

信息安全漏洞周报

2014 年 8 月 25 日-2014 年 8 月 31 日

2014 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 137 个，其中高危漏洞 29 个、中危漏洞 87 个、低危漏洞 21 个。上述漏洞中，可利用来实施远程攻击的漏洞有 114 个。本周收录的漏洞中，已有 90 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“Joomla! Spider Video Player 扩展'theme' SQL 注入漏洞”、“MyBB '/showthread.php' 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 6 家成员单位及个人报送了本周收录的全部 137 个漏洞。报送情况如表 1 所示。其中，奇虎 360、安天实验室、恒安嘉新、天融信、启明星辰等单位报送数量较多。此外，CNCERT 各分中心、习科网络安全及白帽子向 CNVD 提交了 345 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
奇虎 360	324	324
安天实验室	171	0
恒安嘉新	116	0
天融信	96	0
启明星辰	93	0
绿盟科技	35	0

习科网络安全	1	1
CNCERT 山西分中心	6	6
CNCERT 陕西分中心	5	5
CNCERT 宁夏分中心	1	1
CNCERT 河北分中心	1	1
CNCERT 吉林分中心	1	1
个人	6	6
报送总计	856	345
录入总计	137（去重）	345

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 WordPress、IBM、Google 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	WordPress	17	12%
2	IBM	11	8%
3	Google	10	7%
4	Drupal	5	4%
5	PHP	5	4%
6	HP	4	3%
7	MyBB	4	3%
8	Django	4	3%
9	Cisco	2	1%
10	其他	75	55%

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 137 个漏洞。其中应用程序漏洞 90 个，WEB 应用漏洞 36 个，网络设备漏洞 5 个，操作系统漏洞 4 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	90
WEB 应用漏洞	36
网络设备漏洞	5
操作系统漏洞	4

安全产品漏洞	2
--------	---

表 3 漏洞按影响类型统计表

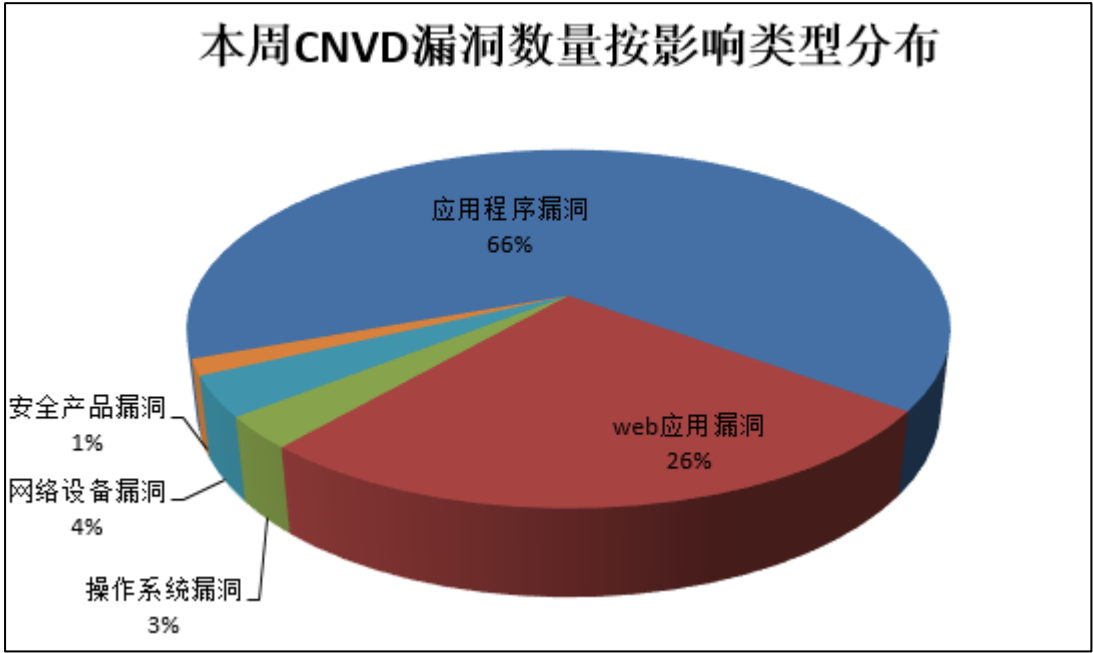


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 3 个电信行业漏洞，4 个移动互联网漏洞，9 个工控行业漏洞（如下图表所示）。其中，“DISCUZ EDITPOST 文件 SQL 注入漏洞、Android for MS M Project 本地安全绕过漏洞（CNVD-2014-05235、CNVD-2014-05239、CNVD-2014-05241）、Invensys Wonderware Information Server SQL 注入漏洞（CNVD-2014-05273）、I nvensys Wonderware Information Server 跨站脚本漏洞（CNVD-2014-05271）”的综合评级均为“高危”。相关厂商已经发布了上述漏洞的修补程序。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2014-05216	DISCUZ EDITPOST 文件 SQL 注入漏洞	高	是
电信	CNVD-2014-05220	Cisco IOS XR Software 数据包解析拒绝服务漏洞	中	是
电信	CNVD-2014-05297	IBM Maximo Asset Management 多个产品未授权操作漏洞	低	是
移动互联网	CNVD-2014-05235	Android for MSM Project 本地安全绕过漏洞（CNVD-2014-05235）	高	是
移动互联网	CNVD-2014-05228	Pebble Smartwatch for Android/iOS 拒绝服务漏洞	高	否
移动互联网	CNVD-2014-05239	Android for MSM Project 本地安全绕过漏洞（CNVD-2014-05239）	高	是
移动互联网	CNVD-2014-05241	Android for MSM Project 本地安全绕	高	是

		过漏洞（CNVD-2014-05241）		
工控系统	CNVD-2014-05215	WAGO I/O System CODESYS WebVisu 密码信息泄露漏洞	中	否
工控系统	CNVD-2014-05274	Invensys Wonderware Information Server 弱加密漏洞	低	是
工控系统	CNVD-2014-05273	Invensys Wonderware Information Server SQL 注入漏洞（CNVD-2014-05273）	高	是
工控系统	CNVD-2014-05272	Invensys Wonderware Information Server 信息泄露漏洞（CNVD-2014-05272）	低	是
工控系统	CNVD-2014-05271	Invensys Wonderware Information Server 跨站脚本漏洞（CNVD-2014-05271）	高	是
工控系统	CNVD-2014-05286	ePAQ-9410 Substation Gateway Serial-Connected 设备本地拒绝服务漏洞	低	否
工控系统	CNVD-2014-05291	ePAQ-9410 Substation Gateway Serial-Connected Devices 本地拒绝服务漏洞	中	是
工控系统	CNVD-2014-05295	Microsys PROMOTIC 存在未明漏洞	中	否
工控系统	CNVD-2014-05298	Cogent DataHub 远程目录遍历漏洞	中	否

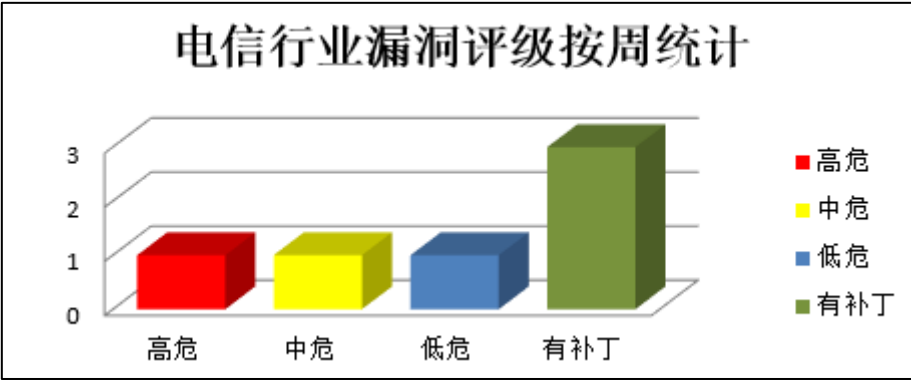


图 1 电信行业漏洞统计

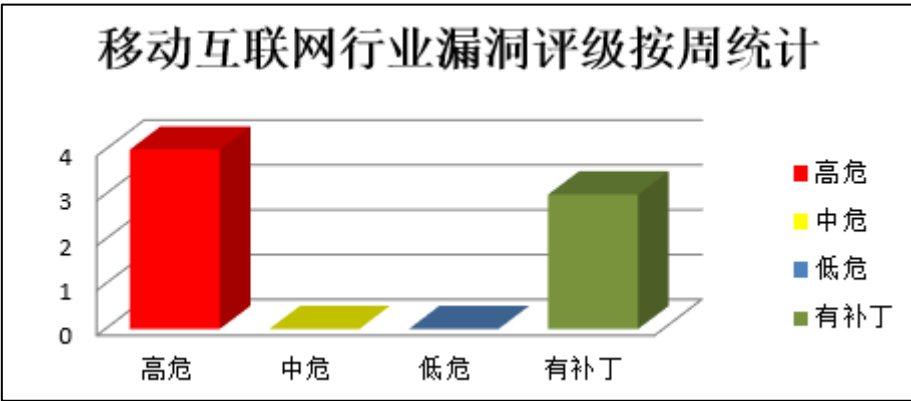


图 2 移动互联网行业漏洞统计

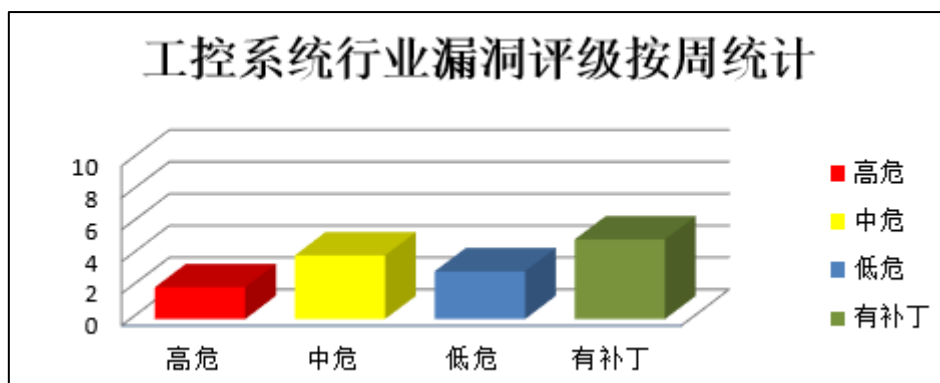


图 3 工控行业漏洞统计

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、IBM 产品安全漏洞

IBM Power 740 是一款灵活的单插槽或双插槽服务器；IBM Emptoris Contract Management 软件是可实现合同生命周期自动化的解决方案；IBM Emptoris Spend Analysis 是解决方案支持企业对来自分散而且各异的系统的支出数据进行整合、清理和分类；IBM Emptoris 是采购寻源解决方案；IBM Flex System Manager 是一个完全集成的平台，可从单一控制台简化硬件、网络和存储的管理；IBM Security AppScan Enterprise 用于提供 Web 应用程序漏洞测试和报告，以扩展安全性测试；PowerVC 是 IBM 基本虚拟化管理的解决方案。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞获取敏感信息、进行跨站脚本攻击或提升权限。

CNVD 收录的相关漏洞包括：IBM Emptoris Contract Management 跨站脚本漏洞、IBM Emptoris Contract Management SQL 注入漏洞、IBM Emptoris Sourcing Portfolio 和 Emptoris Spend Analysis 框架注入漏洞、IBM Emptoris Sourcing Portfolio 存在未明跨站脚本漏洞、IBM Power 7 Systems 存在未明本地权限提升漏洞、IBM Security App Scan Enterprise 信息泄露漏洞、IBM Flex System Manager 弱加密漏洞、IBM PowerVC 'api-paste.ini' 存在多个不安全文件权限漏洞。目前，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-2014-05236>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05233>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05232>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05230>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05211>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05307>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05285>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05299>

2、Google 产品安全漏洞

Google Chrome 是一款流行的 WEB 浏览器。本周，上述产品被披露存在远程代码执行和信息泄露漏洞，攻击者可利用漏洞执行任意脚本代码或获取敏感信息。

CNVD 收录的相关漏洞包括：Google Chrome 内存错误引用远程代码执行漏洞（CNVD-2014-05283、CNVD-2014-05248、CNVD-2014-05249）、Google Chrome 远程代码执行漏洞（CNVD-2014-05251、CNVD-2014-05252）、Google Chrome 存在未明漏洞（CNVD-2014-05254）、Google Chrome 信息泄露漏洞（CNVD-2014-05250、CNVD-2014-05253）。其中，除“Google Chrome 信息泄露漏洞（CNVD-2014-05250、CNVD-2014-05253）”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-2014-05283>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05248>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05249>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05251>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05252>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05254>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05250>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05253>

3、PHP 产品安全漏洞

PHP 是广泛使用的通用目的脚本语言，用于 Web 开发，可嵌入到 HTML 中。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞获取敏感信息、执行任意脚本代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：PHP DNS TXT Record Handling 堆缓冲区溢出漏洞、PHP 'cdf_read_property_info()'函数不完全修复拒绝服务漏洞、PHP imagexxx 函数空字节注入漏洞、PHP 'printf()'函数越界内存破坏漏洞、PHP Pear '/tmp/'目录不安全临时文件创建漏洞。目前，厂商已经发布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-2014-05187>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05188>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05217>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05225>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05263>

4、Drupal 产品安全漏洞

Drupal 是一款开放源码的内容管理系统(CMS)。本周, 上述产品被披露存在跨站脚本和 HTML 注入漏洞, 攻击者可利用漏洞进行跨站攻击执行任意脚本代码。

CNVD 收录的相关漏洞包括: Drupal Social Stats 模块 HTML 注入漏洞、Drupal RedHen CRM 模块存储跨站脚本漏洞、Drupal Social Stats 模块存储跨站脚本漏洞、Drupal Site Banner 模块存储跨站脚本漏洞、Drupal Marketo MA 模块字段标题存储跨站脚本漏洞。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-2014-05206>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05183>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05182>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05181>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05180>

5、Aruba Networks ClearPass Policy Manager 命令注入漏洞

Aruba Networks ClearPass 是 Wi-Fi 网络和有线网络访问接入方案。本周, Aruba Networks ClearPass Policy Manager 被披露存在综合评级为“高危”的命令注入漏洞。攻击者可利用漏洞在当前登录用户的上下文中执行任意命令。目前, 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-2014-05262>

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-2014-05209	Apache OpenOfficeCalc 命令注入漏洞	高	用户可以联系供应商获得补丁信息: http://www.openoffice.org/security
CNVD-2014-05207	AR Web Content Manager (AWCM) 'search.php'搜索参数 SQL 注入漏洞	高	暂无
CNVD-2014-05200	HP Service Manager (SM)存在未明漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题, 请到厂商的主页下载: http://h20566.www2.hp.com/portal/site/hpsc/template.PAGE/public/kb/docDisplay/?docId=emr_na-c04388127&ac.admitted=1408932791924.876444892.199480143
CNVD-2014-05202	HP Service Manager (SM)任意代码执行漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题, 请到厂商的主页下载:

			http://h20566.www2.hp.com/portal/site/hpsc/template.PAGE/public/kb/docDisplay/?docId=emr_na-c04388127&ac.admitted=1408932791924.876444892.199480143
CNVD-2014-05197	Lua 'ldo.c'远程代码执行漏洞	高	Lua 5.2.3 已经修复该漏洞，建议用户下载更新： http://www.lua.org/home.html
CNVD-2014-05301	SolarWinds Storage Manager 'AuthenticationFilter'远程代码执行漏洞	高	用户可以联系供应商获得补丁信息： http://www.solarwinds.com
CNVD-2014-05246	VTLS-Virtua 'InfoStation.cgi' SQL 注入漏洞	高	暂无
CNVD-2014-05257	Ruby dragonfly Gem 存在多个远程代码执行漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： http://markevans.github.com/dragonfly/
CNVD-2014-05288	EMC RSA Identity Management and Governance NovellIM 验证绕过漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： http://www.emc.com/
CNVD-2014-05258	Aruba Networks Web Management Portal 任意文件上传漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，IBM 多款产品被披露存在多个漏洞，允许攻击者利用漏洞获取敏感信息、进行跨站脚本攻击或提升权限。此外，Google、PHP、Drupal 多款产品被披露存在多个漏洞，攻击者利用漏洞获取敏感信息、进行跨站脚本攻击、执行任意脚本代码或发起拒绝服务攻击。另外，Aruba Networks ClearPass 被披露存在一个高危零日漏洞。攻击者可以利用漏洞在当前登录用户的上下文中执行任意命令。建议相关用户应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、Cisco 修补 IOS XR 产品漏洞

Cisco IOS XR 是 Cisco IOS 软件家族的一员，使用基于微内核分配操作系统架构。

本周，Cisco 修补了上述产品存在的数据包解析拒绝服务漏洞，避免攻击者利用此漏洞导致受影响的设备上 NP 芯片和线卡锁定并重新加载，拒绝服务合法用户。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网络安全事件。

补丁下载链接：<http://www.cnvd.org.cn/patchInfo/show/49362>



本周要闻速递

1. Netcore 路由器存在后门，任何人可远程登陆

根据研究人员表示，由中国生产商生产的一系列路由器含有一个严重漏洞，黑客可通过该漏洞监视用户的互联网流量。研究人员在文章中具体写道，Netcore 系列路由器中存在一个后门，进入后门的口令被“硬加密”(hardcoded)写入到设备的固件中，而且所有的口令似乎都一样。攻击者可以轻易的利用这个口令登录路由器，而且用户无法更改或禁用这个后门。

参考链接：<http://www.freebuf.com/news/41940.html>

2. 服务器系统被发现 KVM 漏洞

近日，部分知名厂商的服务器系统被发现存在 KVM 漏洞，该漏洞理论上可能会被黑客利用以获取对受害用户设备系统的控制权限。然而，仍有厂商拒绝公开承认其多款产品存在该漏洞。由于该漏洞可能会导致黑客入侵后端的主机，致使企业的核心信息资产被窃取或是破坏。加之这些厂商的服务器在国内被广泛应用，因此使用这些厂商的服务器无疑会给相关组织带来极大的风险。

参考链接：<http://soft.yesky.com/security/154/38806654.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