国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2015 年 08 月 24 日-2015 年 08 月 30 日 **2015 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 219 个，其中高危漏洞 65 个、中危漏洞 134 个、低危漏洞 20 个。上述漏洞中，可利用来实施远程攻击的漏洞有 187 个。本周收录的漏洞中，已有 193 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“PHP 7 ZEND_HASH_IF_FULL_DO_RESIZE 内存错误引用漏洞”、“多个 Apple Mac OS X 权限提升漏洞”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 219 个漏洞。报送情况如表 1 所示。其中，奇虎、安天实验室、天融信、启明星辰等单位报送数量较多。此外，CNCERT 各分中心、乌云、漏洞盒子及白帽子向 CNVD 提交了 637 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	359	359
安天实验室	118	0
天融信	115	0
启明星辰	79	0
绿盟科技	36	0
恒安嘉新	42	0

东软	2	2
乌云	258	258
CNCERT 上海分中心	3	3
CNCERT 江西分中心	1	1
CNCERT 宁夏分中心	1	1
CNCERT 四川分中心	1	1
CNCERT 福建分中心	1	1
个人	11	11
报送总计	1027	637

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、Cisco、Drupal 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	77	35%
2	Cisco	17	8%
3	Drupal	16	7%
4	Wireshark	9	4%
5	Mozilla	8	4%
6	WordPress	6	3%
7	Microsoft	5	2%
8	Electric Sheep Fencing LLC.	5	2%
9	IBM	4	2%
10	其他	72	33%

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 219 个漏洞。其中操作系统漏洞 80 个，应用程序漏洞 77 个，

Web 应用漏洞 34 个，网络设备漏洞 24，安全产品漏洞 3 个，数据库漏洞 1 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	80
应用程序漏洞	77
WEB 应用漏洞	34
网络设备漏洞	24
安全产品漏洞	3
数据库漏洞	1

表 3 漏洞按影响类型统计表

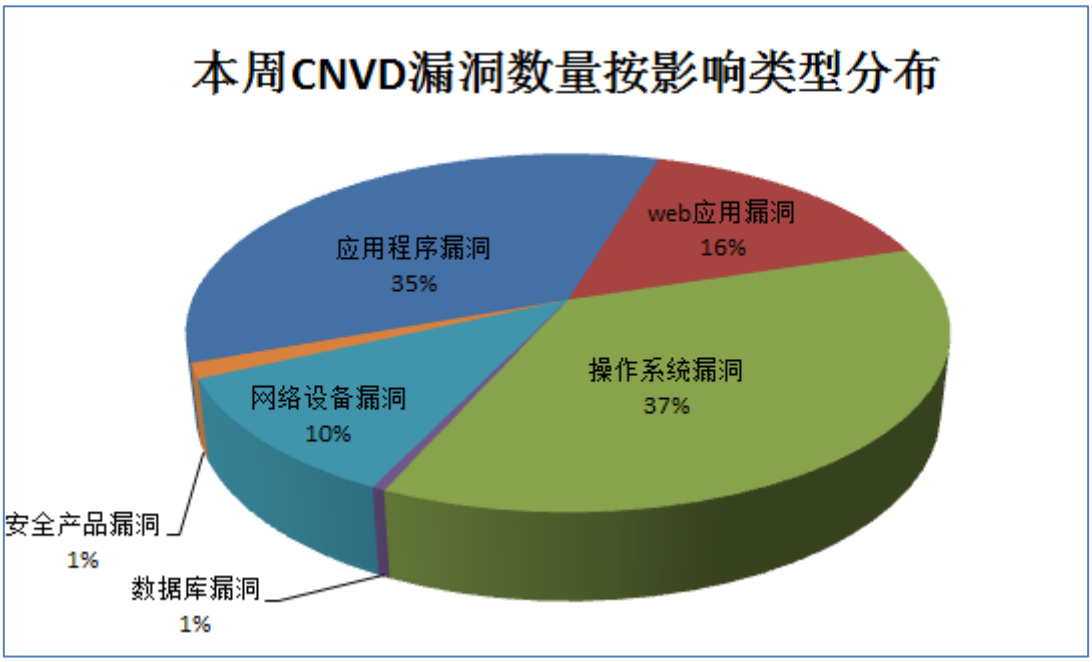

图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 17 个电信行业漏洞、47 个移动互联网行业漏洞、3 个工控系统行业漏洞（如下图表所示）。其中，“Actiontec GT784WN 调制解调器权限获取漏洞、Apple iOS 代码签名绕过漏洞、Apple iOS 代码签名绕过漏洞（CNVD-2015-05539、CNVD-2015-05542、CNVD-2015-05544）、Apple iOS IOHIDFamily 缓冲区溢出漏洞、Apple iOS IOKit 整数溢出漏洞（CNVD-2015-05563）、Apple iOS Libc TRE 库内存破坏漏洞、Apple iOS Libc TRE 库内存破坏漏洞（CNVD-2015-05565、CNVD-2015-05567）、Apple iOS AF_INET6 套接字处理内存破坏漏洞、Apple iOS libpthread 内存破坏漏洞、Apple iOS XPC 消息处理内存破坏漏洞、Apple iOS MSVDX 驱动拒绝服务漏洞、Apple iOS plist 处理内存破坏漏洞、Apple iOS FontParser 内存破坏漏洞、Apple iOS DMG 文件处理内存破坏漏洞、Apple iOS FontParser 内存破坏漏洞（CNVD-2015-05622）、Apple iOS 和 OS X 存在多个漏洞”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-2015-05482	Electric Sheep Fencing pfsense 跨站脚本漏洞	中	是
电信	CNVD-2015-05523	多款 Huawei ME906 产品信息泄露漏洞	中	是
电信	CNVD-2015-05522	IBM Tivoli Storage Manager for Databases 密码信息泄露漏洞	中	是
电信	CNVD-2015-05515	Wireshark GSM RLC/MAC 解析器拒绝服务漏洞	中	是
电信	CNVD-2015-05504	I-O DATA DEVICE NP-BBRS 和 WN-G54/R2 远程拒绝服务漏洞	中	是
电信	CNVD-2015-05532	Cisco ASR 9000 Series Router vty 会话关闭拒绝服务漏洞	中	是
电信	CNVD-2015-05529	Cisco Nexus 3000 Series NX-OS Java 链接目标服务重启漏洞	中	是
电信	CNVD-2015-05524	多款 Huawei ME906 产品安全绕过漏洞	中	是
电信	CNVD-2015-05631	Actiontec GT784WN 调制解调器权限获取漏洞	高	是
电信	CNVD-2015-05630	Actiontec GT784WN 调制解调器跨站请求伪造漏洞	中	是
电信	CNVD-2015-05674	Electric Sheep Fencing pfsense 跨站脚本漏洞（CNVD-2015-05674）	中	是
电信	CNVD-2015-05673	Electric Sheep Fencing pfsense 跨站脚本漏洞（CNVD-2015-05673）	中	是
电信	CNVD-2015-05672	Electric Sheep Fencing pfsense 跨站脚本漏洞（CNVD-2015-05672）	中	是
电信	CNVD-2015-05671	Electric Sheep Fencing Pfsense WebGUI 跨站脚本漏洞	中	否
电信	CNVD-2015-05665	IBM Websphere Message Broker 和 Integration Bus 敏感信息泄露漏洞	低	是
电信	CNVD-2015-05682	Cisco NX-OS on Nexus-OS 缓冲区溢出漏洞	中	否
电信	CNVD-2015-05696	Cisco NX-OS Software 拒绝服务漏洞	中	是
移动互联网	CNVD-2015-05501	Apple iOS Safari WebKit 安全绕过漏洞	中	是
移动互联网	CNVD-2015-05498	Google Android’s media server 存在未明漏洞	中	是
移动互联网	CNVD-2015-05535	Apple iOS CoreText 内存破坏漏洞	中	是
移动互联网	CNVD-2015-05541	Apple iOS 敏感文件访问漏洞	中	是
移动互联网	CNVD-2015-05540	Apple iOS AirTraffic 目录遍历漏洞	中	是
移动互联网	CNVD-2015-05539	Apple iOS 代码签名绕过漏洞（CNVD-2015-05539）	高	是
移动互联网	CNVD-2015-05538	Apple iOS 代码签名绕过漏洞	高	是

移动互联网	CNVD-2015-05537	Apple iOS CoreMedia Playback 内存破坏漏洞（CNVD-2015-05537）	中	是
移动互联网	CNVD-2015-05536	Apple iOS CoreMedia Playback 内存破坏漏洞	中	是
移动互联网	CNVD-2015-05543	Apple iOS Sandbox_profiles 组件信息泄露漏洞	中	是
移动互联网	CNVD-2015-05542	Apple iOS 代码签名绕过漏洞（CNVD-2015-05542）	高	是
移动互联网	CNVD-2015-05544	Apple iOS 代码签名绕过漏洞（CNVD-2015-05544）	高	是
移动互联网	CNVD-2015-05562	Apple iOS IOHIDFamily 缓冲区溢出漏洞	高	是
移动互联网	CNVD-2015-05563	Apple iOS IOKit 整数溢出漏洞（CNVD-2015-05563）	高	是
移动互联网	CNVD-2015-05564	Apple iOS 信息泄露漏洞（CNVD-2015-05564）	低	是
移动互联网	CNVD-2015-05566	Apple iOS Libc TRE 库内存破坏漏洞	高	是
移动互联网	CNVD-2015-05565	Apple iOS Libc TRE 库内存破坏漏洞（CNVD-2015-05565）	高	是
移动互联网	CNVD-2015-05567	Apple iOS Libc TRE 库内存破坏漏洞（CNVD-2015-05567）	高	是
移动互联网	CNVD-2015-05568	Apple iOS AF_INET6 套接字处理内存破坏漏洞	高	是
移动互联网	CNVD-2015-05569	Apple iOS libpthread 内存破坏漏洞	高	是
移动互联网	CNVD-2015-05570	Apple iOS libxml2 用户信息泄露漏洞	中	是
移动互联网	CNVD-2015-05571	Apple iOS XPC 消息处理内存破坏漏洞	高	是
移动互联网	CNVD-2015-05572	Apple iOS 符号链接漏洞	中	是
移动互联网	CNVD-2015-05573	Apple iOS 任意应用扩展替换漏洞	中	是
移动互联网	CNVD-2015-05574	Apple iOS MSVDX 驱动拒绝服务漏洞	高	是
移动互联网	CNVD-2015-05575	Apple iOS Office Viewer 敏感信息泄露漏洞	中	是
移动互联网	CNVD-2015-05576	Apple iOS QL Office 内存破坏漏洞	中	是
移动互联网	CNVD-2015-05577	Apple iOS 警告消息拒绝服务漏洞	中	是
移动互联网	CNVD-2015-05581	Apple iOS Backup 符号链接漏洞	中	是
移动互联网	CNVD-2015-05582	Apple iOS ImageIO 内存破坏漏洞	中	是
移动互联网	CNVD-2015-05584	Apple iOS ImageIO 内存信息泄露漏洞	中	是
移动互联网	CNVD-2015-05585	Apple iOS ImageIO 内存信息泄露漏洞（CNVD-2015-05585）	中	是
移动互联网	CNVD-2015-05583	Apple iOS plist 处理内存破坏漏洞	高	是
移动互联网	CNVD-2015-05599	Apple iOS 安全机制绕过漏洞	低	是
移动互联网	CNVD-2015-05600	Apple iOS WebViews FaceTime URL 解析漏洞	中	是
移动互联网	CNVD-2015-05619	Apple iOS CoreText 内存破坏漏洞（CN	中	是

		VD-2015-05619）		
移动互联网	CNVD-2015-05620	Apple iOS FontParser 内存破坏漏洞	高	是
移动互联网	CNVD-2015-05610	Apple iOS WebKit 安全绕过漏洞	中	是
移动互联网	CNVD-2015-05611	Apple iOS iCloud 信息泄露漏洞	中	是
移动互联网	CNVD-2015-05612	Apple iOS 其他应用管理参数信息泄露漏洞	中	是
移动互联网	CNVD-2015-05625	Apple iOS DMG 文件处理内存破坏漏洞	高	是
移动互联网	CNVD-2015-05621	Apple iOS FontParser 内存破坏漏洞（CNVD-2015-05621）	中	是
移动互联网	CNVD-2015-05622	Apple iOS FontParser 内存破坏漏洞（CNVD-2015-05622）	高	是
移动互联网	CNVD-2015-05645	Apple iOS 和 OS X 信息泄露漏洞	中	是
移动互联网	CNVD-2015-05646	Apple iOS 和 OS X 存在多个漏洞	高	是
移动互联网	CNVD-2015-05649	Google Android SMS 和 MMS 消息篡改漏洞	中	否
移动互联网	CNVD-2015-05697	Google Android 存在漏洞	中	是
工控系统	CNVD-2015-05651	KAKO HMI 硬编码密码安全绕过漏洞	中	否
工控系统	CNVD-2015-05659	Rockwell Automation 1769-L18ER/A LOGIX5318ER 跨站脚本漏洞	中	是
工控系统	CNVD-2015-05660	Rockwell Automation 1766-L32 Series 远程文件包含漏洞	中	是

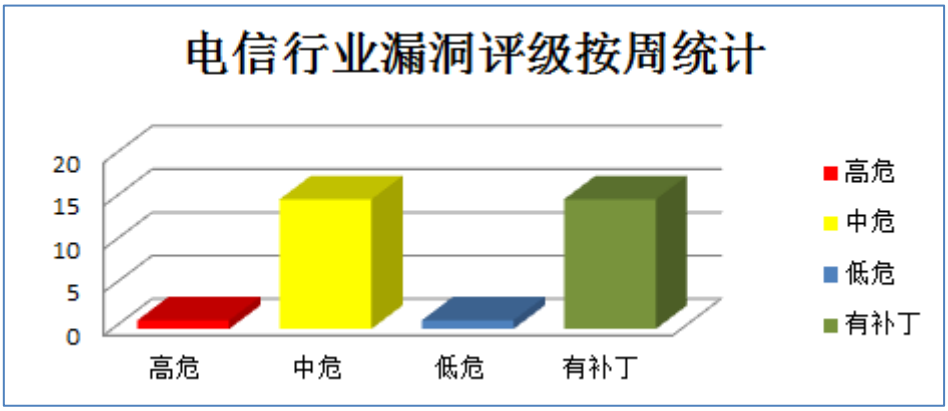

图 1 电信行业漏洞统计

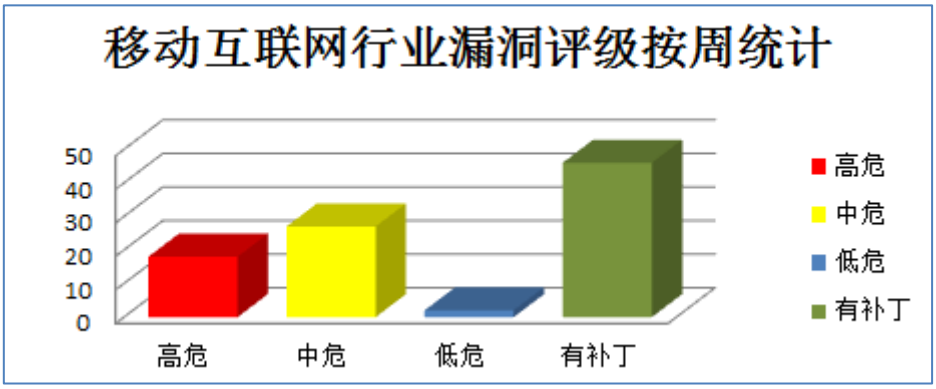

图 2 移动互联网行业漏洞统计

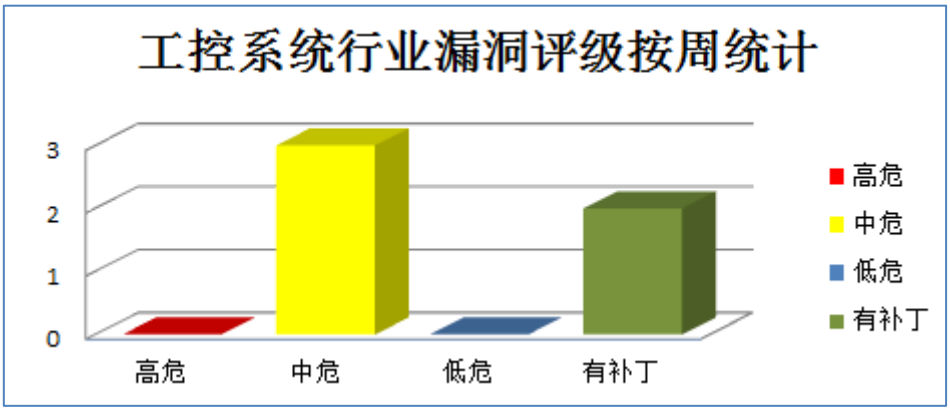

图 3 工控系统行业漏洞统计

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、 Apple 产品安全漏洞

Apple OS X 是一款苹果分发的基于 BSD 的操作系统。本周，上述产品被披露存在内存破坏漏洞。攻击者利用漏洞可执行任意代码。

CNVD 收录的相关漏洞包括：Apple OS X SceneKit 内存破坏漏洞、Apple OS X DMG 文件处理内存破坏漏洞、Apple OS X Data Detectors Engine 内存破坏漏洞、Apple OS X IOFireWireFamily 内存破坏漏洞（CNVD-2015-05547、CNVD-2015-05548、CNVD-2015-05549）、Apple OS X IOGraphics 内存破坏漏洞（CNVD-2015-05551、CNVD-2015-05550）。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-2015-05607

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05613

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05617

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05547

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05548

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05549

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05550

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05551

2、 Mozilla 产品安全漏洞

Mozilla Firefox 和 Firefox ESR 都是美国 Mozilla 基金会开发的浏览器产品。Firefox 是一款开源 Web 浏览器；Firefox ESR 是 Firefox 的一个延长支持版本。Mozilla Maintenance Service 是其中的一个静默升级程序（即在不通知你的情况下自动将浏览器升级

到最新版本）组件。本周，上述产品被披露存在多个安全漏洞。攻击者利用漏洞可获取权限、进行跨站脚本攻击和执行任意代码。

CNVD 收录的相关漏洞包括：Mozilla Firefox 和 Firefox ESR Mozilla Maintenance Service 组件竞争条件漏洞、Mozilla Firefox 中间人攻击漏洞、Mozilla Firefox JSON 解析同源策略绕过漏洞、Mozilla Firefox 共享内存使用拒绝服务漏洞、Mozilla Firefox bitmap 图像处理堆溢出漏洞、Mozilla Firefox 统配字符处理跨站脚本漏洞、Mozilla Firefox 音频处理内存错误引用漏洞、Mozilla Firefox libstagefright 整数溢出漏洞。其中“Mozilla Firefox 和 Firefox ESR Mozilla Maintenance Service 组件竞争条件漏洞、Mozilla Firefox 音频处理内存错误引用漏洞、Mozilla Firefox libstagefright 整数溢出漏洞”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-2015-05676

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05675

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05590

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05589

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05588

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05587

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05586

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05604

3、Cisco 产品安全漏洞

Cisco Aggregation Services Router5000 和 ASR 5500 System Software 是美国思科的 5000 系列无线控制器产品。Cisco Prime Infrastructure 是一套通过 Cisco Prime LAN Management Solution 和 Cisco Prime Network Control System 技术进行无线管理的解决方案。Cisco TelePresence Video Communication Server（VCS）Expressway 是美国思科（Cisco）公司的一款网真视频通信服务器，它能够与统一通信和语音通信环境集成，从而为使用各种通信工具的最终用户提供最佳体验。Cisco TelePresence Video Communication Server（VCS）Expressway 是一款网真视频通信服务器。Cisco NX-OS Software 是美国思科（Cisco）公司的一套面向数据中心的操作系统。Cisco Unified Web Interaction Manager 是一款 WEB 交互管理程序。Cisco FireSIGHT 管理中心可以集中式管理采用 FirePOWER Services 的 Cisco ASA 和思科 FirePOWER 网络安全设备的网络安全和运行功能。本周，上述产品被披露存在多个安全漏洞。攻击者可利用漏洞提升权限、绕过安全限制和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco Aggregation Services Router 5000 和 ASR 5500 System Software 拒绝服务漏洞、Cisco Prime Infrastructure 权限提升漏洞、Cisco TelePresence Video Communication Server Expressway 远程命令注入漏洞、Cisco TelePres

ence Video Communication Server Expressway 密码更改漏洞、Cisco NX-OS Software 拒绝服务漏洞、Cisco Unified Web Interaction Manager Web 接口拒绝服务漏洞、Cisco Unified Web Interaction Manager Web 接口安全限制绕过漏洞、Cisco FireSIGHT Management Center 系统策略删除漏洞。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-2015-05661

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05662

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05505

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05591

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05696

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05526

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05527

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05528

4、Microsoft 产品安全漏洞

Microsoft Internet Explorer 是一款流行的 WEB 浏览器。Microsoft Windows 是一款流行的操作系统。Microsoft XML Core Services(MSXML)是一款允许使用 JScript、VBScript 和 Visual Studio 6.0 的用户开发基于 XML 的应用，以与其他遵循 XML 1.0 标准的应用程序交互操作。本周，上述产品被披露存在信息泄露、跨站脚本和内存破坏漏洞。攻击者可利用漏洞获得敏感信息、进行跨站脚本攻击和执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer 内存破坏漏洞（CNVD-2015-05643）、Microsoft 多个应用本地信息泄露漏洞、Microsoft Windows UDDI 服务跨站脚本漏洞、Microsoft XML Core Services 中间人信息泄露漏洞（CNVD-2015-05495、CNVD-2015-05494）。其中“Microsoft Internet Explorer 内存破坏漏洞（CNVD-2015-05643）”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-2015-05643

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05497

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05496

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05495

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05494

5、WordPress Powerplay Gallery 插件任意文件上传漏洞

WordPress 是 WordPress 软件基金会的一套使用 PHP 语言开发的博客平台，该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。Powerplay Gallery 是其中的一个用于展示图片的画廊插件。本周，WordPress Powerplay Gallery 被披露存在综合评级为“高危”的任意文件上传漏洞。攻击者利用该漏洞可执行任意代码。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-2015-05481

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-2015-05484	Joomla! J2Store 扩展 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：http://j2store.org/download-j2store/j2store-v3-3-1-7.html
CNVD-2015-05483	Joomla! FreiChat 组件 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：http://codologic.com/page/freichat-free-php-chat-script-software
CNVD-2015-05512	Wireshark 存在未明内存破坏漏洞	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：https://www.wireshark.org/security/wnpa-sec-2015-22.html
CNVD-2015-05525	HP Operations Manager i 存在未明任意代码执行漏洞	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：http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c04762687
CNVD-2015-05534	Free MP3 CD Ripper 缓冲区溢出漏洞	高	暂无
CNVD-2015-05596	NAP Turbo NAS Series Devices 'Change Password'函数权限提升漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.qnap.com/i/en/support/con_show.php?cid=83
CNVD-2015-05598	NAP Turbo NAS Series Devices CGI 任意代码执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.qnap.com/i/en/support/con_show.php?cid=83
CNVD-2015-05631	Actiontec GT784WN 调制解调器权限获取漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页：http://www.actiontec.com/
CNVD-2015-05627	Mobile Devices C4 OBD2 Dongle 权限访问漏洞（CNVD-2015-05627）	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页：http://www.mobile-devices.com/

CNVD-2015-05628	Mobile Devices C4 OBD2 Dongle 权限访问漏洞（CNVD-2015-05628）	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页：http://www.mobile-devices.com/

表 3 部分高危漏洞列表

小结：Apple 产品被披露存在内存破坏漏洞。攻击者利用漏洞可执行任意代码。此外，Mozilla、Cisco、Microsoft 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、提升权限、进行跨站脚本攻击、执行任意代码或发起拒绝服务攻击。另外，WordPress Powerplay Gallery 被披露存在一个高危零日漏洞，攻击者利用该漏洞可执行任意代码。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、Adobe 修补 LiveCycle Data Services 产品漏洞

Adobe LiveCycle Data Services 是美国奥多比（Adobe）公司的一套部署在应用服务器上并整合了 RIA 应用和 J2EE 等企业应用的服务器软件。该软件提供远程过程调用（RPC）服务、消息服务和数据管理等功能。

本周，Adobe 修补了上述产品存在的信息泄露漏洞，避免攻击者利用漏洞获得敏感信息。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/62770

本周要闻速递

1. 安卓海豚浏览器存在远程代码执行漏洞

安卓海豚浏览器存在远程代码执行漏洞，攻击者可通过安卓海豚浏览器控制用户的网络通信数据，可以修改下载和应用浏览器新主题的函数。通过利用该函数，攻击者可以写入任意文件，这些文件将会在用户设备中的浏览器环境下变成代码执行。

参考链接：http://www.freebuf.com/news/75837.html

2. 一个针对中国用户的安卓木马

近日，Doctor Web 安全小组发现了一个新的 Android 木马，被命名为 Android.Backdoor.260.origin。该木马在中国用户之间传播，监视着受害者的信息。攻击者可以利用该木马劫持受害者的短信、通话记录、定位 GPS 坐标、屏幕截图，甚至还可以搜集所有用户输入的数据。

参考链接：http://www.freebuf.com/news/76231.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

邮箱：vreport@cert.org.cn

电话：010-82990999