国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2015 年 12 月 14 日-2015 年 12 月 20 日　　2015 年第 51 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 227 个，其中高危漏洞 139 个、中危漏洞 83 个、低危漏洞 5 个。上述漏洞中，可利用来实施远程攻击的漏洞有 208 个。本周收录的漏洞中，已有 207 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“OPC Systems.NET 本地提权漏洞”、“ProFTPD 堆缓冲区溢出漏洞”等零日漏洞，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 227 个漏洞。报送情况如表 1 所示。其中，奇虎(补天平台)、安天实验室、绿盟科技、天融信等单位报送数量较多。补天平台、乌云、漏洞盒子及白帽子向 CNVD 提交了 1105 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(补天平台)	484	484
安天实验室	201	0
绿盟科技	199	0
天融信	150	0
启明星辰	132	0
恒安嘉新	27	0

H3C	3	0
乌云	577	577
漏洞盒子	4	4
High-Tech Bridge Security Research Lab	2	2
中国科学院信息工程研究所第六研究室	12	12
广州白狐网络科技有限公司	1	1
CNCERT 宁夏分中心	1	1
CNCERT 江西分中心	1	1
CNCERT 甘肃分中心	1	1
个人	22	22
报送总计	1817	1105
录入总计	227（去重）	1105

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Adobe、Apple、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	Adobe	80	35%
2	Apple	68	30%
3	Microsoft	20	9%
4	Huawei	8	4%
5	Cisco	5	2%
6	IBM	4	2%
7	Belkin	4	2%
8	Google	3	1%
9	Xerox	2	1%
10	其他	33	14%

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 227 个漏洞。其中应用程序漏洞 139 个，操作系统漏洞 63 个，网络设备漏洞 13 个，Web 应用漏洞 11 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	139
操作系统漏洞	63
网络设备漏洞	13
Web 应用漏洞	11
安全产品漏洞	1

表 3 漏洞按影响类型统计表

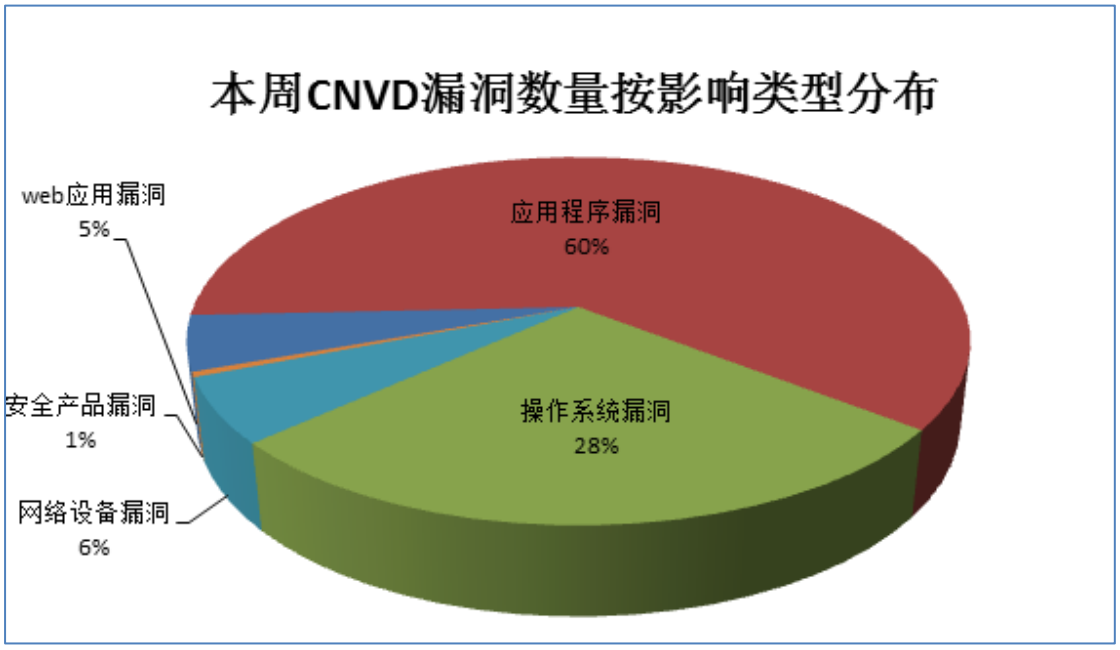

图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 6 个电信行业漏洞、51 个移动互联网行业漏洞（如下图表所示）。其中，“Apple OS X 媒体文件内存破坏漏洞、Apple OS X OKit 空指针引用任意代码执行漏洞、Apple OS X IOHIDFamily 内存破坏任意代码执行漏洞（CNVD-2015-08133）、Apple OS X IOHIDFamily 内存破坏任意代码执行漏洞、Apple OS X 内存破坏漏洞（CNVD-2015-08163、CNVD-2015-08162）、Apple OS X mach 消息处理任意代码执行漏洞、Apple iOS plists 处理内存破坏任意代码执行漏洞、Apple iOS trust cache 加载任意代码执行漏洞、Apple iOS 访问控制任意代码执行漏洞、Apple iOS Mobile Replayer 任意代码执行漏洞（CNVD-2015-08187）、Apple iOS Mobile Replayer 任意代码执行漏洞、Apple iOS dyld 任意代码执行漏洞、Apple iOS dyld 任意代码执行漏洞（CNVD-2015-08185）”

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-2015-08282	Cisco Linksys EA6100 和 EA6300 Routers 未授权访问漏洞	中	否
电信	CNVD-2015-08281	Buffalo AirStation Extreme N600 WZR-600DHP2 路由器安全绕过漏洞	中	否
电信	CNVD-2015-08301	Belkin N150 Wireless Home Router 跨站请求伪造漏洞	中	否
电信	CNVD-2015-08302	Belkin N150 Wireless Home Router HTML 注入漏洞	中	否
电信	CNVD-2015-08303	Belkin N150 Wireless Home Router 会话劫持漏洞	中	否
电信	CNVD-2015-08304	Belkin N150 Wireless Home Router 不安全默认密码漏	中	否
移动互联网	CNVD-2015-08072	Apple OS X 媒体文件内存破坏漏洞	高	是
移动互联网	CNVD-2015-08083	Apple Safari WebKit 内存破坏任意代码执行漏洞（CNVD-2015-08083）	中	是
移动互联网	CNVD-2015-08084	Apple Safari WebKit 内存破坏任意代码执行漏洞（CNVD-2015-08084）	中	是
移动互联网	CNVD-2015-08085	Apple Safari WebKit 内存破坏任意代码执行漏洞（CNVD-2015-08085）	中	是
移动互联网	CNVD-2015-08086	Apple Safari WebKit 内存破坏任意代码执行漏洞（CNVD-2015-08086）	中	是
移动互联网	CNVD-2015-08087	Apple Safari WebKit 内存破坏任意代码执行漏洞（CNVD-2015-08087）	中	是
移动互联网	CNVD-2015-08088	Apple Safari WebKit 内存破坏任意代码执行漏洞（CNVD-2015-08088）	中	是
移动互联网	CNVD-2015-08089	Apple Safari WebKit 内存破坏任意代码执行漏洞（CNVD-2015-08089）	中	是
移动互联网	CNVD-2015-08090	Apple Safari WebKit 内存破坏任意代码执行漏洞（CNVD-2015-08090）	中	是
移动互联网	CNVD-2015-08095	Google Android 信息泄露漏洞（CNVD-2015-08095）	中	是
移动互联网	CNVD-2015-08094	Android 任意代码执行漏洞（CNVD-2015-08094）	中	是
移动互联网	CNVD-2015-08091	Apple Safari WebKit 内存破坏任意代码执行漏洞（CNVD-2015-08091）	中	是
移动互联网	CNVD-2015-08092	Apple Safari WebKit 内存破坏任意代码执行漏洞（CNVD-2015-08092）	中	是
移动互联网	CNVD-2015-08093	Apple Safari WebKit 内存破坏任意代码执行漏洞（CNVD-2015-08093）	中	是
移动互联网	CNVD-2015-08127	Apple OS X iBooks 文件处理信息泄露漏	中	是

		洞		
移动互联网	CNVD-2015-08128	Apple OS X ImageIO 内存破坏任意代码执行漏洞	中	是
移动互联网	CNVD-2015-08130	Apple OS X OKit 空指针引用任意代码执行漏洞	高	是
移动互联网	CNVD-2015-08133	Apple OS X IOHIDFamily 内存破坏任意代码执行漏洞（CNVD-2015-08133）	高	是
移动互联网	CNVD-2015-08132	Apple OS X IOHIDFamily 内存破坏任意代码执行漏洞	高	是
移动互联网	CNVD-2015-08131	Apple OS X URL 验证绕过漏洞	低	是
移动互联网	CNVD-2015-08140	Apple OS X CoreGraphics 字体文件处理代码执行漏洞	中	是
移动互联网	CNVD-2015-08139	Apple OS X 媒体文件处理代码执行漏洞	中	是
移动互联网	CNVD-2015-08154	Apple OS X libc 缓冲区溢出任意代码执行漏洞（CNVD-2015-08154）	中	是
移动互联网	CNVD-2015-08153	Apple OS X libc 缓冲区溢出任意代码执行漏洞	中	是
移动互联网	CNVD-2015-08150	Apple OS X OpenGL 内存破坏任意代码执行漏洞（CNVD-2015-08150）	中	是
移动互联网	CNVD-2015-08151	Apple OS X OpenGL 内存破坏任意代码执行漏洞（CNVD-2015-08151）	中	是
移动互联网	CNVD-2015-08152	Apple OS X OpenGL 内存破坏任意代码执行漏洞	中	是
移动互联网	CNVD-2015-08147	Apple OS X iWork 文件任意代码执行漏洞	中	是
移动互联网	CNVD-2015-08146	Apple OS X ASLR 保护绕过漏洞	低	是
移动互联网	CNVD-2015-08143	Apple OS X SSL 握手内存破坏漏洞	中	是
移动互联网	CNVD-2015-08142	Apple OS X Keychain 项访问漏洞	中	是
移动互联网	CNVD-2015-08166	Apple OS X 拒绝服务漏洞（CNVD-2015-08166）	中	是
移动互联网	CNVD-2015-08165	Apple OS X 拒绝服务漏洞（CNVD-2015-08165）	中	是
移动互联网	CNVD-2015-08164	Apple OS X 拒绝服务漏洞（CNVD-2015-08164）	中	是
移动互联网	CNVD-2015-08163	Apple OS X 内存破坏漏洞（CNVD-2015-08163）	高	是
移动互联网	CNVD-2015-08162	Apple OS X 内存破坏漏洞（CNVD-2015-08162）	高	是
移动互联网	CNVD-2015-08161	Apple OS X mach 消息处理任意代码执行漏洞	高	是
移动互联网	CNVD-2015-08156	Apple OS X zlib 任意代码执行漏洞	中	是
移动互联网	CNVD-2015-08179	Cisco WebEx Meetings for Android 访问绕过漏洞	中	是

移动互联网	CNVD-2015-08176	Apple iOS plists 处理内存破坏任意代码执行漏洞	高	是
移动互联网	CNVD-2015-08170	Apple OS X 沙盒绕过漏洞（CNVD-2015-08170）	中	是
移动互联网	CNVD-2015-08167	Apple OS X 拒绝服务漏洞（CNVD-2015-08167）	中	是
移动互联网	CNVD-2015-08190	Apple iOS trust cache 加载任意代码执行漏洞	高	是
移动互联网	CNVD-2015-08188	Apple iOS 访问控制任意代码执行漏洞	高	是
移动互联网	CNVD-2015-08187	Apple iOS Mobile Replayer 任意代码执行漏洞（CNVD-2015-08187）	高	是
移动互联网	CNVD-2015-08186	Apple iOS Mobile Replayer 任意代码执行漏洞	高	是
移动互联网	CNVD-2015-08184	Apple iOS dyld 任意代码执行漏洞	高	是
移动互联网	CNVD-2015-08185	Apple iOS dyld 任意代码执行漏洞（CNVD-2015-08185）	高	是
移动互联网	CNVD-2015-08183	Apple iOS siri 安全绕过漏洞	低	是
移动互联网	CNVD-2015-08182	Apple iOS URL 伪造漏洞	中	是
移动互联网	CNVD-2015-08191	Apple iOS backup 系统路径校验漏洞	中	是

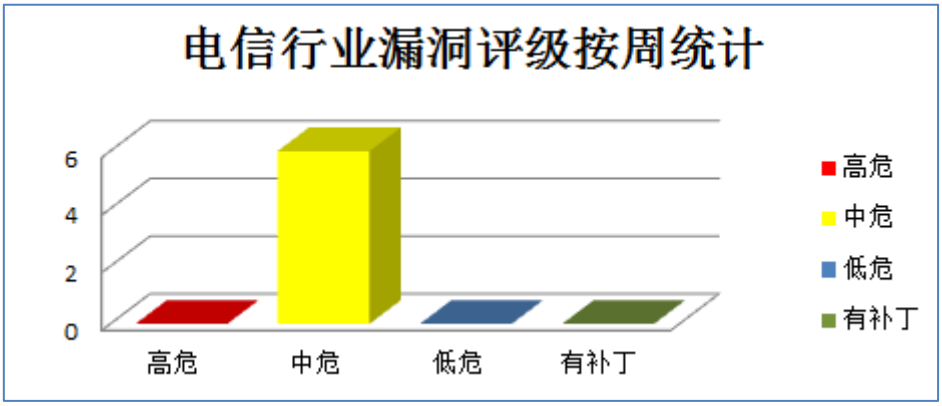

图 1 电信行业漏洞统计

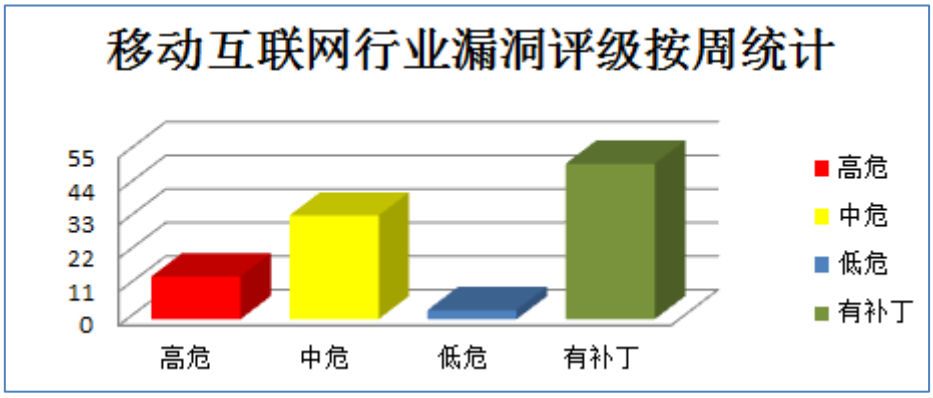

图 2 移动互联网行业漏洞统计

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、 MIT 产品安全漏洞

近日，CNVD 收录了 Kerberos 网络认证协议存在认证绕过漏洞（CNVD-2015-08300）。攻击者利用漏洞可借助 krbtgt 密码绕过身份验证系统，获取管理员访问权限，进而执行一系列管理员操作。

CNVD 收录的相关漏洞包括：Kerberos 网络认证协议存在认证绕过漏洞。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-2015-08300

2、 Adobe 产品安全漏洞

Adobe Flash Player 是一种广泛使用的、专有的多媒体程序播放器。它最初由 Macromedia 编写，在 Macromedia 被 Adobe 收购后由 Adobe 继续开发并分发。本周，上述产品被披露存在内存错误引用任意代码执行漏洞。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 内存错误引用任意代码执行漏洞（CNVD-2015-08249、CNVD-2015-08224、CNVD-2015-08223、CNVD-2015-08222、CNVD-2015-08221、CNVD-2015-08220、CNVD-2015-08219、CNVD-2015-08217）。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-2015-08249
http://www.cnvd.org.cn/flaw/show/CNVD-2015-08224
http://www.cnvd.org.cn/flaw/show/CNVD-2015-08223
http://www.cnvd.org.cn/flaw/show/CNVD-2015-08222
http://www.cnvd.org.cn/flaw/show/CNVD-2015-08221
http://www.cnvd.org.cn/flaw/show/CNVD-2015-08220
http://www.cnvd.org.cn/flaw/show/CNVD-2015-08219
http://www.cnvd.org.cn/flaw/show/CNVD-2015-08217

3、 Apple 产品安全漏洞

Apple Safari 是一款苹果公司开发的 WEB 浏览器。本周，上述产品被披露存在内存破坏任意代码执行漏洞。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 内存破坏任意代码执行漏洞（CNVD-2015-08093、CNVD-2015-08090、CNVD-2015-08091、CNVD-2015-08092、CNVD-2015-08087、CNVD-2015-08088、CNVD-2015-08089、CNVD-2015-08083）。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-2015-08093

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08090

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08091

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08092

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08087

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08088

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08089

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08083

4、Huawei 产品安全漏洞

Huawei LogCenter 是中国华为（Huawei）公司的一套日志管理软件。Huawei VCN500 是中国华为公司的一款一体化智能视频监控产品。Huawei FusionCompute 是中国华为公司的一套基于 Xen 开源设计的企业级开放式服务器虚拟化解决方案。该方案提供实现虚拟数据中心自动化、高级集成和管理功能。Huawei Video Content Management 是中国华为（Huawei）公司的一套视频内容管理系统。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敏感信息、提升权限、执行未授权访问和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Huawei LogCenter 权限提升漏洞、Huawei LogCenter 拒绝服务漏洞、Huawei VCN500 SQL 注入漏洞、Huawei VCN500 身份验证绕过漏洞、Huawei FusionCompute 信息泄露漏洞、Huawei Video Content Management 权限提升漏洞、Huawei VCN500 安全绕过漏洞、Huawei VCN500 拒绝服务漏洞。其中，“Huawei LogCenter 权限提升漏洞、Huawei VCN500 SQL 注入漏洞、Huawei Video Content Management 权限提升漏洞”的综合评级为“高”危。目前，厂商已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-2015-08283

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08284

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08193

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08192

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08199

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08198

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08196

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08195

5、TomatoCart 'json.php'任意文件上传漏洞

TomatoCart 是一套使用 PHP 开发的开源电子商务软件。该软件包含产品分类、产品评论、文章发布等模块。本周，TomatoCart 被披露存在任意文件上传漏洞。攻击者可利用该漏洞执行任意代码。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-2015-08291

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-2015-08100	Microsoft Internet Explorer 拒绝服务漏洞（CNVD-2015-08100）	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://technet.microsoft.com/security/bulletin/MS15-124
CNVD-2015-08099	Microsoft Internet Explorer 拒绝服务漏洞（CNVD-2015-08099）	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://technet.microsoft.com/security/bulletin/MS15-124
CNVD-2015-08096	Microsoft Internet Explorer 任意 web 脚本执行漏洞	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://technet.microsoft.com/security/bulletin/MS15-124
CNVD-2015-08097	Microsoft Internet Explorer 拒绝服务漏洞（CNVD-2015-08097）	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://technet.microsoft.com/security/bulletin/MS15-124
CNVD-2015-08108	Foxit PhantomPDF Print 内存错误引用漏洞	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://www.foxitsoftware.com/support/security-bulletins.php#FRD-36
CNVD-2015-08107	Foxit PhantomPDF App 内存错误引用漏洞	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://www.foxitsoftware.com/support/security-bulletins.php#FRD-36
CNVD-2015-08124	Adobe Flash Player 栈溢出任意代码执行漏洞（CNVD-2015-08124）	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://helpx.adobe.com/security/products/flash-player/apsb15-32.html
CNVD-2015-08123	Adobe Flash Player 整数溢出任意代码执行漏洞（CNVD-2015-08123）	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://helpx.adobe.com/security/products/flash-player/apsb15-32.html
CNVD-2015-08122	Adobe Flash Player 缓冲区溢出任意代码执行漏洞	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：https://helpx.adobe.com/security/products/flash-player/apsb15-32.html

CNVD-2015-08138	IBM Tivoli Storage Manager for Virtual Environments 命令执行漏洞	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://www.ibm.com/

表 3 部分高危漏洞列表

小结：本周，CNVD 收录了 Kerberos 网络认证协议存在认证绕过漏洞。攻击者利用漏洞可借助 krbtgt 密码绕过身份验证系统，获取管理员访问权限，进而执行一系列管理员操作。此外，Adobe、Apple、Huawei 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、执行未授权访问、提升权限、执行任意代码和发起拒绝服务攻击等。另外，TomatoCart 被披露存在一个高危漏洞，攻击者可利用该漏洞执行任意代码。建议相关用户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、ZOHO 修补 ManageEngine Firewall Analyzer 产品漏洞

ZOHO ManageEngine Firewall Analyzer 是一套基于 Web 的防火墙日志分析工具，它能收集、关联分析和汇报整个企业范围内的防火墙、proxy 伺服器和 Radius 伺服器上的日志。

本周，ZOHO 修补了上述产品存在的目录遍历和安全绕过漏洞，避将攻击者利用漏洞查看系统文件和执行未授权访问。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/68152

http://www.cnvd.org.cn/patchInfo/show/68151

本周要闻速递

1. 安全研究员发现 Instagram 漏洞

一位独立安全研究人员发现了一个远程代码执行漏洞，该漏洞存在于 Instagram 处理用户会话 cookie 的方式中，这些 cookie 通常用来记住用户的登录细节。利用该漏洞，Weinberg 能够迫使服务器吐出一个数据库，其中包含登录细节，包括 Instagram 和 Face book 员工的凭证。虽然这些密码以“bcrypt”进行了加密，但 Weinberg 能够在几分钟内破解大量弱密码（例如 changeme、instagram、password）。

参考链接：http://www.freebuf.com/news/90345.html

2. Juniper Networks（瞻博网络）现后门，可解密 VPN 流量

Juniper 高级副总裁兼首席信息安全官 Bob Worrall 称，在最近的内部代码审计过程中发现了两枚漏洞。其中一个是未授权代码漏洞，可解密 VPN 流量；另外一个可允许

攻击者通过 SSH 或者 telnet 远程管理访问设备。Juniper 提到这些系统的访问会被记录，密码认证也会成功，但是攻击者可改变或者删除日志条目。影响 ScreenOS 6.2.0r15—6.2.0r18，6.3.0r12—6.3.0r20 版本。

参考链接：http://www.freebuf.com/news/90323.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