

## 信息安全漏洞周报

2015 年 01 月 05 日-2015 年 01 月 11 日

2015 年第 2 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 164 个，其中高危漏洞 44 个、中危漏洞 103 个、低危漏洞 17 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 108 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“php MyRecipes category 参数 SQL 注入漏洞”、“NotePad++缓冲区溢出漏洞”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、合作伙伴及个人报送了本周收录的全部 164 个漏洞。报送情况如表 1 所示。其中，奇虎 360、安天实验室、启明星辰、天融信、恒安嘉新等单位报送数量较多。此外，CNCERT 各分中心、北京国舜科技有限公司、High-Tech Bridge Security Research Lab 及白帽子向 CNVD 提交了 1029 个原创漏洞(注：奇虎 360 提交漏洞包含其“库带计划”中部分存量漏洞)。

| 报送单位或个人 | 漏洞报送数量 | 原创漏洞数量 |
|---------|--------|--------|
| 奇虎 360  | 1019   | 1019   |
| 安天实验室   | 141    | 0      |
| 启明星辰    | 110    | 0      |
| 天融信     | 107    | 0      |
| 恒安嘉新    | 78     | 0      |

|                                           |         |      |
|-------------------------------------------|---------|------|
| 绿盟科技                                      | 8       | 0    |
| 东软                                        | 2       | 0    |
| High-Tech Bridge<br>Security Research Lab | 1       | 1    |
| 北京国舜科技有限公<br>司                            | 1       | 1    |
| CNCERT 福建分中心                              | 5       | 5    |
| 个人                                        | 3       | 3    |
| 报送总计                                      | 1475    | 1029 |
| 录入总计                                      | 164（去重） | 1029 |

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、Facebook、VideoLAN 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 | 22   | 13%  |
| 2  | Facebook  | 6    | 4%   |
| 3  | VideoLAN  | 6    | 4%   |
| 4  | Google    | 5    | 3%   |
| 5  | EMC       | 5    | 3%   |
| 6  | Huawei    | 5    | 3%   |
| 7  | IBM       | 3    | 2%   |
| 8  | Apache    | 3    | 2%   |
| 9  | AdaptCMS  | 3    | 2%   |
| 10 | 其他        | 106  | 64%  |

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 164 个漏洞。其中应用程序漏洞 94 个，WEB 应用漏洞 55 个，网络设备漏洞 9 个，安全产品漏洞 4 个，操作系统漏洞 2 个。

| 漏洞影响对象类型 | 漏洞数量 |
|----------|------|
| 应用程序漏洞   | 94   |

|          |    |
|----------|----|
| WEB 应用漏洞 | 55 |
| 网络设备漏洞   | 9  |
| 安全产品漏洞   | 4  |
| 操作系统漏洞   | 2  |

表 3 漏洞按影响类型统计表

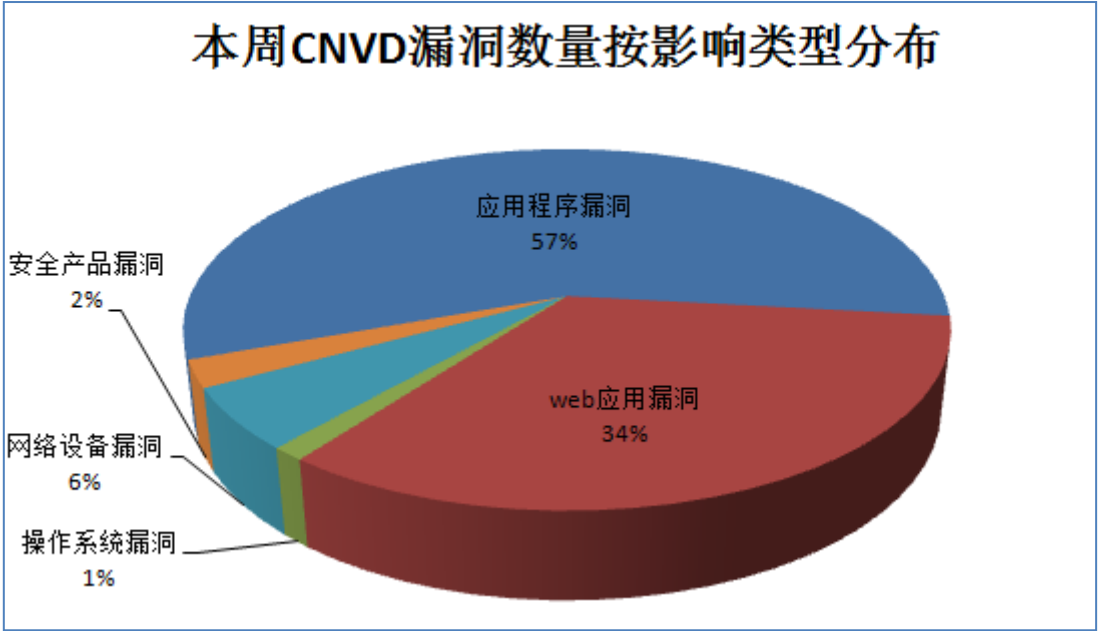


图 1 本周漏洞按影响类型分布

### 本周行业漏洞信息

本周，CNVD 收录了 3 个电信行业漏洞， 1 个移动互联网行业漏洞（如下图表所示）。

| 行业    | 漏洞编号            | 漏洞标题                                                     | 危险等级 | 是否有补丁 |
|-------|-----------------|----------------------------------------------------------|------|-------|
| 电信    | CNVD-2015-00033 | IBM WebSphere Service Registry and Repository 预期访问限制绕过漏洞 | 低    | 是     |
| 电信    | CNVD-2015-00188 | TP-Link TL-WR840N 'Import Configuration'选项跨站请求伪造漏洞       | 中    | 是     |
| 电信    | CNVD-2015-00187 | Brother MFC-J4410DW 打印机'url'参数存在多个跨站脚本漏洞                 | 中    | 是     |
| 移动互联网 | CNVD-2015-00036 | WhatsApp Non-Printable 字符串处理拒绝服务漏洞                       | 中    | 否     |

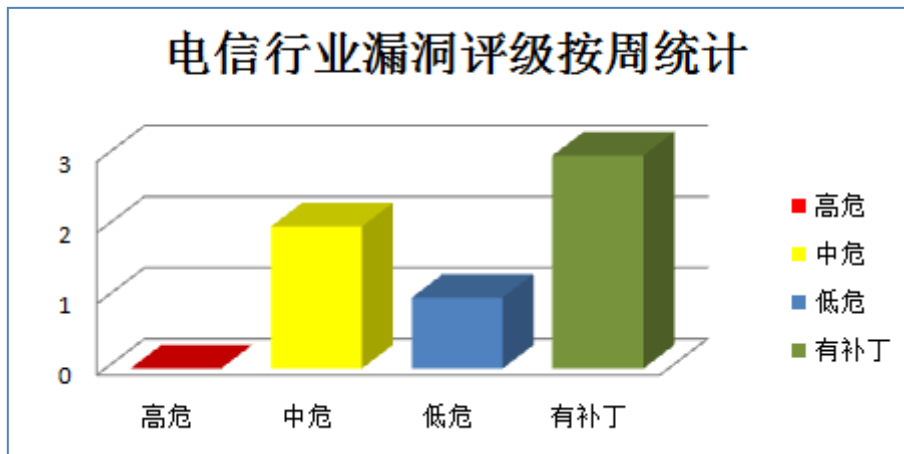


图 1 电信行业漏洞统计

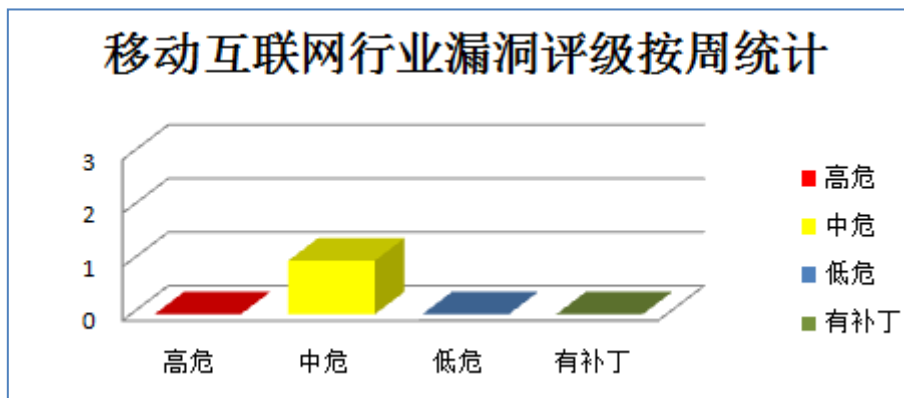


图 2 移动互联网行业漏洞统计

## 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、Google 产品安全漏洞

Google Chrome 是由 Google 开发的一款设计简单、高效的 Web 浏览工具。本周，上述产品被披露存在拒绝服务、整数溢出和内存错误引用漏洞，攻击者可利用漏洞发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Google Chrome 拒绝服务漏洞（CNVD-2015-00023、CNVD-2015-00022、CNVD-2015-00077）、Google Chrome 整数溢出漏洞（CNVD-2015-00062）、Google Chrome 内存错误引用漏洞（CNVD-2015-00063）。上述漏洞的综合评级均为“高危”。目前，厂商尚未发布上述漏洞的修补程序。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-2015-00023>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00022>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00077>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00062>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00063>

## 2、Huawei 产品安全漏洞

HUAWEI MobiConnect 是一个华为开发的软件。Huawei eSpace Desktop 是华为公司开发的统一通信 PC 客户端。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：HUAWEI MobiConnect 存在多个漏洞、Huawei eSpace Desktop V100R001C03 拒绝服务漏洞（CNVD-2015-00027、CNVD-2015-00029、CNVD-2015-00030）、Huawei eSpace Desktop V200R003C00 存在多个不可信搜索路径漏洞。其中“HUAWEI MobiConnect 存在多个漏洞”的综合评级为“高危”。目前，除“HUAWEI MobiConnect 存在多个漏洞”外，厂商已经发布了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-2015-00129>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00027>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00029>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00030>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00028>

## 3、EMC 产品安全漏洞

EMC Documentum Web Development Kit (WDK)是 Web 开发工具包。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任意代码、执行未授权操作或进行跨站攻击。

CNVD 收录的相关漏洞包括：EMC Documentum Web Development Kit (WDK)存在未明漏洞、EMC Documentum Web Development Kit (WDK)存在未明框架注入漏洞、EMC Documentum Web Development Kit (WDK)存在多个跨站脚本漏洞、EMC Documentum Web Development Kit (WDK)URL 重定向漏洞、EMC Documentum Web Development Kit (WDK)跨站请求伪造漏洞。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-2015-00090>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00091>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00092>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00093>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00094>

## 4、VideoLAN 产品安全漏洞

VideoLAN VLC media player 是 VideoLAN 计划的多媒体播放器。本周，上述产品被披露存在缓冲区溢出和拒绝服务漏洞，攻击者可利用漏洞执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：VideoLAN VLC media player 缓冲区溢出漏洞（CNVD-2015-00048、CNVD-2015-00045、CNVD-2015-00047）、VideoLAN VLC media player 拒绝服务漏洞（CNVD-2015-00046）、VideoLAN VLC media player 堆缓冲区溢出漏洞、VideoLAN VLC Media Player 栈缓冲区溢出漏洞。其中，除“VideoLAN VLC media player 拒绝服务漏洞（CNVD-2015-00046）”外，其余漏洞的综合评级均为“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-2015-00048>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00045>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00047>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00046>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00043>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00044>

## 5、CTS Projects & Software ClassAd SQL 注入漏洞

CTS Projects & Software ClassAd 是一个在线广告应用。本周，CTS Projects & Software ClassAd 被披露存在综合评级为“高危”的 SQL 注入漏洞。攻击者可以利用此漏洞提交特制的 SQL 查询，操作或获取数据库数据。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-2015-00130>

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-2015-00031 | LibreSSL 双重释放漏洞                         | 高    | 用户可参考如下供应商提供的安全公告获得补丁信息：<br><a href="https://github.com/robertbachmann/openbsd-libssl/commit/62a110d447bb8c16a4c69629e28a42e8c39fd7e0">https://github.com/robertbachmann/openbsd-libssl/commit/62a110d447bb8c16a4c69629e28a42e8c39fd7e0</a> |
| CNVD-2015-00024 | Telerik UI for ASP.NET AJAX Q3 绝对路径遍历漏洞 | 高    | 用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞：<br><a href="http://itq.nl/arbitrary-file-write-in-telerik-ui-for-asp-net-ajax/">http://itq.nl/arbitrary-file-write-in-telerik-ui-for-asp-net-ajax/</a>                                                          |
| CNVD-2015-00052 | Facebook HipHop Virtual Machine 整数溢出漏洞  | 高    | 用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞：                                                                                                                                                                                                                 |

|                 |                                            |   |                                                                                                                                                                                                                                                                                        |
|-----------------|--------------------------------------------|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 |                                            |   | <a href="https://github.com/facebook/hhvm/commit/1f91e076a585118495b976a413c1df40f6fd3d41">https://github.com/facebook/hhvm/commit/1f91e076a585118495b976a413c1df40f6fd3d41</a>                                                                                                        |
| CNVD-2015-00049 | Facebook HipHop Virtual Machine CRLF 注入漏洞  | 高 | 用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞：<br><a href="https://github.com/facebook/hhvm/commit/506a44194a9016406c752ad8e010c01aeffc18cc">https://github.com/facebook/hhvm/commit/506a44194a9016406c752ad8e010c01aeffc18cc</a>                                                                         |
| CNVD-2015-00058 | Redmine 插件 redmine_git_hosting 任意命令执行漏洞    | 高 | 用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞：<br><a href="http://www.sec-1.com/blog/2013/redmine-git-hosting-plugin-remote-command-execution">http://www.sec-1.com/blog/2013/redmine-git-hosting-plugin-remote-command-execution</a>                                                                     |
| CNVD-2015-00065 | SweetRice CMS 存在多个 SQL 注入漏洞                | 高 | 用户可联系供应商获得补丁信息：<br><a href="https://www.htbridge.com/advisory/HTB22667">https://www.htbridge.com/advisory/HTB22667</a>                                                                                                                                                                 |
| CNVD-2015-00114 | AjaXplorer 'save_zoho.php'任意文件上传漏洞         | 高 | 用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞：<br><a href="https://pyd.io/">https://pyd.io/</a>                                                                                                                                                                                                           |
| CNVD-2015-00118 | Sonatype Nexus OSS and Pro 目录遍历漏洞          | 高 | 用户可联系供应商获得补丁信息：<br><a href="http://www.sonatype.org/advisories/archive/2014-12-23-Nexus/">http://www.sonatype.org/advisories/archive/2014-12-23-Nexus/</a>                                                                                                                             |
| CNVD-2015-00124 | PHP Address Book SQL 注入漏洞（CNVD-2015-00124） | 高 | 暂无                                                                                                                                                                                                                                                                                     |
| CNVD-2015-00140 | VDG Security SENSE 存在多个缓冲区溢出漏洞             | 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://packetstormsecurity.com/files/129656/VDG-Security-SENSE-2.3.13-File-Disclosure-Bypass-Buffer-Overflow.html">http://packetstormsecurity.com/files/129656/VDG-Security-SENSE-2.3.13-File-Disclosure-Bypass-Buffer-Overflow.html</a> |

表 3 部分高危漏洞列表

小结：本周，Google 产品被批露存在拒绝服务、整数溢出和内存错误引用漏洞，攻击者可利用漏洞发起拒绝服务攻击。Huawei、EMC、VideoLAN 多款产品被批露存在多个安全漏洞，允许攻击者利用漏洞执行未经授权操作、执行任意代码、进行跨站攻击或发起拒绝服务攻击。此外，CTS Projects & Software ClassAd 被披露存在一个高危零日漏洞。攻击者可以利用此漏洞提交特制的 SQL 查询，操作或获取数据库数据。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。



CNVD 整理和发布以下重要安全修补信息。

## 1、Linux 修补 Kernel 产品漏洞

Linux Kernel 是 Linux 操作系统的内核。

本周，Linux 修补了上述产品存在的内存破坏漏洞，避免攻击者利用漏洞导致内核崩溃，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/53686>

## 本周要闻速递

### 1. 华硕路由器曝远程命令执行漏洞

安全研究员 Joshua Drake 在几个华硕路由器中的固件里发现了一个严重的漏洞，该漏洞能够使得未经身份认证的攻击者在路由器中执行任意指令。根据专家所说，这个安全漏洞可能影响到目前华硕所有版本的路由器固件。Drake 在 Github 上面发布了一份报告，详细描述了该漏洞。受影响的路由器包括 RT-AC66U，RT-N66U，以及更多其他的型号。

参考链接：<http://www.freebuf.com/news/56074.html>

### 2. 知名论坛系统 vBulletin 常用 SEO 插件 VBSEO 存在严重安全漏洞

vBulletin 团队近日向他们所有客户发出警告，其插件 VBSEO 出现了严重安全漏洞。VBSEO 是一款应用于 vBulletin 且非常普及的第三方 seo 模块，糟糕的是 VBSEO 官方已经在去年停止更新此插件，也就是说没有人能为漏洞提供官方补丁。vBulletin 团队对这个漏洞进行了研究，预计其可能是一个不需要认证的远程 html 脚本注入漏洞，这完全可能会演变成一个远程命令执行漏洞。遗憾的是，我们还没有完全掌握其细节。不过可以肯定的是，这个漏洞是非常严重的，黑客可以利用它进行恶意软件挂马，发送垃圾邮件，或者直接拿下网站。

参考链接：<http://www.freebuf.com/news/56019.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