

## 信息安全漏洞周报

2015 年 07 月 06 日-2015 年 07 月 12 日

2015 年第 28 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 180 个，其中高危漏洞 76 个、中危漏洞 101 个、低危漏洞 3 个。上述漏洞中，可利用来实施远程攻击的漏洞有 171 个。本周收录的漏洞中，已有 152 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“Joomla! Contact Form Maker 组件 SQL 注入漏洞”、“WeBid 'ajax.php'任意文件上传漏洞”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 180 个漏洞。报送情况如表 1 所示。其中，奇虎、启明星辰、安天实验室、天融信等单位报送数量较多。此外，CNCERT 各分中心、四川大学信息安全研究所、深圳市深信服电子科技有限公司、乌云、漏洞盒子及白帽子向 CNVD 提交了 486 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      | 238    | 238    |
| 启明星辰    | 197    | 0      |
| 安天实验室   | 195    | 0      |
| 天融信     | 138    | 0      |
| 恒安嘉新    | 106    | 0      |
| 绿盟科技    | 52     | 0      |

|                |         |     |
|----------------|---------|-----|
| 知道创宇           | 8       | 0   |
| 乌云             | 216     | 216 |
| 漏洞盒子           | 20      | 20  |
| 四川大学信息安全研究所    | 1       | 1   |
| 深圳市深信服电子科技有限公司 | 1       | 1   |
| CNCERT 福建分中心   | 2       | 2   |
| 个人             | 8       | 8   |
| 报送总计           | 1182    | 486 |
| 录入总计           | 180（去重） | 486 |

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Apple、Mozilla、Cisco 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  | Apple        | 69   | 38%  |
| 2  | Mozilla      | 20   | 11%  |
| 3  | Cisco        | 7    | 4%   |
| 4  | IBM          | 5    | 3%   |
| 5  | EMC          | 5    | 3%   |
| 6  | Kguard       | 4    | 2%   |
| 7  | Chamilo      | 3    | 2%   |
| 8  | EFM Networks | 3    | 2%   |
| 9  | RoundCube    | 2    | 1%   |
| 10 | 其他           | 62   | 34%  |

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 180 个漏洞。其中应用程序漏洞 80 个，操作系统漏洞 59 个，

WEB 应用漏洞 21 个，网络设备漏洞 11 个，安全产品漏洞 9 个。

| 漏洞影响对象类型 | 漏洞数量 |
|----------|------|
| 应用程序漏洞   | 80   |
| 操作系统漏洞   | 59   |
| WEB 应用漏洞 | 21   |
| 网络设备漏洞   | 11   |
| 安全产品漏洞   | 9    |

表 3 漏洞按影响类型统计表

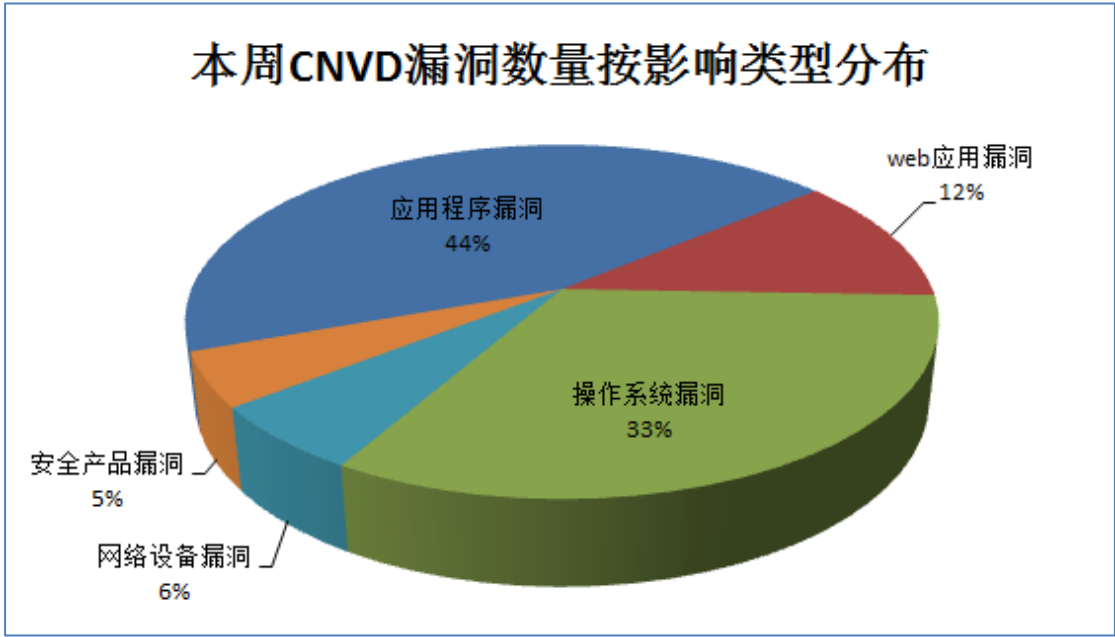


图 1 本周漏洞按影响类型分布

### 本周行业漏洞信息

本周，CNVD 收录了 6 个电信行业漏洞，27 个移动互联网行业漏洞（如下图表所示）。其中，“Cisco Nexus 操作系统设备命令行接口本地权限提升漏洞、Cisco Nexus 7000 设备本地权限提升漏洞、Viber for Android 远程任意代码执行漏洞、Apple iOS 内存信息泄露漏洞（CNVD-2015-04250）、Apple iOS SQLite 缓冲区溢出漏洞、Apple iOS ICC 配置文件处理内存破坏漏洞、Apple iOS 恶意 SIM 卡输入验证漏洞、Apple iOS .tiff 文件处理内存破坏漏洞、ZOHO ManageEngine Desktop Central MSP ‘InventorySW MeteringServlet’任意文件上传漏洞、ZOHO ManageEngine Desktop Central MSP ‘AndroidCheckInServlet’ Servlet 远程代码执行漏洞、Apple iOS WiFi 管理器存在漏洞、Apple iOS text 文件处理内存破坏漏洞（CNVD-2015-04292、CNVD-2015-04293、CNVD-2015-04307、CNVD-2015-04308、CNVD-2015-04309、CNVD-2015-04310）、Apple iOS URL 处理内存破坏漏洞、Apple iOS 字体文件处理内存破坏漏洞、Apple iOS 字体文件处理内存破坏漏洞（CNVD-2015-04311）”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-2015-04324 | Cisco Nexus 操作系统设备命令行接口本地权限提升漏洞                                                   | 高    | 是     |
| 电信    | CNVD-2015-04323 | Cisco Nexus 7000 设备本地权限提升漏洞                                                       | 高    | 是     |
| 电信    | CNVD-2015-04363 | IBM Tivoli Federated Identity Manager 和 Security Access Manager for Mobile 跨站脚本漏洞 | 中    | 是     |
| 电信    | CNVD-2015-04384 | EFM Networks ipTIME 远程代码执行漏洞                                                      | 高    | 否     |
| 电信    | CNVD-2015-04377 | EFM Networks ipTIME 跨站请求伪造漏洞                                                      | 中    | 否     |
| 电信    | CNVD-2015-04388 | EFM Networks ipTIME HTML 注入漏洞                                                     | 中    | 否     |
| 移动互联网 | CNVD-2015-04217 | Apple iOS Webkit SQLite authorizer 任意 SQL 函数调用漏洞                                  | 中    | 是     |
| 移动互联网 | CNVD-2015-04231 | Viber for Android 远程任意代码执行漏洞                                                      | 高    | 是     |
| 移动互联网 | CNVD-2015-04233 | musl libc 'inet_pton.c'栈缓冲区溢出漏洞                                                   | 中    | 是     |
| 移动互联网 | CNVD-2015-04250 | Apple iOS 内存信息泄露漏洞 (CNVD-2015-04250)                                              | 高    | 是     |
| 移动互联网 | CNVD-2015-04244 | Apple iOS 恶意 email 伪造漏洞                                                           | 中    | 是     |
| 移动互联网 | CNVD-2015-04245 | Apple iOS Watch 通用配置文件应用程序安装逻辑漏洞                                                  | 中    | 是     |
| 移动互联网 | CNVD-2015-04246 | Apple iOS Safari 跨站请求伪造漏洞                                                         | 中    | 是     |
| 移动互联网 | CNVD-2015-04247 | Apple iOS SQLite 缓冲区溢出漏洞                                                          | 高    | 是     |
| 移动互联网 | CNVD-2015-04248 | Apple iOS ICC 配置文件处理内存破坏漏洞                                                        | 高    | 是     |
| 移动互联网 | CNVD-2015-04249 | Apple iOS 恶意 SIM 卡输入验证漏洞                                                          | 高    | 是     |
| 移动互联网 | CNVD-2015-04251 | Apple iOS .tiff 文件处理内存破坏漏洞                                                        | 高    | 是     |
| 移动互联网 | CNVD-2015-04277 | ZOHO ManageEngine Desktop Central MSP 'InventorySWMeteringServlet'任意文件上传漏洞        | 高    | 是     |
| 移动互联网 | CNVD-2015-04279 | ZOHO ManageEngine Desktop Central MSP 'AndroidCheckInServlet' Servlet 远程代码执行漏洞    | 高    | 是     |
| 移动互联网 | CNVD-2015-04283 | Apple iOS 通用配置文件应用程序安装逻辑漏洞                                                        | 中    | 是     |
| 移动互联网 | CNVD-2015-04290 | Apple iOS Webkit WebSQL 数据库访问漏洞                                                   | 中    | 是     |

|       |                 |                                             |   |   |
|-------|-----------------|---------------------------------------------|---|---|
| 移动互联网 | CNVD-2015-04291 | Apple iOS WiFi 管理器存在漏洞                      | 高 | 是 |
| 移动互联网 | CNVD-2015-04292 | Apple iOS text 文件处理内存破坏漏洞 (CNVD-2015-04292) | 高 | 是 |
| 移动互联网 | CNVD-2015-04293 | Apple iOS text 文件处理内存破坏漏洞 (CNVD-2015-04293) | 高 | 是 |
| 移动互联网 | CNVD-2015-04307 | Apple iOS text 文件处理内存破坏漏洞 (CNVD-2015-04307) | 高 | 是 |
| 移动互联网 | CNVD-2015-04308 | Apple iOS text 文件处理内存破坏漏洞 (CNVD-2015-04308) | 高 | 是 |
| 移动互联网 | CNVD-2015-04309 | Apple iOS text 文件处理内存破坏漏洞 (CNVD-2015-04309) | 高 | 是 |
| 移动互联网 | CNVD-2015-04310 | Apple iOS text 文件处理内存破坏漏洞 (CNVD-2015-04310) | 高 | 是 |
| 移动互联网 | CNVD-2015-04314 | Apple iOS URL 处理内存破坏漏洞                      | 高 | 是 |
| 移动互联网 | CNVD-2015-04313 | Apple iO 磁盘映像处理信息泄露漏洞                       | 中 | 是 |
| 移动互联网 | CNVD-2015-04312 | Apple iOS 字体文件处理内存破坏漏洞                      | 高 | 是 |
| 移动互联网 | CNVD-2015-04311 | Apple iOS 字体文件处理内存破坏漏洞 (CNVD-2015-04311)    | 高 | 是 |
| 移动互联网 | CNVD-2015-04316 | Android Debuggerd 调试器设备内存泄露漏洞               | 中 | 是 |

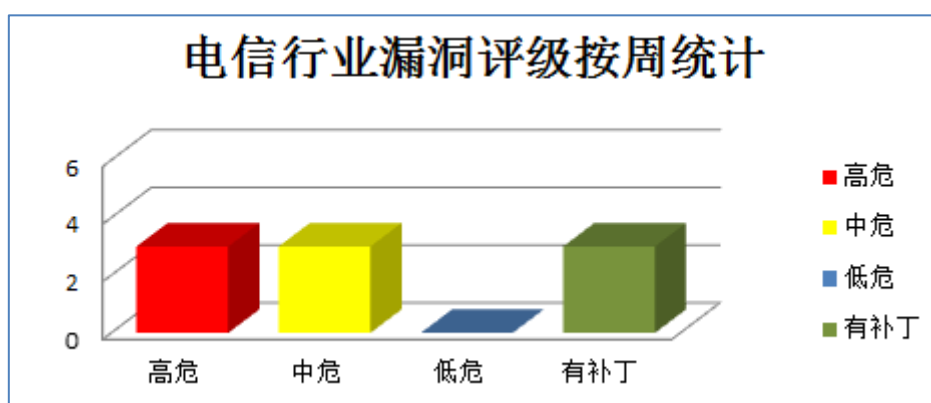


图 1 电信行业漏洞统计

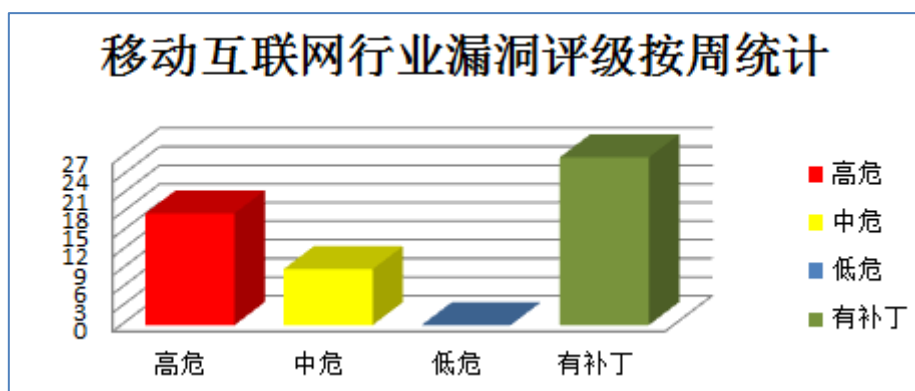


图 2 移动互联网行业漏洞统计



## 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、Apple 产品安全漏洞

Apple Mac OS X 是一款商业性质的操作系统。Apple QuickTime 是一款流行的多媒体播放器。本周，上述产品被披露存在任意代码执行和内存破坏漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Apple MAC OS X 字体文件处理任意代码执行漏洞（CNVD-2015-04269、CNVD-2015-04268、CNVD-2015-04267、CNVD-2015-04266）、Apple QuickTime 内存破坏漏洞（CNVD-2015-04265、CNVD-2015-04264、CNVD-2015-04263、CNVD-2015-04262）。上述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-2015-04269>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04268>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04267>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04266>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04265>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04264>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04263>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04262>

### 2、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信息泄露漏洞。攻击者可利用上述漏洞获取敏感信息。

CNVD 收录的相关漏洞包括：Mozilla Firefox AudioParamTimeline::AudioNodeInputValue 函数信息泄露漏洞、Mozilla Firefox/Firefox ESR/Thunderbird CairoTextureClient D3D9::BorrowDrawTarget 函数信息泄露漏洞、Mozilla Firefox/Firefox ESR/Thunderbird nsZipArchive.cpp 信息泄露漏洞、Mozilla Firefox/Firefox ESR/Thunderbird nsZipArchive::BuildFileList 函数信息泄露漏洞、Mozilla Firefox/Firefox ESR/Thunderbird rx::d3d11::SetBufferData 函数信息泄露漏洞、Mozilla Firefox/Firefox ESR/Thunderbird YCbCr 信息泄露漏洞、Mozilla Firefox/Firefox ESR/Thunderbird ArrayBufferBuilder::append 函数信息泄露漏洞、Mozilla Firefox/Firefox ESR/Thunderbird 信息泄露漏洞。其中，“Mozilla Firefox AudioParamTimeline::AudioNodeInputValue 函数信息泄露漏洞”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-2015-04351>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04331>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04330>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04332>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04333>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04335>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04334>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04338>

### 3、IBM 产品安全漏洞

IBM Tivoli Federated Identity Manager (TFIM) 和 Security Access Manager for Mobile 都是美国 IBM 公司的产品。前者是一款跨企业的联邦身份管理产品。后者是一套通过一个模块式软件包提供移动访问安全防护的解决方案。IBM Business Process Manager (BPM) 是美国 IBM 公司的一套综合的业务流程管理平台。该平台为业务的流程建模、组装、监控和部署提供了一系列的相关工具。IBM UrbanCode Release (UCR) 是美国 IBM 公司的一套用于管理多个相关应用发行及其部署的协作发行软件平台。该平台支持在生命周期模型的每个阶段规划、执行和追踪软件的发行。IBM i Access for Windows 是美国 IBM 公司的一套提供访问和使用各种不同的 Windows 操作系统的桌面资源的客户端解决方案。IBM Security Network Protection 是一套下一代网络入侵防御系统。该系统可监控网络内应用使用、网站访问和操作执行情况,以避免受到恶意软件、僵尸网络等威胁攻击。本周,上述产品被披露存在跨站脚本、栈缓冲区溢出和跨站请求伪造漏洞。攻击者可利用漏洞执行任意代码或进行跨站脚本和跨站请求伪造攻击。

CNVD 收录的相关漏洞包括: IBM Tivoli Federated Identity Manager 和 Security Access Manager for Mobile 跨站脚本漏洞、IBM Business Process Manager 跨站脚本漏洞 (CNVD-2015-04371)、 IBM UrbanCode Release 跨站请求伪造漏洞、IBM i Access for Windows 栈缓冲区溢出漏洞、IBM Security Network Protection 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-2015-04363>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04371>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04372>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04373>  
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04278>

### 4、Cisco 产品安全漏洞

Nexus 是思科的网络交换机系列产品,专为数据中心设计。Cisco Nexus 7000 系列交换机可帮助创建新一代统一阵列数据中心所需的网络基础平台。Cisco Unified

Communications Manager 是企业级 IP 电话呼叫处理系统。Cisco ASA 5500 系列自适应安全设备是用于提供安全和 VPN 服务的模块化平台，可提供防火墙、IPS、anti-X 和 VPN 服务。Cisco Digital Content Manager (DCM) 是美国思科 (Cisco) 公司的一款数字内容管理器。Cisco Headend System Releases 是一款数字宽带传输系统。本周，上述产品被披露存在权限提升和拒绝服务漏洞。攻击者可利用漏洞提升权限或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco Nexus 操作系统设备命令行接口本地权限提升漏洞、Cisco Nexus 7000 设备本地权限提升漏洞、Cisco Unified Communications Domain Manager 默认静态特权帐户漏洞、Cisco Adaptive Security Appliance SNMP 拒绝服务漏洞、Cisco Adaptive Security Appliance OSPFv2 拒绝服务漏洞、Cisco Digital Content Manager 消息处理拒绝服务漏洞、Cisco Headend System Releases 拒绝服务漏洞。其中，“Cisco Nexus 操作系统设备命令行接口本地权限提升漏洞、Cisco Nexus 7000 设备本地权限提升漏洞、Cisco Unified Communications Domain Manager 默认静态特权帐户漏洞”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-2015-04324>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04323>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04320>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04319>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04318>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04315>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04242>

## 5、Berta CMS 'upload.php'任意文件上传漏洞

Berta CMS 是一套基于 PHP 的 Web 内容管理系统。本周，Berta CMS 被披露存在综合评级为“高危”的任意文件上传漏洞。攻击者利用该漏洞提交特殊的文件，并以 WEB 权限执行。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-2015-04239>

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-2015-04227 | WatchGuard XCS SQL 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://www.watchguard.com/support/release-notes/xcs/9/en-US/EN_ReleaseNotes_XCS_9_2_Security_Hotfix/EN_Release_Notes_XCS_v9_2_Sec">https://www.watchguard.com/support/release-notes/xcs/9/en-US/EN_ReleaseNotes_XCS_9_2_Security_Hotfix/EN_Release_Notes_XCS_v9_2_Sec</a> |

|                 |                                                                                      |   |                                                                                                                                                                                                                                                                                                                                                    |
|-----------------|--------------------------------------------------------------------------------------|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 |                                                                                      |   | urity_Hotfix.pdf                                                                                                                                                                                                                                                                                                                                   |
| CNVD-2015-04229 | WatchGuard XCS 'FixCorruptMail'权限提升漏洞                                                | 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://www.watchguard.com/support/release-notes/xcs/9/en-US/EN_ReleaseNotes_XCS_9_2_Security_Hotfix/EN_Release_Notes_XCS_v9_2_Security_Hotfix.pdf">https://www.watchguard.com/support/release-notes/xcs/9/en-US/EN_ReleaseNotes_XCS_9_2_Security_Hotfix/EN_Release_Notes_XCS_v9_2_Security_Hotfix.pdf</a> |
| CNVD-2015-04322 | EMC 多款产品任意文件上传漏洞                                                                     | 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://emc.subscribenet.com/control/dctm/download?element=3887191">https://emc.subscribenet.com/control/dctm/download?element=3887191</a>                                                                                                                                                           |
| CNVD-2015-04339 | Mozilla Firefox/Firefox ESR/Thunderbird PDF.js 权限提升漏洞                                | 高 | Mozilla 已经为此发布了一个安全公告（mfsa2015-69）以及相应补丁：<br><a href="https://www.mozilla.org/en-US/security/advisories/mfsa2015-69/">https://www.mozilla.org/en-US/security/advisories/mfsa2015-69/</a>                                                                                                                                                           |
| CNVD-2015-04342 | Mozilla Firefox/Firefox ESR CanonicalizeXPComParticipant 函数内存错误引用漏洞（CNVD-2015-04342） | 高 | Mozilla 已经为此发布了一个安全公告（mfsa2015-65）以及相应补丁：<br><a href="https://www.mozilla.org/en-US/security/advisories/mfsa2015-65/">https://www.mozilla.org/en-US/security/advisories/mfsa2015-65/</a>                                                                                                                                                           |
| CNVD-2015-04341 | Mozilla Firefox/Firefox ESR CanonicalizeXPComParticipant 函数内存错误引用漏洞（CNVD-2015-04341） | 高 | Mozilla 已经为此发布了一个安全公告（mfsa2015-65）以及相应补丁：<br><a href="https://www.mozilla.org/en-US/security/advisories/mfsa2015-65/">https://www.mozilla.org/en-US/security/advisories/mfsa2015-65/</a>                                                                                                                                                           |
| CNVD-2015-04340 | Mozilla Firefox/Firefox ESR/Thunderbird CSPService::ShouldLoad 函数内存错误引用漏洞            | 高 | Mozilla 已经为此发布了一个安全公告（mfsa2015-63/）以及相应补丁：<br><a href="https://www.mozilla.org/en-US/security/advisories/mfsa2015-63/">https://www.mozilla.org/en-US/security/advisories/mfsa2015-63/</a>                                                                                                                                                          |
| CNVD-2015-04346 | D-Link DSP-W 存在多个漏洞                                                                  | 高 | 目前厂商已经发布了升级补丁以修复这个安全问题，请用户及时下载更新：<br><a href="http://www.dlink.com/">http://www.dlink.com/</a>                                                                                                                                                                                                                                                     |
| CNVD-2015-04353 | Mozilla Firefox 任意代码执行漏洞（CNVD-2015-04353）                                            | 高 | Mozilla 已经为此发布了一个安全公告（mfsa2015-60）以及相应补丁：<br><a href="https://www.mozilla.org/en-US/security/advisories/mfsa2015-60/">https://www.mozilla.org/en-US/security/advisories/mfsa2015-60/</a>                                                                                                                                                           |
| CNVD-2015-04352 | Mozilla Firefox IndexedDatabase Manager 类拒绝服务漏洞                                      | 高 | Mozilla 已经为此发布了一个安全公告（mfsa2015-61）以及相应补丁：<br><a href="https://www.mozilla.org/en-US/security/advisories/mfsa2015-61/">https://www.mozilla.org/en-US/security/advisories/mfsa2015-61/</a>                                                                                                                                                           |

表 3 部分高危漏洞列表

小结：本周，Apple 产品被披露存在任意代码执行和内存破坏漏洞，攻击者可利用漏洞执行任意代码。此外，Mozilla、IBM、Cisco 多款产品被披露存在多个安全漏洞，攻击者利用漏洞可获取敏感信息、提升权限、执行任意代码、进行跨站脚本和跨站请求伪造攻击或发起拒绝服务攻击。另外，Berta CMS 被披露存在一个高危零日漏洞，攻击者利用该漏洞提交特殊的文件，并以 WEB 权限执行。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、GNU 修补 glibc 产品漏洞

GNU glibc（又称 GNU C Library，libc6）是一种按照 LGPL 许可协议发布的开源免费的 C 语言编译程序。

本周，GNU 修补了上述产品存在的拒绝服务漏洞，避免攻击者利用漏洞发起拒绝服务攻击。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/60644>

## 本周要闻速递

### 1. OpenSSL 最新高危漏洞（CVE-2015-1793）补丁发布

研究人员 Adam Langley/David Benjamin (Google/BoringSSL)近日发现了一枚新的 OpenSSL 严重安全漏洞。该漏洞的漏洞编号为 CVE-2015-1793，是证书验证的逻辑过程中没能正确验证新的且不受信任证书造成的。攻击者可以绕过证书警告，强制应用程序将无效证书当作合法证书使用。目前 OpenSSL 发布了 OpenSSL 1.0.2b 和 OpenSSL 1.0.1n 两个版本的最新更新，修复了加密协议中的证书伪造问题。

参考链接：<http://www.freebuf.com/news/72139.html>

### 2. 安卓 adb 备份存在漏洞

Android 在系统备份后还原的处理上存在严重漏洞（CVE-2014-7952），使得攻击者可以注入恶意的 apk 文件到备份文件中(这样还原的时候恶意的应用也安装上去了)。该漏洞是由 Android 的命令行工具 adb 的问题导致的，影响目前所有版本的安卓系统(包括 Android L)。目前该漏洞没有修复。

参考链接：<http://www.freebuf.com/news/72099.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