

信息安全漏洞周报

2015 年 04 月 13 日-2015 年 04 月 19 日

2015 年第 16 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**高**。

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 195 个，其中高危漏洞 77 个、中危漏洞 99 个、低危漏洞 19 个。上述漏洞中，可利用来实施远程攻击的漏洞有 159 个。本周收录的漏洞中，已有 173 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“Crystal Player 播放列表文件缓冲区溢出漏洞”、“Clever Internet ActiveX Suite CLINetSuite X6.OCX 存在多个漏洞”等零日攻击代码，请使用相关产品的用户注意加强防范。

本周微软 IIS 服务器或部署开放 IIS 服务的主机受到 HTTP.sys 远程代码执行漏洞的影响，根据 CNCERT 4 月 19 日对境内 IP 主机的检测情况，境内仍有 44.4% 的 IIS 主机未修复漏洞。

成员单位报送漏洞统计

本周，共 6 家成员单位、合作伙伴及个人报送了本周收录的全部 195 个漏洞。报送情况如表 1 所示。其中，启明星辰、安天实验室、天融信、恒安嘉新等单位报送数量较多。此外，CNCERT 各分中心、深圳市深信服电子科技有限公司、上海天泰网络科技有限公司、安徽讯成创安科技有限公司、乌云、漏洞盒子及白帽子向 CNVD 提交了 33 5 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
启明星辰	204	0
安天实验室	192	0
天融信	165	1

恒安嘉新	100	0
绿盟科技	23	0
知道创宇	9	0
乌云	286	286
漏洞盒子	21	21
深圳市深信服电子科技有限公司	2	2
上海天泰网络技术有限公司	1	1
安徽讯成创安科技有限公司	1	1
CNCERT 福建分中心	1	1
CNCERT 山西分中心	1	1
个人	21	21
报送总计	1027	335
录入总计	195（去重）	335

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、Microsoft、IBM 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	63	32%
2	Microsoft	27	14%
3	IBM	12	6%
4	Adobe	12	6%
5	MediaWiki	12	6%
6	Oracle	10	5%
7	WordPress	8	4%
8	Cisco	7	4%
9	Kemp	6	3%

10	其他	38	20%
----	----	----	-----

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 195 个漏洞。其中应用程序漏洞 96 个，操作系统漏洞 66 个，WEB 应用漏洞 13 个，网络设备漏洞 9 个，数据库漏洞 6 个，安全产品漏洞 5 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	96
操作系统漏洞	66
WEB 应用漏洞	13
网络设备漏洞	9
数据库漏洞	6
安全产品漏洞	5

表 3 漏洞按影响类型统计表

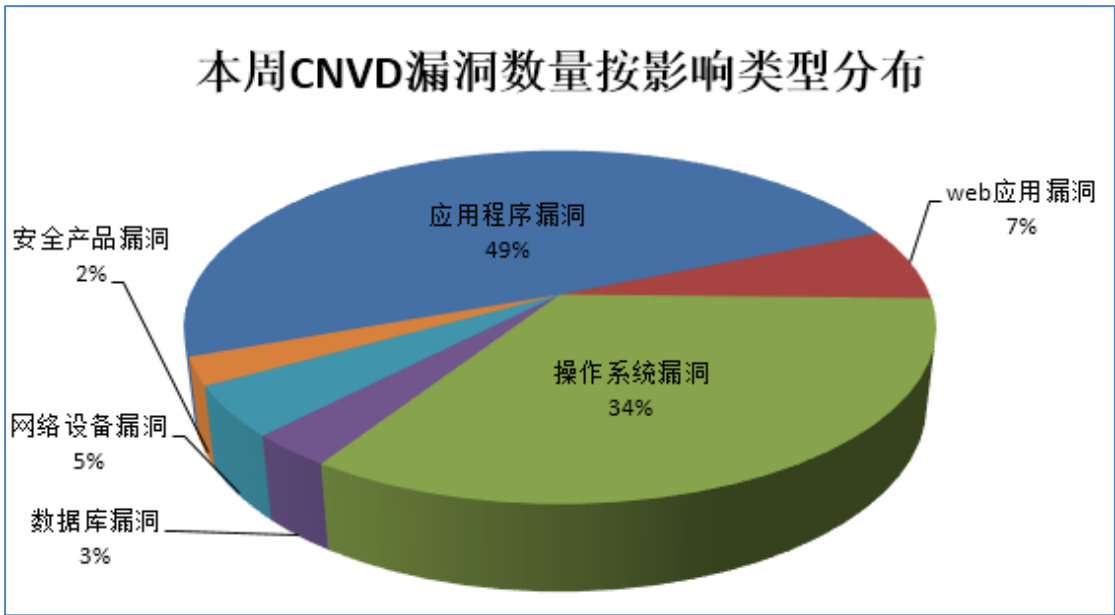


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 15 个电信行业漏洞，38 个移动互联网行业漏洞，4 个工控系统行业漏洞（如下图表所示）。其中，“IBM Tivoli Storage Manager FastBack 缓冲区溢出漏洞、IBM Tivoli Storage Manager 栈缓冲区溢出漏洞（CNVD-2015-02431）、IBM Tivoli Storage Manager (TSM) FastBack Mount Process 缓冲区溢出漏洞、Apple iOS 存在未明内存破坏漏洞、Apple iOS IOHIDFamily API 内存破坏漏洞、Apple iOS TCP

头处理拒绝服务漏洞、Apple iOS ICMP 用户重定向漏洞、Apple iOS 音频使用 IOKit 对象验证漏洞”的综合评级均为“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-2015-02383	Cisco ASR ASR9K 安全绕过漏洞	中	是
电信	CNVD-2015-02384	IBM Tivoli Storage Manager FastBack 缓冲区溢出漏洞	高	是
电信	CNVD-2015-02375	Juniper Networks Junos on SRX Series 存在未明漏洞	中	是
电信	CNVD-2015-02376	Juniper Junos 本地特权提升漏洞	中	是
电信	CNVD-2015-02392	Juniper Junos J-Web 点击劫持漏洞	中	是
电信	CNVD-2015-02391	Juniper Junos Dynamic VPN 跨站脚本漏洞	中	是
电信	CNVD-2015-02394	Asterisk Open Source/Certified Asterisk 证书校验漏洞	中	是
电信	CNVD-2015-02431	IBM Tivoli Storage Manager 栈缓冲区溢出漏洞 (CNVD-2015-02431)	高	是
电信	CNVD-2015-02473	Oracle MySQL Server 存在未明漏洞 (CNVD-2015-02473)	中	是
电信	CNVD-2015-02474	Oracle MySQL Server 存在未明漏洞 (CNVD-2015-02474)	中	是
电信	CNVD-2015-02475	Oracle MySQL Server 存在未明漏洞 (CNVD-2015-02475)	中	是
电信	CNVD-2015-02476	Oracle MySQL Server 存在未明漏洞 (CNVD-2015-02476)	中	是
电信	CNVD-2015-02477	Oracle MySQL Server 存在未明漏洞 (CNVD-2015-02477)	中	是
电信	CNVD-2015-02478	Oracle MySQL Server 存在未明漏洞 (CNVD-2015-02478)	中	是
电信	CNVD-2015-02499	IBM Tivoli Storage Manager (TSM) FastBack Mount Process 缓冲区溢出漏洞	高	是
移动互联网	CNVD-2015-02317	Apple iOS MobileFrameBuffer 内存泄露漏洞	中	是
移动互联网	CNVD-2015-02318	Apple iOS iWork 文件内存破坏漏洞	中	是
移动互联网	CNVD-2015-02319	Apple iOS 存在未明内存破坏漏洞	高	是
移动互联网	CNVD-2015-02320	Apple iOS QuickType 用户密码获取漏洞	低	是
移动互联网	CNVD-2015-02305	Apple iOS 沙盒绕过敏感信息泄露漏洞 (CNVD-2015-02305)	中	是
移动互联网	CNVD-2015-02306	Apple iOS 沙盒绕过敏感信息泄露漏洞 (CNVD-2015-02306)	中	是
移动互联网	CNVD-2015-02307	Apple iOS telephony 子系统访问控制漏洞	中	是

移动互联网	CNVD-2015-02316	Apple iOS 备份系统受限文件访问漏洞	低	是
移动互联网	CNVD-2015-02308	Apple iOS Task Switcher 敏感信息泄露漏洞	低	是
移动互联网	CNVD-2015-02315	Apple iOS 浏览历史不能删除漏洞	中	是
移动互联网	CNVD-2015-02314	Apple iOS NSXMLParser XML 处理信息泄露漏洞	中	是
移动互联网	CNVD-2015-02309	Apple iOS Webkit 点击劫持漏洞	中	是
移动互联网	CNVD-2015-02310	Apple iOS 字体处理文件内存破坏漏洞	中	是
移动互联网	CNVD-2015-02311	Apple iOS IOAcceleratorFamily 内核内存泄露漏洞	低	是
移动互联网	CNVD-2015-02312	Apple iOS IOHIDFamily API 内存破坏漏洞	高	是
移动互联网	CNVD-2015-02313	Apple iOS IOHIDFamily 内存泄露漏洞	低	是
移动互联网	CNVD-2015-02338	Apple iOS setreuid 调用拒绝服务漏洞	低	是
移动互联网	CNVD-2015-02333	Apple iOS 内存越界访问漏洞	中	是
移动互联网	CNVD-2015-02334	Apple iOS TCP 头处理拒绝服务漏洞	高	是
移动互联网	CNVD-2015-02335	Apple iOS ICMP 用户重定向漏洞	高	是
移动互联网	CNVD-2015-02336	Apple iOS 存在未明拒绝服务漏洞	中	是
移动互联网	CNVD-2015-02337	Apple iOS 音频使用 IOKit 对象验证漏洞	高	是
移动互联网	CNVD-2015-02321	Apple iOS 恶意配置文件内存破坏漏洞	中	是
移动互联网	CNVD-2015-02322	Apple iOS 安全绕过漏洞 (CNVD-2015-02322)	低	是
移动互联网	CNVD-2015-02323	Apple iOS 密码尝试安全绕过漏洞	低	是
移动互联网	CNVD-2015-02324	Apple iOS VPN 配置日志信息泄露漏洞	低	是
移动互联网	CNVD-2015-02331	Apple iOS Safari 历史记录泄露漏洞 (CNVD-2015-02331)	中	是
移动互联网	CNVD-2015-02332	Apple iOS Safari 历史记录泄露漏洞 (CNVD-2015-02332)	中	是
移动互联网	CNVD-2015-02327	Apple iOS Webkit 存在未明内存破坏漏洞 (CNVD-2015-02327)	中	是
移动互联网	CNVD-2015-02326	Apple iOS Webkit 存在未明内存破坏漏洞 (CNVD-2015-02326)	中	是
移动互联网	CNVD-2015-02325	Apple iOS Webkit 存在未明内存破坏漏洞 (CNVD-2015-02325)	中	是
移动互联网	CNVD-2015-02328	Apple iOS Webkit 存在未明内存破坏漏洞 (CNVD-2015-02328)	中	是
移动互联网	CNVD-2015-02329	Apple iOS Webkit 存在未明内存破坏漏洞 (CNVD-2015-02329)	中	是
移动互联网	CNVD-2015-02330	Apple iOS Webkit 存在未明内存破坏漏洞 (CNVD-2015-02330)	中	是
移动互联网	CNVD-2015-02340	Apple iOS 用户密码猜测漏洞	低	是
移动互联网	CNVD-2015-02339	Apple iOS setreuid 和 setregid 调用权限	中	是

		提升漏洞		
移动互联网	CNVD-2015-02353	Apple Mac OS X/iOS CFNetwork HTTPProtocol 跨域 COOKIE 泄露漏洞	中	是
移动互联网	CNVD-2015-02351	Apple Mac OS X/iOS URL 处理任意代码执行漏洞	中	是
工控系统	CNVD-2015-02364	Modicon M218 ModBus/TCP 流量攻击漏洞	中	否
工控系统	CNVD-2015-02363	Siemens SIMATIC WinCC 7.3 PN-DC P 缓冲区溢出漏洞	高	否
工控系统	CNVD-2015-02362	Schneider Modicon M340 Modbus/TCP "Write Multiple Registers 异常取值 DoS 攻击漏洞	高	否
工控系统	CNVD-2015-02365	罗克韦尔 FactoryTalk View RSlinx Classic 服务器进程的 EtherNet/IP 报文异常长度攻击漏洞	中	否

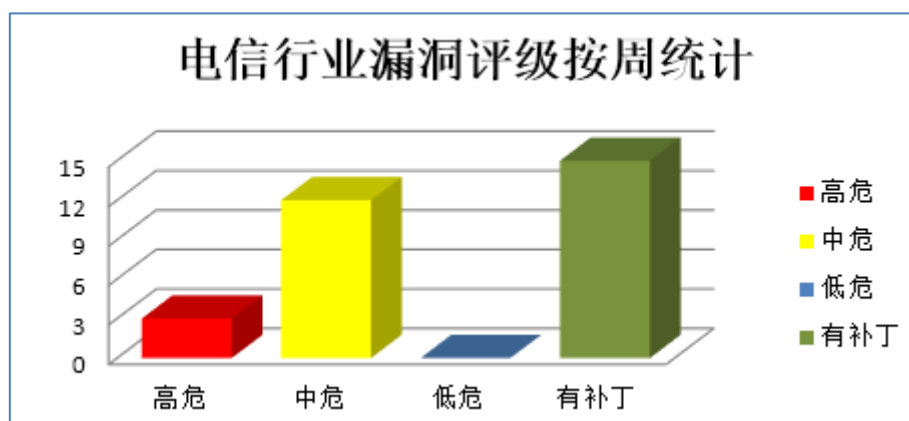


图 1 电信行业漏洞统计

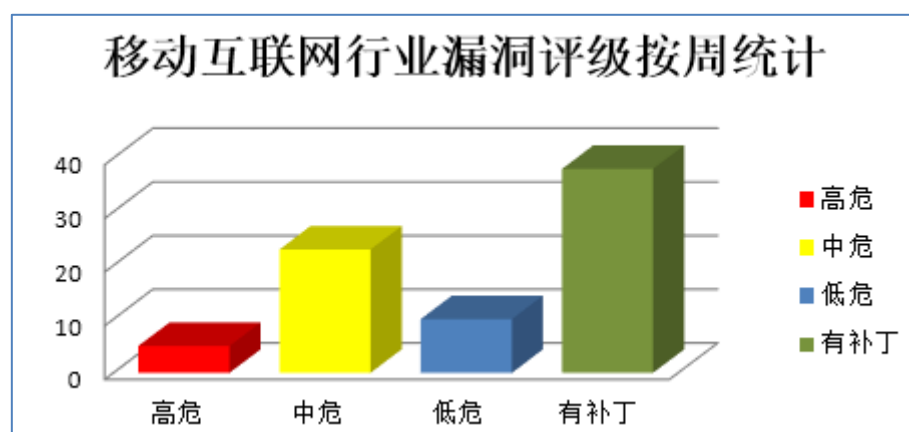


图 2 移动互联网系统行业漏洞统计

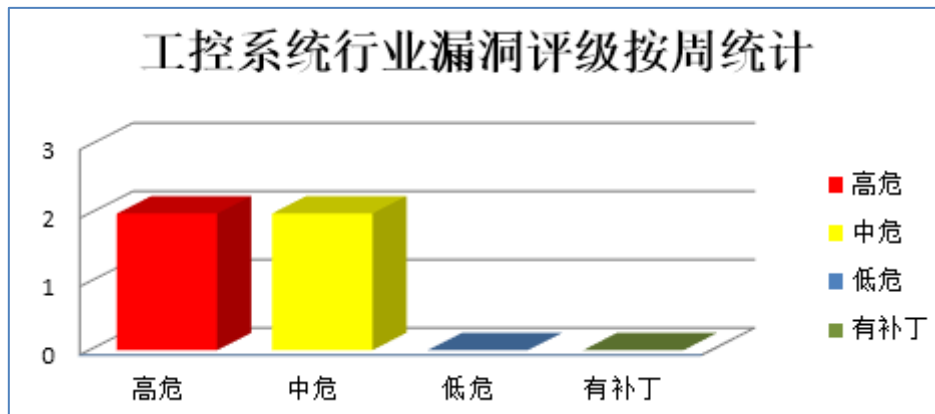


图3 工控系统行业漏洞统计

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

4月14日，微软发布了2015年4月份的月度例行安全公告，共含11项更新，修复了Microsoft Windows、Internet Explorer、Office、.NET Framework、Server 软件、Office Services 和 Web Apps 中存在的26个安全漏洞。其中，4项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，绕过安全功能限制，获得敏感信息，或拒绝服务攻击。在此例行安全公告中重点披露了一个HTTP.sys 远程代码执行漏洞，主要威胁到IIS服务器的安全。该漏洞存在于HTTP 协议堆栈(HTTP.sys) 中，攻击者可以在系统帐户的上下文中执行任意代码或提升权限。

CNVD 收录的相关漏洞包括：Microsoft IIS 远程代码执行漏洞、Microsoft Internet Explorer 内存破坏漏洞（CNVD-2015-02444、CNVD-2015-02445、CNVD-2015-02446、CNVD-2015-02447、CNVD-2015-02448、CNVD-2015-02449、CNVD-2015-02450）。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/webinfo/show/3612>

2、Oracle 产品安全漏洞

4月14日，Oracle 发布了2015年4月份的安全更新，修复了其多款产品存在的98个安全漏洞。受影响的产品包括Oracle 数据库、中间件产品Fusion Middleware、Java SE、MySQL 数据库等。本次安全更新提供了针对18个高危漏洞的补丁，有87个漏洞可被远程利用。

CNVD 收录的相关漏洞包括：Oracle Java SE 存在远程漏洞（CNVD-2015-02506、CNVD-2015-02507）、Oracle MySQL Server 存在未明漏洞（CNVD-2015-02478、CNVD

-2015-02477、CNVD-2015-02476、CNVD-2015-02475、CNVD-2015-02474、CNVD-2015-02473)。其中，“Oracle Java SE 存在远程漏洞（CNVD-2015-02506、CNVD-2015-02507）”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/webinfo/show/3613>

3、Adobe 产品安全漏洞

Adobe Flash Player 是美国奥多比（Adobe）公司的一款跨平台、基于浏览器的多媒体播放器产品。该产品支持跨屏幕和浏览器查看应用程序、内容和视频。本周，上述产品被披露存在内存破坏和内存错误引用漏洞。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：Adobe Flash Player 内存破坏漏洞（CNVD-2015-02492、CNVD-2015-02493、CNVD-2015-02494、CNVD-2015-02495、CNVD-2015-02496、CNVD-2015-02497）、Adobe Flash Player 内存错误引用漏洞（CNVD-2015-02491、CNVD-2015-02498）。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-2015-02492>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02493>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02494>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02495>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02496>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02497>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02491>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02498>

4、Apple 产品安全漏洞

Apple Mac OS X 是苹果公司开发的操作系统。本周，上述产品被披露存在任意代码执行、内存破坏、缓冲区溢出和内存错误引用漏洞。攻击者可利用漏洞提升权限。

CNVD 收录的相关漏洞包括：Apple Mac OS X fontd 任意代码执行漏洞（CNVD-2015-02345、CNVD-2015-02343、CNVD-2015-02344、CNVD-2015-02342、CNVD-2015-02341）、Apple Mac OS X CoreAnimation 内存错误引用漏洞、Apple Mac OS X .sgi 文件内存破坏漏洞、Apple Mac OS X IOHIDFamily 缓冲区溢出漏洞。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-2015-02345>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02343>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02344>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02342>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02341>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02350>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02302>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02303>

5、Barracuda Web 界面任意命令注入漏洞

Barracuda 是一款硬盘产品系列的总称。本周，Barracuda 被披露存在综合评级为“高危”的任意命令注入漏洞。攻击者利用该漏洞可在受影响设备上任意执行命令。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-2015-02430>

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-2015-02385	Novell ZenWorks Configuration Management 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： https://github.com/pedrib/PoC/blob/master/generic/zenworks_zcm_rce.txt
CNVD-2015-02381	BitTorrent Sync BTSync.exe 任意代码执行漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页： http://www.bittorrent.com/
CNVD-2015-02382	Moxa SoftCMS RTSPVIDEO.rtsp videoCtrl.1 ActiveX 栈缓冲区溢出漏洞	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://www.moxa.com/support/download.aspx?d_id=2114
CNVD-2015-02379	Red Hat openstack-puppet-modules 信任管理漏洞	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： https://rhn.redhat.com/errata/RHSA-2015-0789.html
CNVD-2015-02400	IBM Security SiteProtector System 本地权限提升漏洞	高	目前厂商已经发布升级补丁/版本以修复这个安全问题，请用户及时下载更新： http://www.ibm.com/us/en/
CNVD-2015-02420	MediaWiki 拒绝服务漏洞 (CNVD-2015-02420)	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： https://lists.wikimedia.org/pipermail/mediawiki-announce/2015-March/00

			0175.html
CNVD-2015-02419	MediaWiki 拒绝服务漏洞 (CNVD-2015-02419)	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： https://lists.wikimedia.org/pipermail/mediawiki-announce/2015-March/000175.html
CNVD-2015-02421	MediaWiki 拒绝服务漏洞 (CNVD-2015-02421)	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： https://lists.wikimedia.org/pipermail/mediawiki-announce/2015-March/000175.html
CNVD-2015-02456	WordPress 插件 All In One WP Security & Firewall admin/wp-security-list-login-fails.php SQL 注入漏洞	高	暂无
CNVD-2015-02455	WordPress 插件 All In One WP Security & Firewall admin/wp-security-list-acct-activity.php SQL 注入漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，微软发布了 2015 年 4 月份的月度例行安全公告，共含 11 项更新，修复了 Microsoft Windows、Internet Explorer、Office、.NET Framework、Server 软件、Office Services 和 Web Apps 中存在的 26 个安全漏洞。同时重点披露了 HTTP.sys 远程代码执行漏洞。4 月 14 日，Oracle 发布了 2015 年 4 月份的安全更新，修复了其多款产品存在的 98 个安全漏洞。此外，Adobe、Apple 多款产品被披露存在多个安全漏洞，允许攻击者利用漏洞获取敏感信息、执行任意代码、提升权限或发起拒绝服务攻击。另外，Barracuda 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设备上任意执行命令。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、Novell 修补 ZENworks Configuration Management 产品漏洞

Novell ZENworks Configuration Management 是 ZENworks 系统网关工具中的配置管理解决方案。

本周，Novell 修补了上述产品存在的远程代码执行漏洞，避免攻击者利用漏洞执行任意代码。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/57237>

本周要闻速递

1. Java 曝远程代码执行漏洞

继本月初 Java 官网曝本地文件包含 (LFI) 漏洞, 可读取超过 460 位 Oracle 公司员工邮箱之后。今天 Java 又曝一系列安全漏洞, Oracle 已发布补丁。攻击者可在未授权的情况下在受害者的 Java 应用上远程执行命令, 影响 5-8 版本的 JRE/JDK。强烈建议企业尽快更新它们的 Java Runtime Environments (JREs) 和 (Java Development Kits) JDKs。

参考链接: <http://www.freebuf.com/news/64305.html>

2. 苹果 iOS 及 Mac 系统存在漏洞, 可导致远程 DoS (拒绝式服务) 攻击

某研究人员在 Apple OS X 及 iOS 操作系统的开源组件 Darwin 内核中发现一个漏洞 Darwin Nuke。Darwin Nuke 漏洞可在处理一定大小的 IP 数据包并具有无效 IP 选项时被利用。远程攻击者可对 OS X 10.10 或 iOS 8 的设备发动 DoS 攻击, 向目标发送不正确的网络数据包。处理完无效网络数据包后, 系统将会崩溃。该漏洞会影响 Mac OS X 10.10 和 iOS 8, 但苹果已经在 iOS 8.3 和 Mac OS X 10.10.3 中进行了修复。研究人员建议所有 OS X 10.10 以及 iOS 8 的用户将设备更新至 OS X 10.10.3 及 iOS 8.3。

参考链接: <http://www.freebuf.com/news/63608.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