

信息安全漏洞周报

2013 年 08 月 12 日-2013 年 08 月 18 日

2013 年第 33 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低。

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 73 个，其中高危漏洞 25 个、中危漏洞 41 个、低危漏洞 7 个。上述漏洞中，可利用来实施远程攻击的漏洞有 67 个。本周收录的漏洞中，已有 53 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“OneHTTPD 拒绝服务漏洞”、“Telmanik CMS Press 'page_name'参数 SQL 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 7 家成员单位及个人报送了本周收录的全部 73 个漏洞。各单位报送情况如表 1 所示。其中，天融信、安天实验室、启明星辰、绿盟科技等单位报送数量较多。此外，知道创宇公司和个人报送者向 CNVD 提交了 12 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	55	0
绿盟科技	37	0
安天实验室	77	0
天融信	97	0
恒安嘉新	35	0
知道创宇	1	1
东软	3	0
个人	16	11

报送总计	321	12
录入总计	73（去重）	12

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、IBM、Drupal 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	9	12%
2	IBM	7	9%
3	Drupal	6	8%
4	WordPress	4	5%
5	Mi Casa Verde	4	5%
6	Joomla!	2	3%
7	Cisco	2	3%
8	openstack	2	3%
9	Google	1	1%
10	Siemens	1	1%
11	其它	35	50%

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 73 个漏洞。其中应用程序漏洞 44 个，WEB 应用漏洞 20 个，操作系统漏洞 3 个，网络设备漏洞 6 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	44
WEB 应用漏洞	20
网络设备漏洞	6
操作系统漏洞	3
安全产品漏洞	0
数据库漏洞	0

表 3 漏洞按影响类型统计表

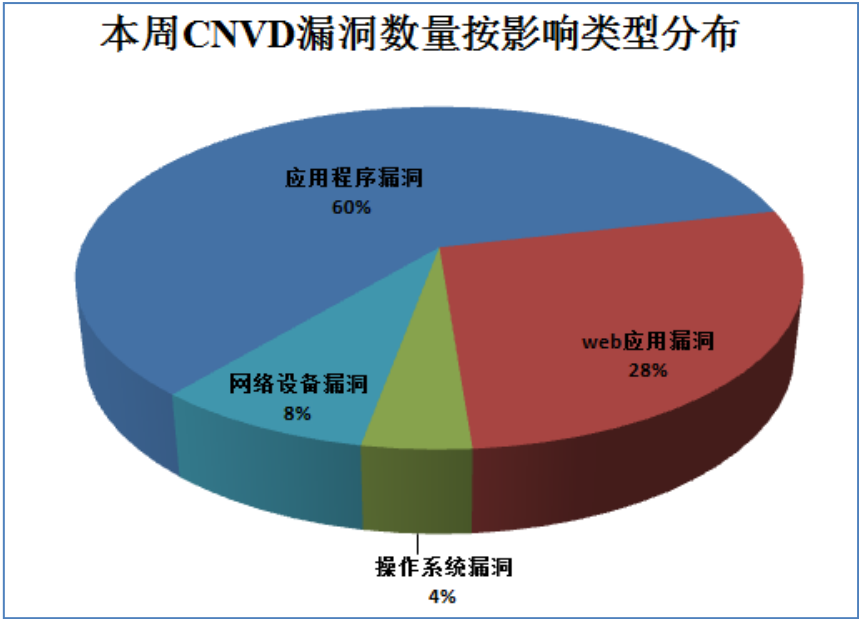


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 5 个电信行业漏洞、1 个移动互联网行业漏洞和 2 个工控系统漏洞（如下列表所示）。其中，“WiMAX 多个模块 L5 链接 PDU 处理整数溢出漏洞、Schweitzer Engineering Laboratories 多个设备远程拒绝服务漏洞”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-2013-12230	IBM WebSphere Portal 存在多个跨站脚本漏洞	中危	有补丁
电信	CNVD-2013-12146	Intel OSAL Crypt 模块密码记录信息泄漏漏洞	低危	无补丁
电信	CNVD-2013-12148	WiMAX 多个模块 L5 链接 PDU 处理整数溢出漏洞	高危	无补丁
电信	CNVD-2013-12147	WiMAX Supplicant 代理私钥管理本地信息泄漏漏洞	低危	无补丁
电信	CNVD-2013-12145	Intel wimax-ns Trace 模块不安全权限本地文件操作漏洞	低危	无补丁
移动互联网	CNVD-2013-12139	docomo overseas usage 应用敏感信息泄漏漏洞	中危	有补丁
工控系统	CNVD-2013-12159	Schweitzer Engineering Laboratories 多个设备本地拒绝服务漏洞	中危	有补丁
工控系统	CNVD-2013-12158	Schweitzer Engineering Laboratories 多个设备远程拒绝服务漏洞	高危	有补丁

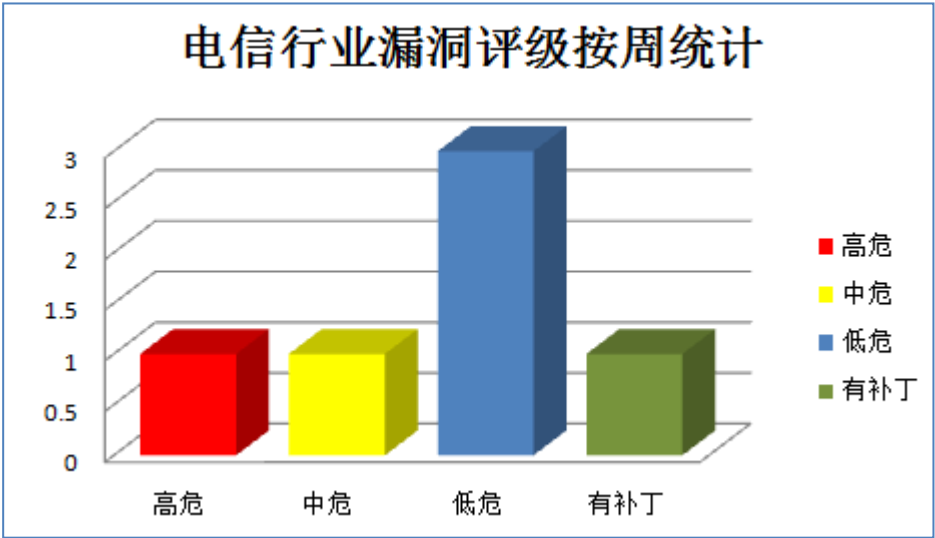


图 2 电信行业漏洞统计

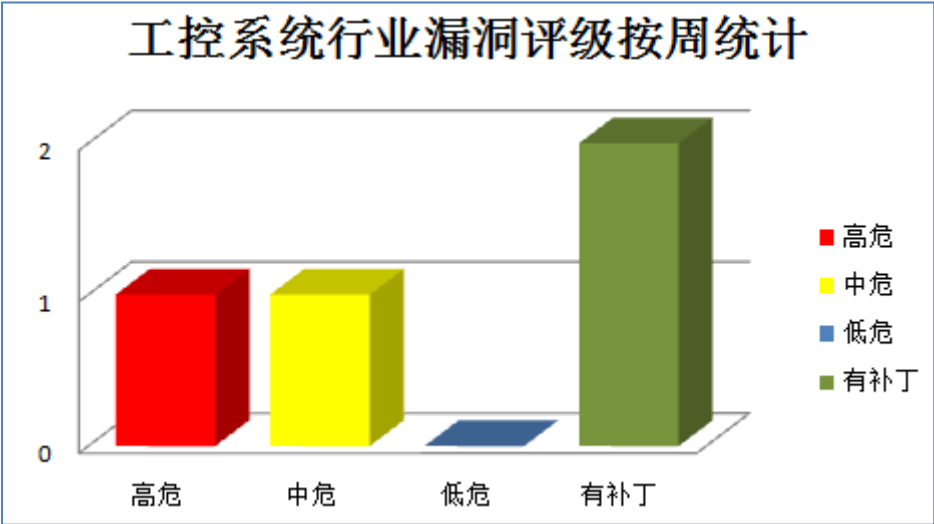


图 3 工控系统行业漏洞统计

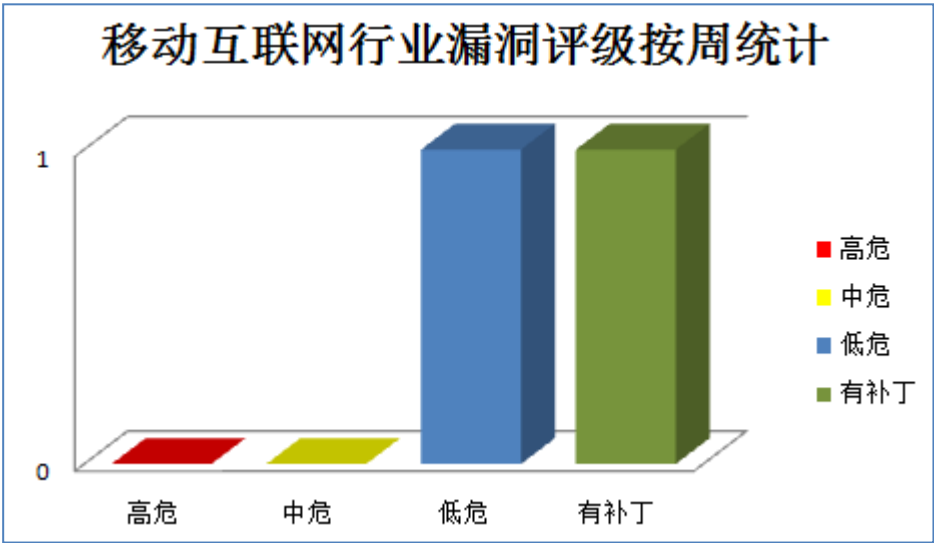


图 4 移动互联网行业漏洞统计



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

8 月 14 日，微软发布了 2013 年 8 月份的月度例行安全公告，共含 8 项更新，修复了 Microsoft Windows、Internet Explorer 和 Microsoft Server 软件中存在的 23 个安全漏洞。其中，MS13-059、MS13-060 和 MS13-061 项更新综合评级均为“严重”级别（微软最高危险级别），剩余 5 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 远程权限提升漏洞、Microsoft Internet Explorer 内存破坏漏洞（CNVD-2013-12324、CNVD-2013-12323、CNVD-2013-12320、CNVD-2013-12316）、Microsoft Windows Kernel 本地权限提升漏洞（CNVD-2013-12318、CNVD-2013-12317）、Microsoft Windows Uniscribe 字体解析远程代码执行漏洞等。上述漏洞的综合评级均为“高危”。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-2013-12423>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12424>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12425>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12426>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12427>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12428>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12429>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12433>

2、IBM 产品安全漏洞

IPMI 是智能型平台管理接口(Intelligent Platform Management Interface)的缩写，是管理基于 Intel 结构的企业系统中所使用的外围设备采用的一种工业标准；Libmodplug 是用于播放 mod 类音乐格式的开源函数库；ThinkVantage Access Connections 是一款网络管理软件；IBM WebSphere Portal 提供了一个组合应用程序或业务 mashup 框架，并且提供了一种基于 SOA 的解决方案；IBM OpenAdmin Tool (OAT) for Informix 是管理和分析 IBM Informix 数据库服务器的 Web 应用程序。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，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括 IBM 多个产品 IMM IPMI 默认账户漏洞、libmodplug 整数溢出漏洞（CNVD-2013-12222）、libmodplug 'abc_MIDI_drum()'堆缓冲区溢出漏洞、IBM ThinkVantage Access Connections 不安全库加载漏洞、IBM ThinkVantage Access Connections 不安全库加载漏洞、IBM 多个产品 IMM IPMI 明文密码敏感信息泄露漏洞、IBM WebSphere Portal 存在多个跨站脚本漏洞、IBM Informix Open Admin Tool 跨站脚本

漏洞等。其中，“IBM 多个产品 IMM IPMI 默认账户漏洞、libmodplug 整数溢出漏洞（CNVD-2013-12222）、libmodplug 'abc_MIDI_drum()' 堆缓冲区溢出漏洞、IBM ThinkVantage Access Connections 不安全库加载漏洞”的综合评级均为“高危”。厂商已发布了除“libmodplug 整数溢出漏洞(CNVD-2013-12222)、libmodplug 'abc_MIDI_drum()' 堆缓冲区溢出漏洞、IBM ThinkVantage Access Connections 不安全库加载漏洞”外，其余漏洞的修补程序。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-2013-12150>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12149>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12151>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12144>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12230>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12222>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12250>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12270>

3、WordPress 产品安全漏洞

WordPress 是一种使用 PHP 语言开发的博客平台,用户可以在支持 PHP 和 MySQL 数据库的服务器上架设自己的网志。本周,该产品的多个插件被披露存在多个安全漏洞。远程攻击者利用漏洞可获取敏感信息,注入任意 SQL 代码,执行 SQL 查询。

CNVD 收录的相关漏洞包括: IBM iNotes ActiveX 整数溢出漏洞、WordPress 插件 All-in-One Event Calendar SQL 注入漏洞、WordPress 插件 All-in-One Event Calendar 脚本注入漏洞、WordPress 插件 HMS Testimonials 存在多个跨站脚本漏洞。其中,“WordPress 插件 All-in-One Event Calendar SQL 注入漏洞”的综合评级为“高危”。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-2013-12261>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12260>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12413>

4、Google Chrome 安全漏洞

Google Chrome 是一款 Web 浏览工具。本周,该产品被披露存在多个漏洞,攻击者利用漏洞可使应用程序崩溃,导致拒绝服务攻击。

CNVD收录的相关漏洞包括: Google Chrome 'WebVTTParser::createDocumentFragmentFromCueText()'拒绝服务漏洞。该漏洞的综合评级为“高危”。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-2013-12257>

5、OneHTTPD 拒绝服务漏洞

OneHTTPD 是一款 Web 服务器。本周, 该产品被披露存在一个拒绝服务漏洞。攻击者利用漏洞可发起拒绝服务攻击。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-2013-12228>

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-2013-12416	ISC BIND 9 SRTT 算法授权服务器选择安全漏洞	高	暂无
CNVD-2013-12411	The PI Interface for IEEE C37.1 内存损坏漏洞	高	请安装厂商已发布的最新版本或补丁: http://www.osisoft.com/
CNVD-2013-12417	SAP BusinessObjects 'Axis2'组件默认密码安全绕过漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息: https://service.sap.com/sap/support/notes/1432881
CNVD-2013-12430	LibRaw 缓冲区溢出漏洞	高	LibRaw 0.15.2 已修复此漏洞, 建议用户下载使用: http://www.libraw.org/
CNVD-2013-12431	PHPFox '[gender]' SQL 注入漏洞	高	用户可联系供应商获得补丁信息: http://www.phpfox.com/
CNVD-2013-12250	libmodplug 'abc_MIDI_drum()'堆缓冲区溢出漏洞	高	暂无
CNVD-2013-12227	Sami FTP Server 'MKD'命令缓冲区溢出漏洞	高	暂无
CNVD-2013-12158	Schweitzer Engineering Laboratories 多个设备远程拒绝服务漏洞	高	用户可联系厂商获得相应的升级固件以修复该漏洞: https://www.selinc.com/
CNVD-2013-12225	vbBux 和 vbPlaza 'vbplaza_lottery_history'参数 SQL 注入漏洞	高	暂无

CNVD-2013-12217	Kwok Information Server 存在未明 SQL 注入漏洞	高	用户可联系供应商获得补丁信息： http://www.kwoksys.com/wiki/index.php?title=Release_Notes
-----------------	---------------------------------------	---	--

表 3 部分高危漏洞列表

小结：本周，微软发布了 2013 年 8 月份的月度例行安全公告，共含 8 项更新，修复了 Microsoft Windows、Internet Explorer 和 Microsoft Server 软件中存在的 23 个安全漏洞。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。

本周，Google Chrome、WordPress 多款插件以及 IBM 多款产品被披露存在多个漏洞。远程攻击者利用漏洞可获得敏感信息，执行未授权的访问，发起拒绝服务攻击。此外，OneHTTPD 服务器被披露存在一个零日漏洞，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、Siemens 发布升级程序，修补 COMOS 产品安全漏洞

Siemens COMOS 是西门子开发的工厂管理软件。本周，Siemens 发布升级程序，修补 COMOS 产品存在的漏洞，本地攻击者利用特制的客户端应用，通过 COMOS 图形用户接口提升权限。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/38163>

本周要闻速递

1. 苹果 App Store 存在漏洞

8 月 18 日据美国科技资讯网 CNET 报道，研究者再次让一款恶意程序顺利通过了苹果 App Store 的应用程序审批过程，这证明了苹果应用商店仍然存在漏洞。麻省理工学院著名科技杂志 Technology Review 发布的一份研究报告称，来自佐治亚理工学院的一组研究人员开发了一款特别的应用程序，该应用程序被伪装成了一款新闻阅读软件，在该软件被下载安装到手机后，它能够重新编码变成一款恶意程序。实验证明，苹果的安全审核程序无法识别这种伪装的恶意程序。一旦通过远程配置成功，该软件就能够执行各种任务，如发送短信、电子邮件、在 Twitter 上发布消息、拍照、拨打电话，甚至重启系统。

参考链接: <http://tech.qq.com/a/20130818/004021.htm>

2. 苹果发布 iTunes 11.0.5 修复云计算服务漏洞

北京时间 8 月 17 日上午消息, 苹果公司周五发布了 iTunes 的 11.0.5 版本。上月, 苹果公司曾发布了 iTunes 的一次升级, 修复了同步和 iTunes 商店登录的问题。此次升级修复了 iTunes 云计算服务的漏洞。由于这一漏洞, 一些用户可能会下载或播放未知的媒体内容。目前用户可以通过 Mac App Store 应用商店、苹果软件升级服务, 或直接从苹果公司的软件下载页面获得这一升级。64 位 Windows 版本也已同步发布。

参考链接: <http://tech.sina.com.cn/mobile/n/apple/2013-08-17/09538648096.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路安全技术协调组织, 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