

## 信息安全漏洞周报

2015 年 08 月 10 日-2015 年 08 月 16 日

2015 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**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 130 个，其中高危漏洞 60 个、中危漏洞 59 个、低危漏洞 11 个。上述漏洞中，可利用来实施远程攻击的漏洞有 116 个。本周收录的漏洞中，已有 104 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。其中互联网上出现“Fiyo CMS SQL 注入漏洞”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 5 家成员单位、合作伙伴及个人报送了本周收录的全部 130 个漏洞。报送情况如表 1 所示。其中，奇虎、安天实验室、恒安嘉新、天融信等单位报送数量较多。此外，CNCERT 各分中心、北京国舜科技股份有限公司、乌云、漏洞盒子及白帽子向 CNVD 提交了 869 个以事件型漏洞为主的原创漏洞。

| 报送单位或个人 | 漏洞报送数量 | 原创漏洞数量 |
|---------|--------|--------|
| 奇虎      | 424    | 424    |
| 安天实验室   | 179    | 0      |
| 恒安嘉新    | 84     | 0      |
| 天融信     | 45     | 0      |
| 绿盟科技    | 37     | 0      |
| 乌云      | 396    | 396    |

|              |         |     |
|--------------|---------|-----|
| 漏洞盒子         | 28      | 28  |
| 北京国舜科技股份有限公司 | 1       | 1   |
| CNCERT 福建分中心 | 7       | 7   |
| CNCERT 江西分中心 | 5       | 5   |
| CNCERT 上海分中心 | 1       | 1   |
| 个人           | 7       | 7   |
| 报送总计         | 1214    | 869 |
| 录入总计         | 130（去重） | 869 |

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、General Electric Company、WordPress 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                | 24   | 18%  |
| 2  | General Electric Company | 12   | 10%  |
| 3  | WordPress                | 10   | 8%   |
| 4  | Adobe                    | 8    | 6%   |
| 5  | Mozilla                  | 7    | 5%   |
| 6  | Polycom                  | 5    | 4%   |
| 7  | Koha                     | 5    | 4%   |
| 8  | Linux                    | 5    | 4%   |
| 9  | McAfee                   | 3    | 2%   |
| 10 | 其他                       | 51   | 39%  |

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 130 个漏洞。其中应用程序漏洞 81 个，WEB 应用漏洞 21 个，操作系统漏洞 19 个，网络设备漏洞 4 个，安全产品漏洞 4 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   | 81 |
| WEB 应用漏洞 | 21 |
| 操作系统漏洞   | 19 |
| 网络设备漏洞   | 4  |
| 安全产品漏洞   | 4  |
| 数据库漏洞    | 1  |

表 3 漏洞按影响类型统计表

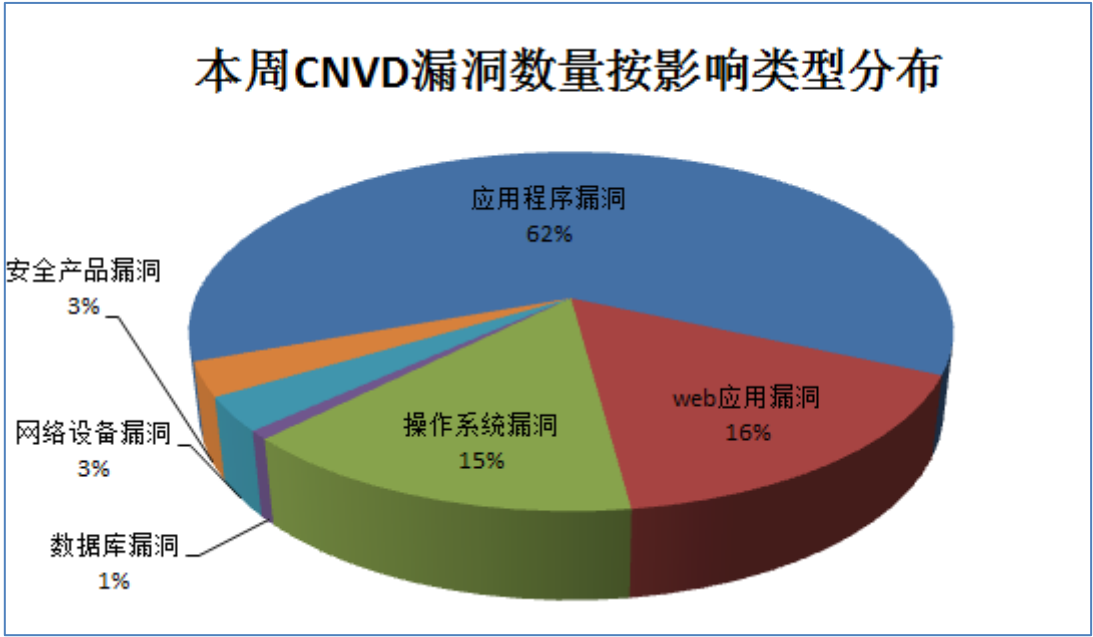


图 1 本周漏洞按影响类型分布

### 本周行业漏洞信息

本周，CNVD 收录了 2 个电信行业漏洞，2 个移动互联网行业漏洞，5 个工控系统行业漏洞（如下图表所示）。其中，“Google Android 整数溢出漏洞、Koha SQL 注入漏洞”的综合评级为“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-2015-05239 | Electric Sheep Fencing Pfsense 'zone'参数跨站脚本漏洞       | 中    | 是     |
| 电信    | CNVD-2015-05260 | ISC BIND 'name.c'远程拒绝服务漏洞                           | 中    | 是     |
| 移动互联网 | CNVD-2015-05187 | Yodobashi Camera Yodobashi APP for Android 敏感信息泄露漏洞 | 中    | 是     |
| 移动互联网 | CNVD-2015-05243 | Google Android 整数溢出漏洞                               | 高    | 是     |
| 工控系统  | CNVD-2015-05197 | Koha SQL 注入漏洞                                       | 高    | 是     |
| 工控系统  | CNVD-2015-05198 | Koha 目录遍历漏洞                                         | 中    | 是     |
| 工控系统  | CNVD-2015-05199 | Koha HTML 注入漏洞                                      | 中    | 是     |
| 工控系统  | CNVD-2015-05200 | Koha 跨站脚本漏洞                                         | 中    | 是     |

|      |                 |               |   |   |
|------|-----------------|---------------|---|---|
| 工控系统 | CNVD-2015-05201 | Koha 跨站请求伪造漏洞 | 中 | 是 |
|------|-----------------|---------------|---|---|

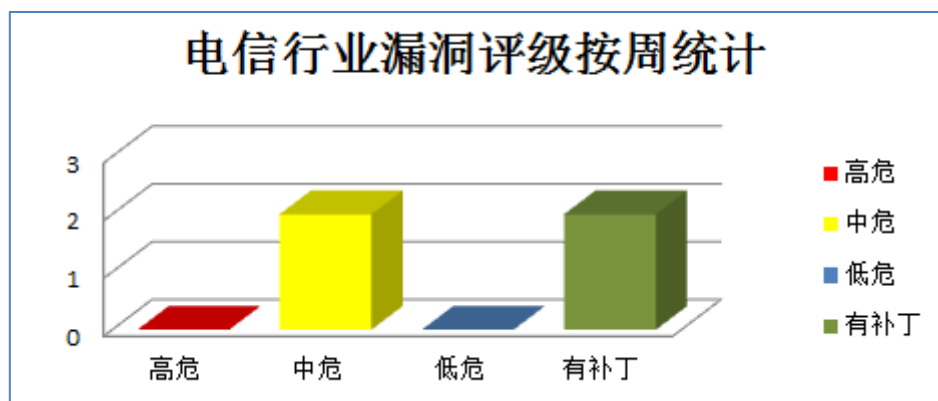


图 1 电信行业漏洞统计

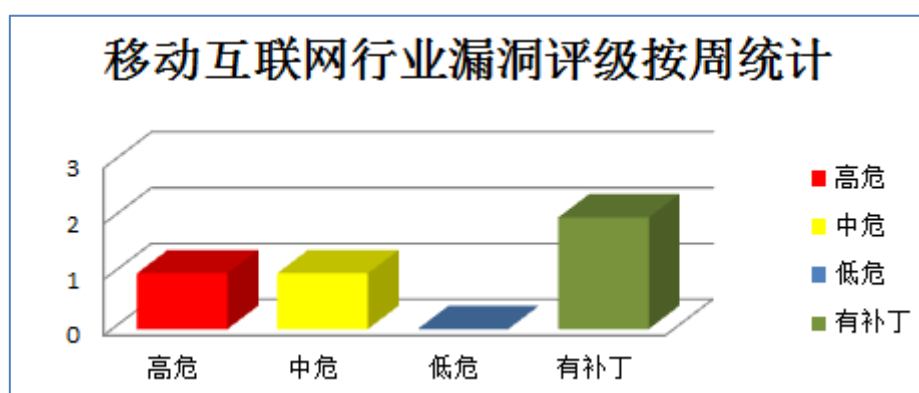


图 2 移动互联网行业漏洞统计

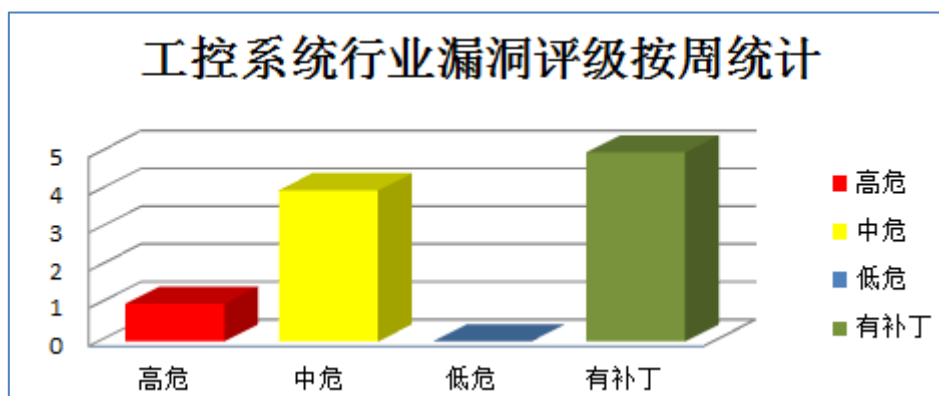


图 3 工控系统行业漏洞统计



## 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、Microsoft 产品安全漏洞

8 月 11 日，微软发布了 2015 年 8 月份的月度例行安全公告，共含 14 项更新，修复了 Microsoft Windows、Office、Silverlight、Edge、Lync、Server 软件、.NET Framework

和 Internet Explorer 中存在的 58 个安全漏洞。其中，4 项远程代码更新的综合评级为最高级“严重”级别。利用上述漏洞，攻击者可以执行远程代码，提升权限，获得敏感信息。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer 内存破坏漏洞（CNVD-2015-05238、CNVD-2015-05237、CNVD-2015-05236、CNVD-2015-05235、CNVD-2015-05234、CNVD-2015-05233、CNVD-2015-05209、CNVD-2015-05210）。上述漏洞的综合评级为“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/webinfo/show/3682>

## 2、Adobe 产品安全漏洞

Adobe Flash Player 是一款 Flash 文件处理程序。本周，上述产品被披露存在未明内存破坏漏洞。攻击者利用漏洞可执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Flash Player 存在未明内存破坏漏洞（CNVD-2015-05266、CNVD-2015-05265、CNVD-2015-05269、CNVD-2015-05268、CNVD-2015-05267、CNVD-2015-05272、CNVD-2015-05271、CNVD-2015-05270）。上述漏洞的综合评级为“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-2015-05266>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05265>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05269>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05268>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05267>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05272>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05271>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05270>

## 3、Mozilla 产品安全漏洞

Mozilla Firefox 是一款开源的 WEB 浏览器。Firefox OS 是开放源代码移动操作系统，采用 Linux 核心，应用于智能手机。本周，上述产品被披露存在信息泄露、跨站脚本、安全限制绕过和拒绝服务漏洞。攻击者可利用漏洞获取敏感信息、进行跨站脚本攻击和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Mozilla Firefox OS 访问限制绕过漏洞、Mozilla Firefox OS 拒绝服务漏洞、Mozilla Firefox OS 跨站脚本漏洞（CNVD-2015-05190、CNVD-2015-05193）、Mozilla Firefox OS 安全机制绕过漏洞、Mozilla Firefox OS 信息泄露漏洞、Mozilla Firefox PDF Viewer 同源绕过信息泄露漏洞。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-2015-05188>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05189>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05190>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05193>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05191>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05192>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05159>

4、Linux 产品安全漏洞

Linux kernel 是一款开源的操作系统。本周，上述产品被披露存在内存泄露、安全绕过和拒绝服务漏洞。攻击者可利用漏洞获得内存信息、执行未授权操作和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括:Linux Kernel 本地拒绝服务漏洞(CNVD-2015-05215、CNVD-2015-05213)、Linux Kernel 本地安全绕过漏洞 (CNVD-2015-05214)、Linux UDF 文件系统拒绝服务漏洞、Linux MD 驱动初始化内存泄露漏洞。目前，除“Linux Kernel 本地拒绝服务漏洞 (CNVD-2015-05213)”外，厂商已经发布了其余漏洞的修补程序。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-2015-05215>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05213>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05214>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05161>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05162>

5、McAfee Application Control 缓冲区溢出漏洞

McAfee Application Control 是美国迈克菲 (McAfee) 公司的一套程序管控软件。本周，McAfee Application Control 被披露存在综合评级为“高危”的缓冲区溢出漏洞。攻击者利用该漏洞可在受影响应用程序上下文中执行任意代码，或发起拒绝服务。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-2015-05275>

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-2015-05167 | GE Healthcare Discovery 530C 内置账户漏洞 | 高    | 暂无   |

|                 |                                              |   |                                                                                                                                                                                                                                                                                                              |
|-----------------|----------------------------------------------|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CNVD-2015-05168 | GE Healthcare Centricity PACS Server 内置账户漏洞  | 高 | 暂无                                                                                                                                                                                                                                                                                                           |
| CNVD-2015-05171 | GE Healthcare CADStream Server 内置账户漏洞        | 高 | 暂无                                                                                                                                                                                                                                                                                                           |
| CNVD-2015-05172 | GE Healthcare Optima MR360 内置账户漏洞            | 高 | 暂无                                                                                                                                                                                                                                                                                                           |
| CNVD-2015-05186 | Sierra Wireless ALEOS 管理员访问权限获取漏洞            | 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://source.sierrawireless.com/resources/airlink/software_reference_docs/release-notes/aleos-4,-d-,4,-d-,2-release-notes/#">http://source.sierrawireless.com/resources/airlink/software_reference_docs/release-notes/aleos-4,-d-,4,-d-,2-release-notes/#</a> |
| CNVD-2015-05197 | Koha SQL 注入漏洞                                | 高 | 用户可联系供应商获得补丁信息：<br><a href="http://koha-community.org/">http://koha-community.org/</a>                                                                                                                                                                                                                       |
| CNVD-2015-05242 | Pimcore CMS 'filter'参数 SQL 注入漏洞              | 高 | 目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：<br><a href="https://www.pimcore.org/">https://www.pimcore.org/</a>                                                                                                                                                                                                             |
| CNVD-2015-05248 | Polycom RealPresence Resource Manager 权限提升漏洞 | 高 | 用户可联系供应商获得补丁信息：<br><a href="http://www.polycom.com/content/dam/polycom/www/includes/site-selector.html?urc=CN">http://www.polycom.com/content/dam/polycom/www/includes/site-selector.html?urc=CN</a>                                                                                                         |
| CNVD-2015-05255 | GNOME Clutter 本地安全绕过漏洞                       | 高 | 目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：<br><a href="https://git.gnome.org/browse/clutter/commit/?h=clutter-1.18&amp;id=97724939c8de004d7fa230f3ff64862d957f93a9">https://git.gnome.org/browse/clutter/commit/?h=clutter-1.18&amp;id=97724939c8de004d7fa230f3ff64862d957f93a9</a>                                       |
| CNVD-2015-05252 | Ubuntu oxide-qt Package 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此安全问题，补丁获取链接：<br><a href="http://www.ubuntu.com/usn/usn-2677-1/">http://www.ubuntu.com/usn/usn-2677-1/</a>                                                                                                                                                                                   |

表 3 部分高危漏洞列表

小结:8月11日,微软发布了2015年8月份的月度例行安全公告,共含14项更新,修复了Microsoft Windows、Office、Silverlight、Edge、Lync、Server 软件、.NET Framework 和 Internet Explorer 中存在的58个安全漏洞。其中,4项远程代码更新的综合评级为最高级“严重”级别。利用上述漏洞,攻击者可以执行远程代码,提升权限,获得敏感信息。此外,Adobe、Mozilla、Linux 多款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、执行未经授权操作、进行跨站脚本攻击和发起拒绝服务攻击。另外,McAfee Application Control 被披露存在一个高危零日漏洞,攻击者利用该漏洞

可在受影响应用程序上下文中执行任意代码，或发起拒绝服务。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、Google 修补 Android 产品漏洞

Android 是基于 Linux 开放性内核的操作系统，是 Google 公司在 2007 年 11 月 5 日公布的手机操作系统。

本周，Google 修补了上述产品存在的整数溢出漏洞，避免攻击者利用漏洞在受影响设备上下文中执行任意代码，或发起拒绝服务攻击。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/62278>

## 本周要闻速递

### 1. 安卓系统 Google Admin 应用曝 0day 漏洞，可绕过沙箱

MWR 实验室的研究人员发现一个 0day 漏洞，该漏洞存在于安卓手机上的谷歌 Admin 应用程序处理一些 URL 的方式中。如果手机上的另一个应用程序向 Admin 应用程序发送一种特定的 URL，那么攻击者就可以绕过同源策略，并能够获取到 Admin 沙箱中的数据。

参考链接：<http://www.freebuf.com/news/75092.html>

### 2. 序列化漏洞影响半数以上 Android 手机

近日，Android 平台又爆出一重大漏洞，影响 55% 的手机。这个 Android 序列化漏洞(CVE-2015-3825)存在于 Android 平台本身，影响的版本包括 4.3 至 5.1，也就是 Jelly Bean、KitKat、棒棒糖和 Android M 预览版 1，波及 55% 的 Android 设备。

参考链接：<http://www.freebuf.com/news/74676.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