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 17 日-2015 年 08 月 23 日 **2015 年第 34 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 183 个，其中高危漏洞 85 个、中危漏洞 90 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 169 个。本周收录的漏洞中，已有 162 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“Arab Portal SQL 注入漏洞”、“Xceedium Xsuite 任意访问根用户漏洞”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 183 个漏洞。报送情况如表 1 所示。其中，启明星辰、奇虎、天融信、安天实验室等单位报送数量较多。此外，CNCERT 各分中心、中国科学院信息工程研究所第六研究室、深圳市深信服电子科技有限公司、广州白狐网络科技有限公司、乌云、漏洞盒子及白帽子向 CNVD 提交了 735 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
启明星辰	388	0
奇虎	331	331
天融信	312	0
安天实验室	193	0
绿盟科技	117	0

恒安嘉新	55	0
知道创宇	14	0
乌云	319	319
漏洞盒子	46	46
中国科学院信息工程研究所第六研究室	15	15
深圳市深信服电子科技有限公司	5	5
广州白狐网络科技有限公司	1	1
CNCERT 上海分中心	1	1
CNCERT 福建分中心	2	2
个人	15	15
报送总计	1814	735
录入总计	183（去重）	735

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、Adobe、Microsoft 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	36	20%
2	Adobe	26	14%
3	Microsoft	26	14%
4	EMC	14	8%
5	Mozilla	13	7%
6	Cisco	12	7%
7	Xceedium	6	3%
8	Drupal	5	3%
9	WordPress	3	2%
10	其他	42	22%

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 183 个漏洞。其中应用程序漏洞 131 个，操作系统漏洞 34 个 Web 应用漏洞 17 个，安全产品漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	131
操作系统漏洞	34
WEB 应用漏洞	17
安全产品漏洞	1

表 3 漏洞按影响类型统计表

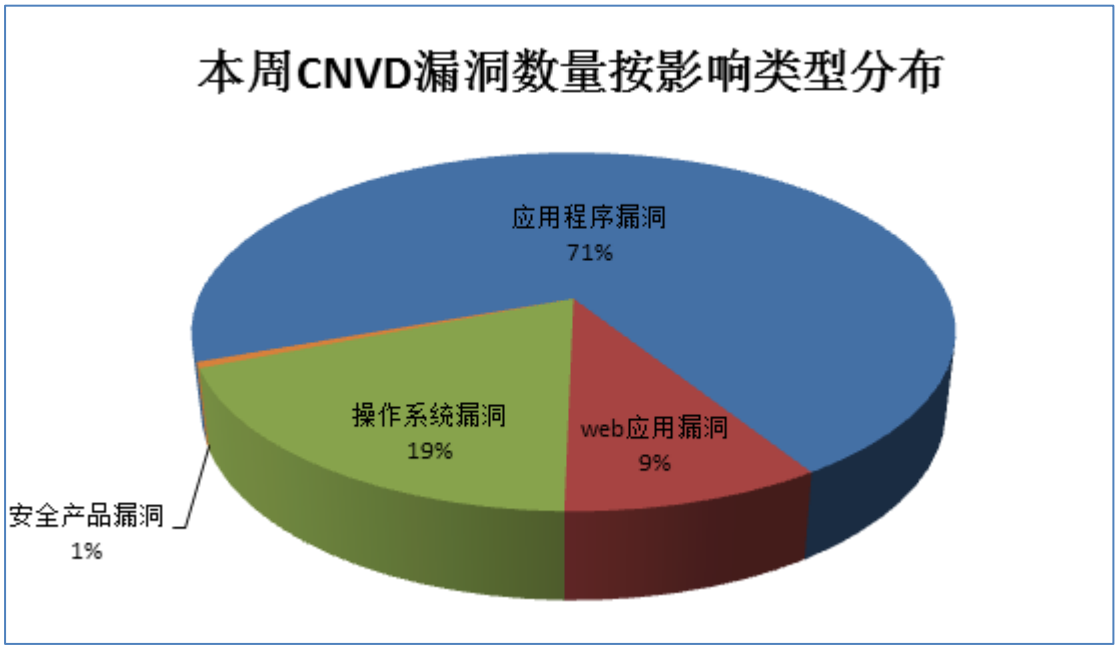

图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 20 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
移动互联网	CNVD-2015-05409	Apple Safari WebKit 存在未明内存破坏漏洞（CNVD-2015-05409）	中	是
移动互联网	CNVD-2015-05408	Apple Safari WebKit 存在未明内存破坏漏洞（CNVD-2015-05408）	中	是
移动互联网	CNVD-2015-05407	Apple Safari WebKit 存在未明内存破坏漏洞（CNVD-2015-05407）	中	是
移动互联网	CNVD-2015-05406	Apple Safari WebKit 存在未明内存破坏漏洞（CNVD-2015-05406）	中	是

移动互联网	CNVD-2015-05405	Apple Safari WebKit 存在未明内存破坏漏洞（CNVD-2015-05405）	中	是
移动互联网	CNVD-2015-05424	Apple Safari WebKit 存在未明内存破坏漏洞（CNVD-2015-05424）	中	是
移动互联网	CNVD-2015-05423	Apple Safari WebKit 存在未明内存破坏漏洞（CNVD-2015-05423）	中	是
移动互联网	CNVD-2015-05422	Apple Safari WebKit 存在未明内存破坏漏洞（CNVD-2015-05422）	中	是
移动互联网	CNVD-2015-05421	Apple Safari WebKit 存在未明内存破坏漏洞（CNVD-2015-05421）	中	是
移动互联网	CNVD-2015-05420	Apple Safari WebKit 存在未明内存破坏漏洞（CNVD-2015-05420）	中	是
移动互联网	CNVD-2015-05419	Apple Safari WebKit 存在未明内存破坏漏洞（CNVD-2015-05419）	中	是
移动互联网	CNVD-2015-05418	Apple Safari WebKit 存在未明内存破坏漏洞（CNVD-2015-05418）	中	是
移动互联网	CNVD-2015-05417	Apple Safari WebKit 存在未明内存破坏漏洞（CNVD-2015-05417）	中	是
移动互联网	CNVD-2015-05416	Apple Safari WebKit 存在未明内存破坏漏洞（CNVD-2015-05416）	中	是
移动互联网	CNVD-2015-05415	Apple Safari WebKit 存在未明内存破坏漏洞（CNVD-2015-05415）	中	是
移动互联网	CNVD-2015-05414	Apple Safari WebKit 存在未明内存破坏漏洞（CNVD-2015-05414）	中	是
移动互联网	CNVD-2015-05413	Apple Safari WebKit 存在未明内存破坏漏洞（CNVD-2015-05413）	中	是
移动互联网	CNVD-2015-05412	Apple Safari WebKit 存在未明内存破坏漏洞（CNVD-2015-05412）	中	是
移动互联网	CNVD-2015-05411	Apple Safari WebKit 存在未明内存破坏漏洞（CNVD-2015-05411）	中	是
移动互联网	CNVD-2015-05410	Apple Safari WebKit 存在未明内存破坏漏洞（CNVD-2015-05410）	中	是

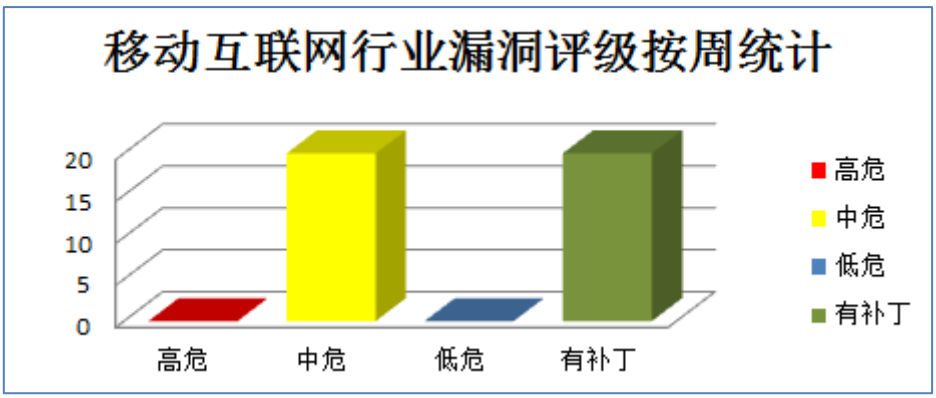

图 1 移动互联网行业漏洞统计

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 Safari 是一款开源的 WEB 浏览器。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：Apple Safari WebKit 存在未明内存破坏漏洞（CNVD-2015-05408、CNVD-2015-05407、CNVD-2015-05406、CNVD-2015-05405、CNVD-2015-05423、CNVD-2015-05422、CNVD-2015-05421、CNVD-2015-05420）。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-2015-05408

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05407

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05406

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05405

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05423

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05422

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05421

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05420

2、 Adobe 产品安全漏洞

Adobe Flash Player、Adobe AIR SDK 和 Adobe AIR SDK & Compiler 都是美国奥多比（Adobe）公司的产品。Adobe Flash Player 是一款多媒体播放器产品；Adobe AIR SDK 和 Adobe AIR SDK & Compiler 都是适用于 Adobe AIR（一个跨操作系统的运行时环境）的标准开发工具包。本周，上述产品被披露存在内存错误引用漏洞。攻击者利用漏洞可执行任意代码。

CNVD 收录的相关漏洞包括：多款 Adobe 产品内存错误引用漏洞（CNVD-2015-05301、CNVD-2015-05300、CNVD-2015-05303、CNVD-2015-05302、CNVD-2015-05305、CNVD-2015-05304、CNVD-2015-05307、CNVD-2015-05306）。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-2015-05301

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05300

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05303

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05302

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05305

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05304

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05307

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05306

3、 Mozilla 产品安全漏洞

Mozilla Firefox 是一款开源的 WEB 浏览器。本周，上述产品被披露存在内存破坏和缓冲区溢出漏洞。攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Mozilla Firefox 存在未明内存破坏漏洞（CNVD-2015-05438、CNVD-2015-05437、CNVD-2015-05436、CNVD-2015-05435、CNVD-2015-05434）、Mozilla Firefox MPEG4 视频处理缓冲区溢出漏洞（CNVD-2015-05452、CNVD-2015-05453、CNVD-2015-05454）。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-2015-05438

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05437

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05436

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05435

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05434

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05452

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05453

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05454

4、 Cisco 产品安全漏洞

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。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得敏感信息、读取任意文件、执行任意代码和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco TelePresence Video Communication Server Expressway 任意命令执行漏洞、Cisco TelePresence Video Communication Server Expressway 权限获取漏洞、Cisco TelePresence Video Communication Server Expressway 记录错误信息获取漏洞、Cisco TelePresence Video Communication Server Expressway 拒绝服务漏洞、Cisco TelePresence Video Communication Server Expressway HTTP GET 请求拒绝服务漏洞、Cisco TelePresence Video Communication Server Expressway 用户伪造漏洞、Cisco TelePresence Video Communication Server Expressway 外部 DTD 文件读取漏洞、Cisco TelePresence Video Communication Server Expresswa 密码哈希获取漏洞。目前，厂商已经发布了“Cisco TelePresence Video Communication Server Expressway

记录错误信息获取漏洞”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-2015-05465

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05455

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05425

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05429

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05428

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05427

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05426

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05431

5、Kernel Virtual Machine 内存破坏漏洞

Linux kernel 是美国 Linux 基金会发布的操作系统 Linux 所使用的内核。Kernel Virtual Machine（KVM，Kernel-based Virtual Machine，基于内核的虚拟机）是用于其中的一种虚拟化基础设施。本周，Kernel Virtual Machine 被披露存在综合评级为“高危”的内存破坏漏洞。攻击者利用该漏洞可获取敏感信息或造成应用程序拒绝服务。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-2015-05358

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-2015-05323	Microsoft .NET Framework 权限提升漏洞（CNVD-2015-05323）	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：http://technet.microsoft.com/security/bulletin/MS15-092
CNVD-2015-05322	Microsoft Windows filesystem 远程权限提升漏洞	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：http://technet.microsoft.com/security/bulletin/MS15-090
CNVD-2015-05320	Microsoft Windows 注册表远程权限提升漏洞	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：http://technet.microsoft.com/security/bulletin/MS15-090
CNVD-2015-05319	Microsoft RDP DLL 加载远程代码执行漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页

			下载：http://technet.microsoft.com/security/bulletin/ms15-082
CNVD-2015-05333	FreeBSD patch(1) shell 注入漏洞	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：ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-15:18.bsdpatch.asc
CNVD-2015-05325	Microsoft .NET Framework 权限提升漏洞（CNVD-2015-05325）	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：http://technet.microsoft.com/security/bulletin/MS15-092
CNVD-2015-05324	Microsoft .NET Framework 权限提升漏洞（CNVD-2015-05324）	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：http://technet.microsoft.com/security/bulletin/MS15-092
CNVD-2015-05346	Microsoft Office 内存破坏漏洞（CNVD-2015-05346）	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：http://technet.microsoft.com/security/bulletin/MS15-081
CNVD-2015-05351	Microsoft Windows TrueType 字体远程代码执行漏洞（CNVD-2015-05351）	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：http://technet.microsoft.com/security/bulletin/MS15-080
CNVD-2015-05354	Codoforum 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，请到厂商的主页下载：http://www.codoforum.com/

表 3 部分高危漏洞列表

小结：Apple 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。此外，Adobe、Mozilla、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得敏感信息、读取任意文件、执行任意代码或发起拒绝服务攻击。另外，Kernel Virtual Machine 被披露存在一个高危零日漏洞，攻击者利用该漏洞可获取敏感信息或造成应用程序拒绝服务。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 Golang Go 产品漏洞

Google Golang Go 是一种针对多处理器系统应用程序的编程进行了优化的编程语言。

本周，Google 修补了上述产品存在的 HTTP 头注入漏洞，避免攻击者利用漏洞向服务器响应中注入 HTTP 头，欺骗目标用户，实施缓存中毒攻击等。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/62589

本周要闻速递

1. Camera360 被爆存在漏洞：数据存在泄露风险导致未经授权可访问他人照片

Camera360 被爆存在漏洞，该 App 虽然能够让用户的照片变得十分漂亮，但是在无意之间泄露了用户的隐私数据：恶意攻击者可以未经过授权就能够访问到 Camera360 用户的云账户和相册。

参考链接：http://www.freebuf.com/news/75569.html

2. Mac OS X 操作系统被爆权限提升 0day 漏洞

意大利安全研究员 Luca Todesco 发现苹果 Mac OS X 操作系统中存在 2 枚新的 0day 漏洞，攻击者可利用这两个漏洞破坏 OS X 内核中的内存，然后绕过系统的安全功能，运行相关代码，攻击者可获得 root 权限。受影响的版本：OS X 10.9.5 到 OS X 10.10.5。OS X 10.11 已经修复了该漏洞。

参考链接：http://www.freebuf.com/news/75318.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