive Security Appliance 是一款自适应安全设备，可提供安全和 VPN 服务的模块。本周，上述产品被披露存在多个安全漏洞。攻击者利用漏洞可获得敏感信息，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco SocialMiner 信息泄漏漏洞、Cisco Unified IP Phone 8945 Series 拒绝服务漏洞、Cisco Adaptive Security Appliance (ASA) Software 拒绝服务漏洞、Cisco SocialMiner 跨站脚本漏洞。厂商已经发布了除“Cisco SocialMiner 跨站脚本漏洞”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-2013-12989>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12923>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12910>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12909>

4、IBM 产品安全漏洞

IBM Rational Requirements Composer 软件是一项需求定义解决方案；IBM Securityl AppScan Enterprise 是一个多用户 Web 应用程序安全解决方案，提供集中的安全性扫描、数据合并和报告、补救功能、执行仪表板等功能。本周，上述产品被披露存在多个漏洞，攻击者利用漏洞可获得未授权的访问，获取敏感信息，执行任意代码。

CNVD 收录的相关漏洞包括：IBM Rational Requirements Composer 存在未明验证绕过漏洞、IBM Rational Requirements Composer 存在未明验证绕过漏洞、IBM Rational Requirements Composer 存在未明任意代码执行漏洞、IBM Rational Requirements Composer URI 重定向漏洞、IBM Security AppScan Enterprise 会话固定漏洞。其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-2013-12959>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12980>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12981>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12982>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12915>

5、Bo-Blog SQL 注入漏洞

Bo-Blog 是一套基于 PHP 和 MySQL 的免费博客系统软件，该软件包括留言本、表情、天气等。本周，该产品被披露存在一个综合评级为“高危”的 SQL 注入漏洞。由于程序未能正确过滤用户提交的输入，攻击者利用漏洞可控制应用程序，访问或修改数据。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-2013-12867>

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-2013-12937	VMware ESX 和 ESXi 缓冲区溢出漏洞	高	用户可联系厂商获得相应的升级或补丁程序: http://www.vmware.com
CNVD-2013-12986	E-Local Business Directory 'category_val'参数 SQL 注入漏洞	高	暂无
CNVD-2013-12987	D-Link DIR-505 路由器存在多个漏洞	高	D-Link Dir-505 1.07 版本已经修改该漏洞, 建议用户下载更新: ftp://ftp.dlink.com/Gateway/dir505/Firmware/dir505_fw_107.zip
CNVD-2013-12972	TORQUE pbs_mom 后台程序任意作业提交远程命令执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞: http://www.adaptivecomputing.com/torquepatch/fix_mom_priv_2.5.patch
CNVD-2013-12973	SUBNET Solutions SubSTATION Server 存在未明远程拒绝服务漏洞	高	用户可联系厂商获得相应的升级或者补丁程序: http://www.subnet.com/
CNVD-2013-12976	GOM Player 存在未明缓冲区溢出漏洞	高	GOMPlayer 2.2.53.5169 已经修改该漏洞, 建议用户下载更新: http://player.gomlab.com/eng/download/
CNVD-2013-12926	glFusion search.php SQL 注入漏洞	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://www.glfusion.org/article.php/glfusion131
CNVD-2013-12930	ProSoft RadioLinx ControlScape 可预测随机数生成器漏洞	高	用户可联系供应商获得补丁信息: http://www.prosoft-technology.com/
CNVD-2013-12931	TYPO3 File Abstraction Layer 远程 PHP 代码执行漏洞	高	用户可联系供应商获得补丁信息: http://typo3.org/
CNVD-2013-12913	AjaXplorer 文件上传漏洞	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://ajaxplorer.info/ajaxplorer-core-5-0-3/

表 3 部分高危漏洞列表

小结: 本周, Microsoft 和 Adobe 均发布了安全公告, 修复了其多款产品存在的多

个漏洞，而 IBM 和 Cisco 的多款产品被披露存在多个漏洞，攻击者利用上述漏洞可获得敏感信息，执行任意代码，或发起拒绝服务攻击。对于博客系统网站建设方，Bo-Blog 博客系统被披露存在一个高危零日漏洞需要引起重视对于虚拟化服务提供商，本周披露的 VMware ESX 和 ESXi 缓冲区溢出漏洞也应引起重视。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获得 root 权限。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/39410>

本周要闻速递

1. Android 新漏洞可被利用窃取信息和金钱

近期爆出 Android WebView 安全漏洞会导致大量应用成为黑客管道。该漏洞的原理是在 Android 的 SDK 中封装了 WebView 控件，该控件可以和使用它的应用程序结合得更加紧密，在页面内允许 JavaScript 调用 Java 代码。Java 代码本身可以调用系统本身的很多功能，如读写文件，打电话、发短信扣费等，甚至可以 root 手机、安装恶意程序。系统在设计时，对可以调用的 Java 代码做了一定限制，但这个限制在 4.2 之前的系统上不严密，导致限制可被绕过，形同虚设。为此，Google 在 Android 4.2 版本后规定允许被调用的函数必须以 Java script Interface 进行注解，所以如果某应用依赖的 API Level 为 17 或以上，就不会受到该问题的影响。如今漏洞危及 90% 的 Android 手机，当用户通过存在漏洞的 APP 打开网页后，可被大规模利用，如远程操控手机窃取隐私、扣费等。在各 App 开发者还没升级 App 之前，建议大家使用系统自带的浏览器访问网页，并慎重访问陌生人发来的链接。

参考链接：<http://news.163.com/13/0910/18/98EC32UT00014JB6.html>

2. 腾讯大幅提高漏洞报告赏金

腾讯安全团队今日发布消息“【感恩 致敬】互联网迈入大数据时代，用户安全至关重要。过去两年，TSRC 得到许多安全大牛帮助，向我们反馈漏洞，帮助快速修补。因

此我们时刻心怀感恩，不敢懈怠。为了更好答谢这些帮助腾讯用户的安全大牛，我们将大幅提升奖金额度，最高奖项可达 10 万，2013 年总金额 100 万。详细计划，敬请期待”。据悉，腾讯是目前国内甲方公司第一家采取现金模式来鼓励黑客、安全白帽子向其提交业务安全方面的漏洞，并且有知情人透露，腾讯安全会在现有额度技术上，最高金额大幅提升，单个漏洞最高奖金可达 10 万人民币，基本和国际巨头（facebook、google、paypal 等）标准看齐，本年度总额度会达到百万级。

参考链接：<http://digi.163.com/13/0909/15/98BER0IV00162OUT.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