

## 信息安全漏洞周报

2014 年 12 月 01 日-2014 年 12 月 07 日

2014 年第 49 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 142 个，其中高危漏洞 53 个、中危漏洞 81 个、低危漏洞 8 个。上述漏洞中，可利用来实施远程攻击的漏洞有 129 个。本周收录的漏洞中，已有 105 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“多个 ManageEngine 产品任意文件下载漏洞（CNVD-2014-08684）”、“ZTE ZXDSL 831CII 默认配置漏洞”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、企业用户及个人报送了本周收录的全部 142 个漏洞。报送情况如表 1 所示。其中，安天实验室、恒安嘉新、奇虎 360、启明星辰、天融信等单位报送数量较多。此外，CNCERT 各分中心、北京安信天行科技有限公司、北京国舜科技有限公司及白帽子向 CNVD 提交了 142 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   | 132    | 0      |
| 恒安嘉新    | 120    | 0      |
| 奇虎 360  | 115    | 115    |
| 启明星辰    | 88     | 0      |
| 天融信     | 88     | 0      |
| 绿盟科技    | 73     | 0      |

|              |         |     |
|--------------|---------|-----|
| 北京安信天行科技有限公司 | 7       | 7   |
| 北京国舜科技有限公司   | 1       | 1   |
| CNCERT 福建分中心 | 5       | 5   |
| CNCERT 山西分中心 | 1       | 1   |
| CNCERT 宁夏分中心 | 1       | 1   |
| CNCERT 河南分中心 | 1       | 1   |
| 个人           | 11      | 11  |
| 报送总计         | 643     | 142 |
| 录入总计         | 142（去重） | 142 |

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Mozilla、MantisBT、IBM 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  | Mozilla   | 9    | 6%   |
| 2  | MantisBT  | 8    | 6%   |
| 3  | IBM       | 7    | 5%   |
| 4  | ownCloud  | 7    | 5%   |
| 5  | WordPress | 6    | 4%   |
| 6  | Drupal    | 5    | 4%   |
| 7  | D-Link    | 5    | 4%   |
| 8  | WebKit    | 4    | 2%   |
| 9  | ZTE       | 2    | 1%   |
| 10 | 其他        | 89   | 63%  |

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 142 个漏洞。其中应用程序漏洞 91 个，WEB 应用漏洞 29 个，网络设备漏洞 18 个，操作系统漏洞 2 个，安全产品漏洞 1 个，数据库漏洞 1 个。

| 漏洞影响对象类型 | 漏洞数量 |
|----------|------|
| 应用程序漏洞   | 91   |
| WEB 应用漏洞 | 29   |
| 网络设备漏洞   | 18   |
| 操作系统漏洞   | 2    |
| 安全产品漏洞   | 1    |
| 数据库漏洞    | 1    |

表 3 漏洞按影响类型统计表

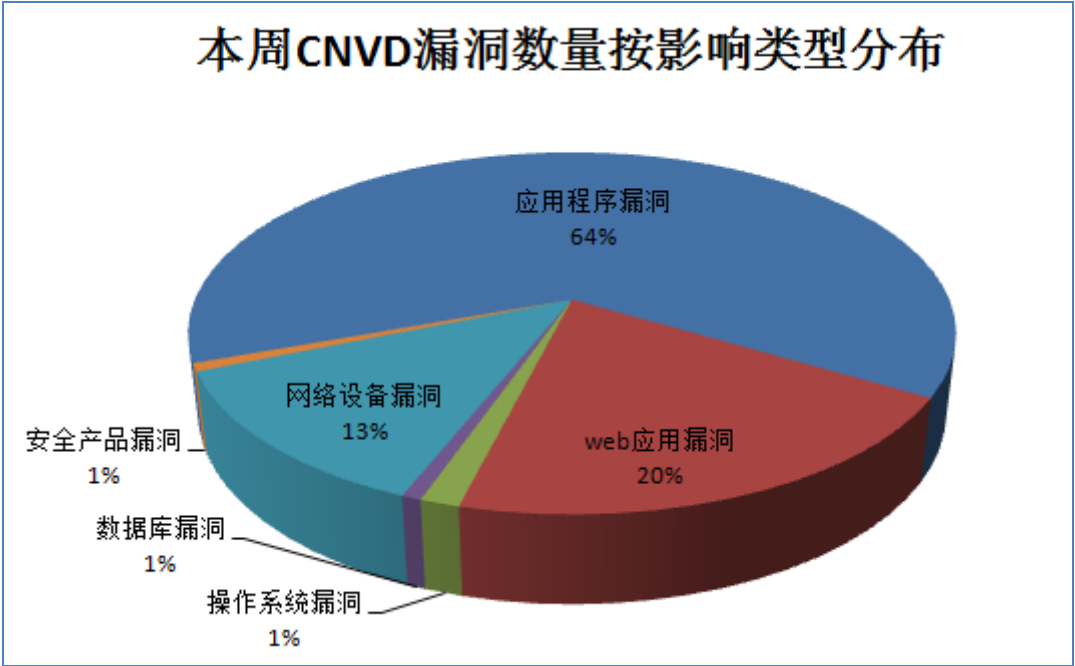


图 1 本周漏洞按影响类型分布

### 本周行业漏洞信息

本周，CNVD 收录了 12 个电信行业漏洞，1 个移动互联网漏洞，4 个工控系统行业漏洞（如下图表所示）。其中，“Siemens SIMATIC WinCC/PCS 7 目录遍历漏洞、Siemens SIMATIC WinCC/PCS 7 任意代码执行漏洞”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-2014-08588 | Oracle Database Server 存在未明漏洞           | 中    | 是     |
| 电信 | CNVD-2014-08617 | 多个 IBM QRadar 产品会话劫持漏洞                  | 中    | 是     |
| 电信 | CNVD-2014-08616 | 多个 IBM QRadar 产品跨站请求伪造漏洞                | 中    | 是     |
| 电信 | CNVD-2014-08627 | D-Link DAP-1360 'index.cgi'存在多个跨站请求伪造漏洞 | 低    | 否     |
| 电信 | CNVD-2014-08742 | D-Link DAP-1360 跨站脚本漏洞                  | 中    | 否     |

|       |                 |                                                              |   |   |
|-------|-----------------|--------------------------------------------------------------|---|---|
| 电信    | CNVD-2014-08626 | D-Link DAP-1360 'index.cgi' HTML 注入漏洞                        | 中 | 否 |
| 电信    | CNVD-2014-08645 | SEIL Series Routers 远程拒绝服务漏洞 (CNVD-2014-08645)               | 中 | 是 |
| 电信    | CNVD-2014-08651 | SEIL Series Routers 存在多个拒绝服务漏洞                               | 中 | 是 |
| 电信    | CNVD-2014-08690 | OMAP Mobile Processors Syslink Driver 存在多个漏洞                 | 中 | 是 |
| 电信    | CNVD-2014-08685 | Alcatel-Lucent 1830 Photonic Service Switch 'pop.html'跨站脚本漏洞 | 中 | 否 |
| 电信    | CNVD-2014-08743 | Prolink PRN2001 Router 存在多个漏洞                                | 高 | 否 |
| 电信    | CNVD-2014-08741 | D-Link DAP-1360 跨站请求伪造漏洞                                     | 低 | 否 |
| 移动互联网 | CNVD-2014-08688 | WhatsApp 拒绝服务漏洞                                              | 中 | 否 |
| 工控系统  | CNVD-2014-08594 | Siemens SIMATIC WinCC/PCS 7 目录遍历漏洞                           | 高 | 是 |
| 工控系统  | CNVD-2014-08593 | Siemens SIMATIC WinCC/PCS 7 任意代码执行漏洞                         | 高 | 是 |
| 工控系统  | CNVD-2014-08646 | Yokogawa FAST/TOOLS XML 外部实体注入漏洞                             | 低 | 是 |
| 工控系统  | CNVD-2014-08734 | 多个 Emerson Process Management RTUs 安全绕过漏洞                    | 中 | 是 |

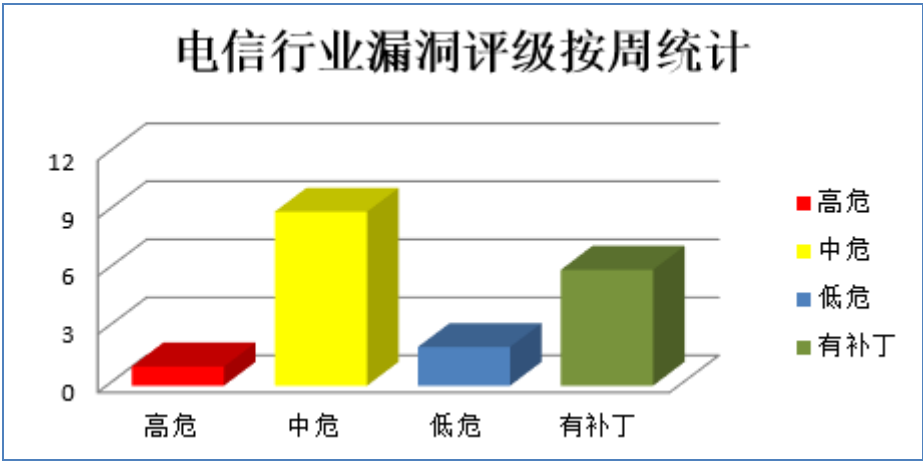


图 1 电信行业漏洞统计

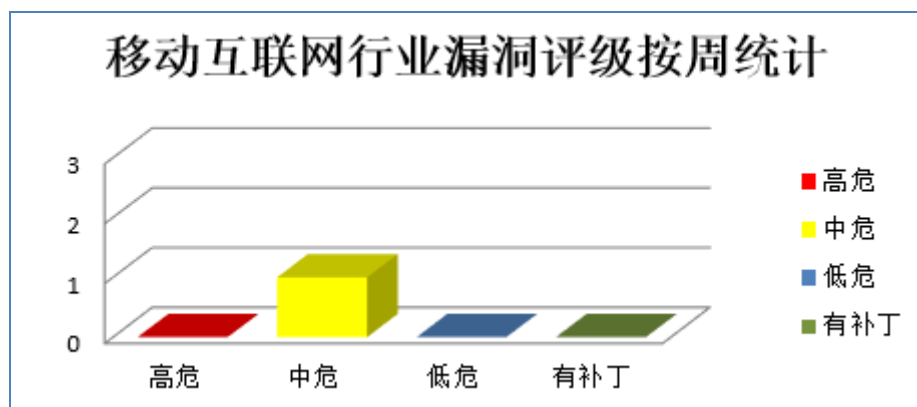


图 2 移动互联网行业漏洞统计

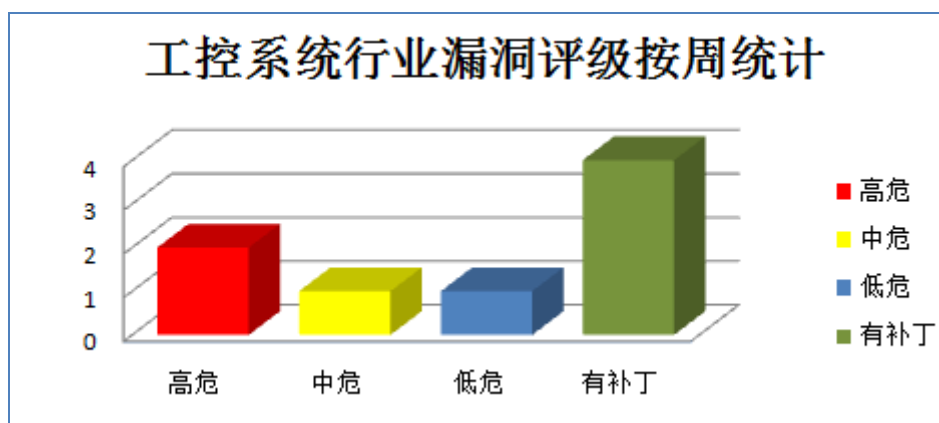


图 3 工控系统行业漏洞统计

## 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、Mozilla 产品安全漏洞

Mozilla Firefox/Thunderbird 是 Mozilla 所发布的 WEB 浏览器/邮件客户端。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞获取敏感信息、发起拒绝服务或执行任意代码。

CNVD 收录的相关漏洞包括：Mozilla Firefox 信息泄露漏洞（CNVD-2014-08709）、Mozilla Firefox/Thunderbird 内存错误引用内存破坏漏洞（CNVD-2014-08698）、Mozilla Firefox/Thunderbird 拒绝服务漏洞（CNVD-2014-08700）、Mozilla Firefox/Thunderbird 存在远程漏洞（CNVD-2014-08701）、Mozilla Firefox/Thunderbird 存在多个内存破坏漏洞（CNVD-2014-08696、CNVD-2014-08697）、Mozilla Firefox/Thunderbird 缓冲区溢出漏洞、Mozilla Firefox/Thunderbird 存在多个本地信息泄露漏洞。其中，除“Mozilla Firefox 信息泄露漏洞（CNVD-2014-08709）、Mozilla Firefox/Thunderbird 拒绝服务漏洞（CNVD-2014-08700）、Mozilla Firefox/Thunderbird 存在多个本地信息泄露漏洞”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-2014-08709>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08698>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08700>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08701>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08696>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08697>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08702>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08704>

## 2、MantisBT 产品安全漏洞

MantisBT 是一个基于 web 的流行 bug 跟踪系统。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞执行未授权操作、进行跨站脚本攻击或发起拒绝服务。

CNVD 收录的相关漏洞包括：MantisBT 'admin/upgrade\_unattended.php'安全绕过漏洞、MantisBT 'core/current\_user\_api.php' PHP 对象注入漏洞、MantisBT 'helper\_api.php' 跨站脚本漏洞、MantisBT 'copy\_field.php'存在多个跨站脚本漏洞、MantisBT 'projax\_api.php' HTML 注入漏洞、MantisBT 'string\_api.php'跨站脚本漏洞、MantisBT 'file\_download.php' HTML 注入漏洞、MantisBT Captcha System 拒绝服务漏洞。其中“MantisBT 'core/current\_user\_api.php' PHP 对象注入漏洞”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-2014-08629>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08630>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08631>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08632>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08633>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08635>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08647>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08599>

## 3、IBM 产品安全漏洞

IBM Systems Director 是易于使用的集成工具套件，为客户提供了灵活的系统管理功能，从而帮助实现最大限度的系统可用性并降低 IT 成本。IBM Tivoli Endpoint Manager 提供了统一、实时的可视化和实施方法来向所有端点部署和管理补丁。IBM Java 是所有 IBM 计算平台上使用的应用开发 Java 编程语言。IBM QRadar Risk Manager 是可监控网络拓扑、交换机、路由器、防火墙和入侵防御系统 (IPS) 的配置以降低风险并

提高合规性解决方案。IBM Security QRadar SIEM 是一套可对分散在整个网络中的数千个设备和应用中的日志源事件数据进行整合的解决方案。IBM Security QRadar Vulnerability Manager 会主动发现网络设备和应用的安全漏洞并划分其优先级，添加上下文并按优先顺序实施补救和缓解活动。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发起拒绝服务。

CNVD 收录的相关漏洞包括：IBM Systems Director 存在未明漏洞、IBM Tivoli Endpoint Manager Mobile Device Management 跨站脚本漏洞、IBM Java 认证管理系统私钥信息泄露漏洞、多个 IBM QRadar 产品跨站请求伪造漏洞、多个 IBM QRadar 产品会话劫持漏洞、IBM Security QRadar SIEM/QRadar Risk Manager 信息泄露漏洞（CNVD-2014-08589）、IBM Sterling Selling and Fulfillment Suite 拒绝服务漏洞。目前，厂商已经发布了修补程序。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-2014-08744>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08745>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08692>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08616>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08617>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08589>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08587>

#### 4、D-Link 产品安全漏洞

D-link IP camera DCS-2103 是一款 IP 监控解决方案的摄像机。D-Link DAP-1360 是一款无线路由器。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、进行跨站攻击或执行任意代码。

CNVD 收录的相关漏洞包括：D-link IP camera DCS-2103 with firmware 目录遍历漏洞、D-Link DAP-1360 跨站请求伪造漏洞、D-Link DAP-1360 跨站脚本漏洞、D-Link DAP-1360 'index.cgi' HTML 注入漏洞、D-Link DAP-1360 'index.cgi'存在多个跨站请求伪造漏洞。其中，“D-link IP camera DCS-2103 with firmware 目录遍历漏洞”厂商已经发布了该漏洞的修补程序。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-2014-08721>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08741>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08742>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08626>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08627>

#### 5、Cisco Integrated Management Controller 'map-nfs'命令本地权限提升漏洞

Cisco Integrated Management Controller 是思科集成管理控制器。本周，Cisco Integrated Management Controller 被披露存在综合评级为“高危”的本地权限提升漏洞。攻击者可利用漏洞提升权限。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-2014-08649>

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-2014-08592 | Libflac 'src/Libflac '/stream_decoder.c'堆缓冲区溢出漏洞                   | 高    | 用户可参考如下的安全公告获取补丁以修复该漏洞：<br><a href="https://git.xiph.org/?p=flac.git;a=commit;h=fcf0ba06ae12ccd7c67cee3c8d948df15f946b85">https://git.xiph.org/?p=flac.git;a=commit;h=fcf0ba06ae12ccd7c67cee3c8d948df15f946b85</a> |
| CNVD-2014-08591 | Libflac 'src/Libflac '/stream_decoder.c'堆栈缓冲区溢出漏洞                  | 高    | 用户可参考如下的安全公告获取补丁以修复该漏洞：<br><a href="https://git.xiph.org/?p=flac.git;a=commit;h=5b3033a2b355068c11fe637e14ac742d273f076e">https://git.xiph.org/?p=flac.git;a=commit;h=5b3033a2b355068c11fe637e14ac742d273f076e</a> |
| CNVD-2014-08595 | Aruba Networks ClearPass Policy Manager SQL 注入漏洞 (CNVD-2014-08595) | 高    | 用户可参考如下的安全公告获取补丁以修复该漏洞：<br><a href="http://xforce.iss.net/xforce/xfdb/98870">http://xforce.iss.net/xforce/xfdb/98870</a>                                                                                           |
| CNVD-2014-08596 | Mountall 安全限制绕过漏洞                                                  | 高    | 用户可参考如下的安全公告获取补丁以修复该漏洞：<br><a href="http://www.ubuntu.com/usn/USN-2411-1">http://www.ubuntu.com/usn/USN-2411-1</a>                                                                                                 |
| CNVD-2014-08585 | Drupal Protected Pages 模块密码保护绕过漏洞                                  | 高    | 用户可参考如下的安全公告获取补丁以修复该漏洞：<br><a href="https://www.drupal.org/node/2353451">https://www.drupal.org/node/2353451</a>                                                                                                   |
| CNVD-2014-08601 | Aruba Networks AirWave 任意命令执行漏洞                                    | 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：<br><a href="http://www.arubanetworks.com/">http://www.arubanetworks.com/</a>                                                                                                     |
| CNVD-2014-08603 | Enalean Tuleap 'unserialize()'函数远程 PHP 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：<br><a href="https://www.tuleap.org/about-tuleap/release-notes">https://www.tuleap.org/about-tuleap/release-notes</a>                                                             |
| CNVD-2014-08604 | Mutt 'mutt_substrdup()'堆缓冲区溢出漏洞                                    | 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：<br><a href="http://www.mutt.org/">http://www.mutt.org/</a>                                       |
| CNVD-2014-08605 | Centreon 'file_put_contents()'函数<br>远程命令执行漏洞 | 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：<br><a href="http://www.centreon.com/">http://www.centreon.com/</a> |
| CNVD-2014-08609 | phpMyRecipes 'dosearch.php' SQL<br>注入漏洞      | 高 | 暂无                                                                                                   |

表 3 部分高危漏洞列表

小结：本周，Mozilla 多款产品被批露存在多个安全漏洞，攻击者可利用漏洞获取敏感信息、发起拒绝服务或执行任意代码。此外，MantisBT、IBM、D-Link 多款产品被批露存在多个安全漏洞，允许攻击者利用漏洞获取敏感信息、执行任意代码、发起拒绝服务、执行未经授权操作或进行跨站脚本攻击。另外，Cisco Integrated Management Controller 被批露存在一个高危零日漏洞。攻击者可利用漏洞提升权限。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、Apache 修补 HTTP Server 产品漏洞

Apache HTTP Server 是 Apache 软件基金会的一个开放源码的网页服务器。

本周，Apache 修补了上述产品存在的未授权访问漏洞，避免攻击者利用漏洞执行未授权访问，获取敏感信息。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/52326>

## 本周要闻速递

### 1. 印度研究人员发现美国版微信 WhatsApp 漏洞

WhatsApp 是一款流行的即时通讯手机 APP，相当于美国版微信。两名年仅 17 岁的印度安全研究人员发现热门应用 WhatsApp 中存在漏洞，攻击者可以通过向受害者发送特定的消息使对方的应用崩溃。该漏洞已经在多个版本的安卓系统下测试成功，其中包括 Jellybean (Android 4.1)，Kitkat (Android 4.4) 及其以下的安卓版本。

参考链接：<http://www.freebuf.com/news/53490.html>

### 2. 伊朗黑客组织手术刀 (Operation Cleaver) 向全球发起攻击

安全公司 Cylance 爆料，伊朗黑客组织“手术刀 (Operation Cleaver)”正在全球范围内攻击航空、能源行业和国防领域。“手术刀”由伊朗政府赞助，在它的攻击目标中

目前有 10 个是美国重要基础设施。安全研究人员预测该黑客组织的攻击动机很可能是报复美国曾对伊朗造成损伤的震网病毒（Stuxnet）和其他黑客活动。

参考链接: <http://www.freebuf.com/news/53492.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](http://www.cert.org.cn)

邮箱: [vreport@cert.org.cn](mailto:vreport@cert.org.cn)

电话: 010-82990999