

信息安全漏洞周报

2014 年 10 月 13 日-2014 年 10 月 19 日

2014 年第 42 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 308 个，其中高危漏洞 75 个、中危漏洞 216 个、低危漏洞 17 个。上述漏洞中，可利用来实施远程攻击的漏洞有 291 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。本周互联网上出现“WordPress 插件 Users Ultra 'view'参数 SQL 注入漏洞”、“Bacula-web 'joblogs.php' SQL 注入漏洞”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 5 家成员单位、合作伙伴及个人报送了本周收录的全部 308 个漏洞。报送情况如表 1 所示。其中，奇虎 360、安天实验室、启明星辰、恒安嘉新等单位报送数量较多。此外，CNCERT 各分中心、及白帽子向 CNVD 提交了 304 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
奇虎 360	281	281
安天实验室	224	0
启明星辰	224	0
恒安嘉新	66	0
绿盟科技	43	
High-Tech Bridge Security Research Lab	2	2

CNCERT 上海分中心	7	7
CNCERT 江西分中心	4	4
CNCERT 山西分中心	2	2
CNCERT 福建分中心	2	2
CNCERT 河南分中心	2	2
个人	4	4
报送总计	861	304
录入总计	308（去重）	304

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Cisco、Microsoft、Oracle 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	Cisco	22	7%
2	Microsoft	22	7%
3	Oracle	21	7%
4	IBM	18	6%
5	WordPress	9	3%
6	Jenkins	7	2%
7	Mozilla	6	2%
8	Adobe	6	2%
9	NeuroML	4	1%
10	其他	193	63%

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 308 个漏洞。其中应用程序漏洞 240 个，WEB 应用漏洞 32 个，安全产品漏洞 15 个，操作系统漏洞 7 个，网络设备漏洞 7 个，数据库漏洞 7 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	240
WEB 应用漏洞	32

安全产品漏洞	15
操作系统漏洞	7
网络设备漏洞	7
数据库漏洞	7

表 3 漏洞按影响类型统计表

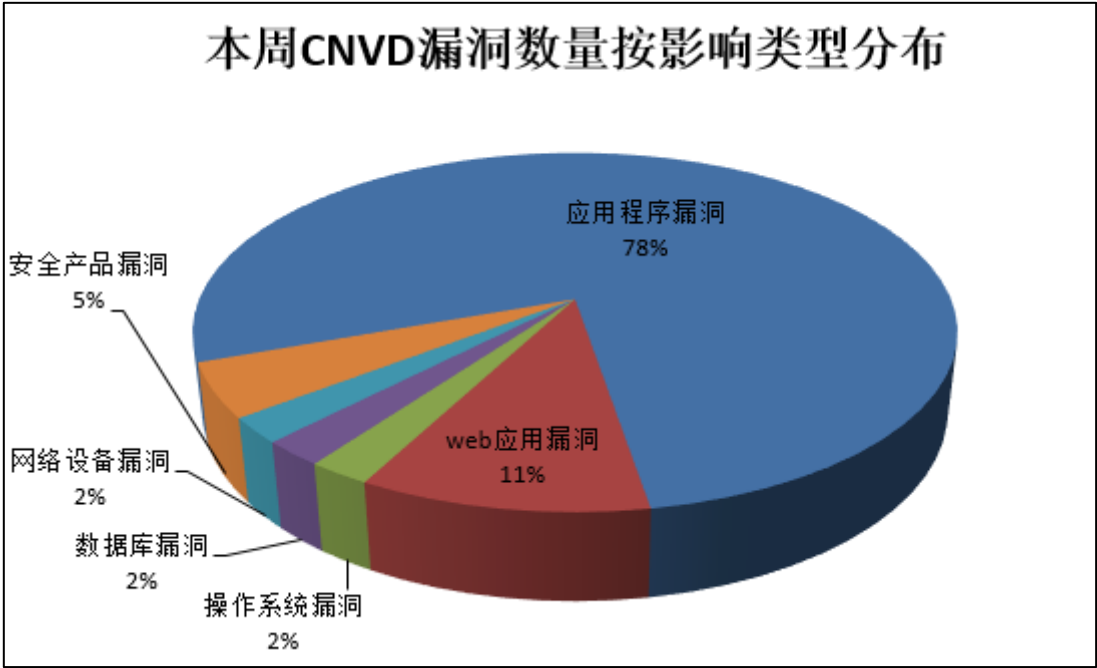


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 22 个电信行业漏洞，104 个移动互联网漏洞，2 个工控系统漏洞（如下图表所示）。其中，“Oracle Database Server 远程代码执行漏洞、Google Android API WebView 组件远程代码执行漏洞、Rockwell Micrologix 1400 DNP3 拒绝服务漏洞、HP Network Automati 安全绕过漏洞”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-2014-06654	Cisco IOS XE Software 存在未明漏洞	中	否
电信	CNVD-2014-06655	Cisco IOS XE 证书验证安全绕过漏洞（CNVD-2014-06655）	中	否
电信	CNVD-2014-06656	Cisco IOS XE 证书验证安全绕过漏洞（CNVD-2014-06656）	中	否
电信	CNVD-2014-06681	Draytek Vigor 2130 Router 存在多个漏洞	高	否
电信	CNVD-2014-06726	IBM Directory Server 存在多个未明跨站脚本漏洞	中	是

电信	CNVD-2014-06791	IBM WebSphere MQ 验证绕过漏洞	中	是
电信	CNVD-2014-06779	Oracle MySQL Server 远程漏洞 (CNVD-2014-06779)	中	是
电信	CNVD-2014-06778	Oracle MySQL Server 远程漏洞 (CNVD-2014-06778)	低	是
电信	CNVD-2014-06777	Oracle MySQL Server 远程漏洞 (CNVD-2014-06777)	中	是
电信	CNVD-2014-06795	Oracle Database Server 存在远程漏洞 (CNVD-2014-06795)	中	是
电信	CNVD-2014-06796	Oracle Database Server 远程代码执行漏洞	高	是
电信	CNVD-2014-06815	IBM WebSphere MQ 安全绕过漏洞 (CNVD-2014-06815)	低	是
电信	CNVD-2014-06816	IBM Maximo Asset Management 信息泄露漏洞 (CNVD-2014-06816)	中	是
电信	CNVD-2014-06817	IBM Tivoli Federated Identity Manager 开放重定向漏洞	中	是
电信	CNVD-2014-06818	IBM WebSphere DataPower XC10 Appliance 本地信息泄露漏洞	低	是
电信	CNVD-2014-06819	IBM WebSphere DataPower XC10 Appliance 本地信息泄露漏洞 (CNVD-2014-06819)	低	是
电信	CNVD-2014-06830	IBM Security Access Manager 存在未明跨站脚本漏洞	中	是
电信	CNVD-2014-06826	Linksys EA6500 跨站脚本漏洞	低	否
电信	CNVD-2014-06827	Linksys EA6500 开放重定向漏洞	中	否
电信	CNVD-2014-06876	Oracle MySQL Server CLIENT:MYSQ LADMIN 子件存在未明漏洞	低	是
电信	CNVD-2014-06898	IBM WebSphere MQ 本地信息泄露漏洞	低	是
电信	CNVD-2014-06915	Huawei E5332 Router API 服务请求消息处理拒绝服务漏洞	中	是
移动互联网	CNVD-2014-06664	Pharmaguideline for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06663	Pesca de Carpa Lite for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06662	Kayak Angler Magazine for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06698	Google Android API WebView 组件远程代码执行漏洞	高	是
移动互联网	CNVD-2014-06728	Google Android Browser 同源策略安全绕过漏洞	中	是
移动互联网	CNVD-2014-06723	mksh 'mksh/var.c'存在未明漏洞	中	是

移动互联网	CNVD-2014-06807	CIH Quiz Game for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06806	United Educational CU for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06808	Reddit Aww for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06838	Daily Advertiser Print application for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06842	Instaroid - Instagram Viewer for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06841	Hippo Studio for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06839	kuailecaidengmi app for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06837	Nerdico App for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06836	AZ fan for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06835	Amebra Ameba app for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06833	Lapp Group Catalogue for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06840	My T-Mobile @7F0C0030 for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06834	Westpac Mobile Banking for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06844	Four Seasons Beverly Hills application for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06845	MediaFire application for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06846	ABC Song application for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06847	Sweatshop application for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06850	RTI INDIA application for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06853	My Wedding Planner application for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06854	Alma Corinthiana application for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06857	Groupamatoujours la application for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06856	Hillside application for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06849	AuctionTrac Dealer for Android SSL 信	中	否

		息泄露漏洞		
移动互联网	CNVD-2014-06848	Bersa Forum for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06858	DK ONLINE Beta for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06855	Tic-Tac To MAX FREE for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06851	Teatro Franco Parenti for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06852	kamkomesan app for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06860	SDN Forum application for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06859	Melodigram for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06863	Vodafone AvantajCepte for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06862	EXPRESS for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06861	Ocean Avenue Mobile Pro for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06884	Jazeera Airways for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06897	Fermononrespiri Mobile App for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06896	United Advantage NW Federal Cr for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06894	Light for Pets applicationn for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06895	USEK Application for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06893	United Heritage Mobile application for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06888	Aerospace Jobs application for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06889	MeteoBelgique application for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06890	Anywhere Anytime Yoga Workout Application for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06891	Juggle! FREE application for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06892	Afro-Beat application for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06899	Harem Thief Dating application for An	中	否

		droid SSL 信息泄露漏洞		
移动互联网	CNVD-2014-06887	Downton Abbey Fan Portal application for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06883	Qin Story application for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06886	Mikeius (Official App) for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06885	30A for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06900	Campus Link - Campus TV, HKUSU for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06901	Abraham Tours for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06902	Aloha Stadium - Hawaii for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06903	MeiTalk App for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06904	Cart App for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06905	Goat Forum for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06910	ModSim Connected for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06912	AMGC for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06913	TTNET Müzik for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06911	Hogs Fly Crazy for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06914	EPL Hat Trick for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06924	Steyr Forum for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06931	Pushpins Grocery Coupons for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06922	Terrarienbilder.com Forum for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06921	Trial Tracker for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06920	Daum Maps - Subway for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06919	MostafaShemeas App for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06918	Car Wallpapers HD for Android SSL 信息泄露漏洞	中	否

移动互联网	CNVD-2014-06917	AHRAH for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06916	Long app for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06925	New Beginnings CFC application for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06926	SED Account application for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06927	DS file application for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06928	Horoscopes Dreams application for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06923	DS photo+ for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06930	Imagine Next Bmobile for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06929	Wine Making for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06932	kalahari.com Shopping App for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06933	CouponCabin - Coupons and Deals for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06934	GunBroker.com for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06935	PennyTalk Mobile for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06939	HomeAdvisor Mobile for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06938	Forest River Forums for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06937	ArtAccés for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06943	EyeXam for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06942	FoxitMobilePDF - PDF Reader for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06941	LedLine.gr (Official App) for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06944	Cove application for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06945	WISDOM application for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06946	Vouch! application for Android SSL 信息泄露漏洞	中	否

移动互联网	CNVD-2014-06947	Sentinels Randomizer application for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06940	ThinkPal for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06954	OHBM 20th Annual Meeting for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06948	klassens application for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06949	Aloha Guide for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06950	RIMS application for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06953	LocalSense for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06952	Alfa-Bank for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06951	Grilling with Rich for Android 信息泄露漏洞	中	否
工控系统	CNVD-2014-06674	Rockwell Micrologix 1400 DNP3 拒绝服务漏洞	高	是
工控系统	CNVD-2014-06689	HP Network Automati 安全绕过漏洞	高	是

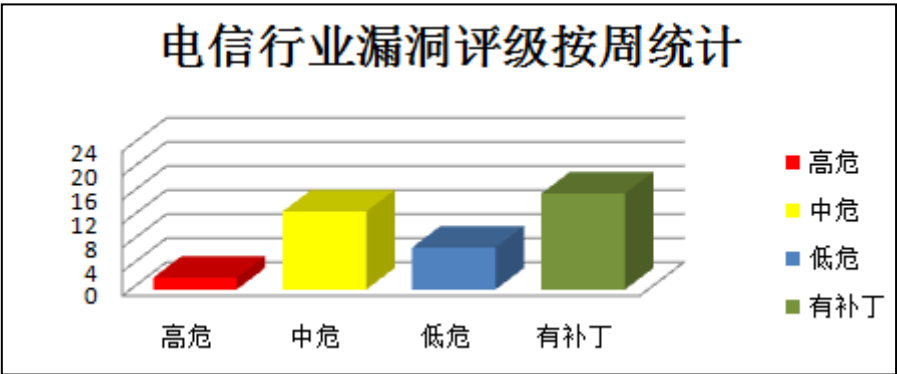


图 1 电信行业漏洞统计

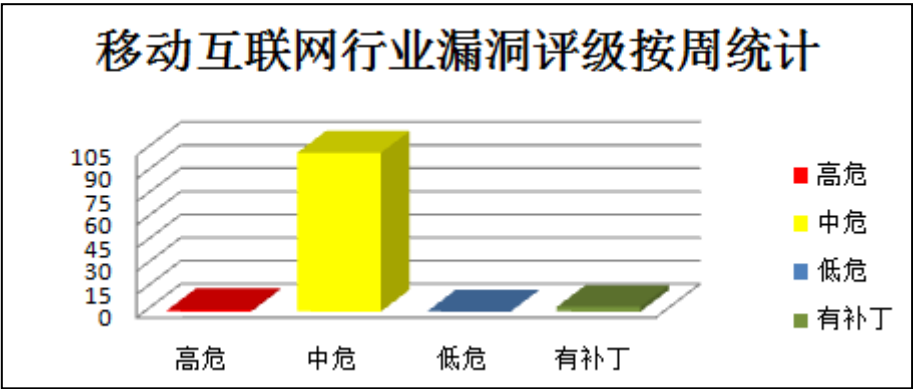


图 2 移动互联网行业漏洞统计

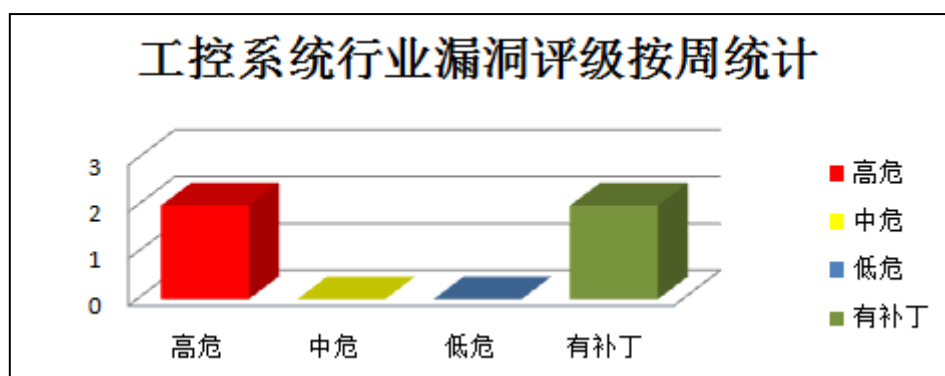


图 3 工控系统行业漏洞统计

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、SSL V3 Protocol 产品安全漏洞

10 月 15 日，CNVD 收录了 SSL V3 协议存在的一个可导致信息泄露的高危漏洞（CNVD-2014-06718，对应 CVE-2014-3566）。攻击者可利用漏洞发起远程攻击，窃取采用 sslv3 加密通信过程中的内容，构成信息泄露安全风险。

CNVD 收录的相关漏洞包括：SSL V3 Protocol 信息泄露漏洞。上述漏洞的综合评级为“高危”。目前厂商暂时没有提供升级补丁。

参考链接：<http://www.cnvd.org.cn/webinfo/show/3518>

2、Microsoft 产品安全漏洞

10 月 15 日，CNVD 收录了最新披露的 Windows OLE 远程代码执行漏洞（CNVD-2014-06717，对应 CVE-2014-4114）。攻击者可通过精心构造包含文件，并诱使用户执行文件触发远程代码执行漏洞，进而控制用户操作系统主机。此外，10 月 15 日，微软发布了 2014 年 10 月份的月度例行安全公告，共含 8 项更新，修复了 Microsoft Windows、Internet Explorer、.NET Framework、ASP.NET MVC、Office、Office Services 和 Web Apps 中存在的 24 个安全漏洞。其中，3 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。

CNVD 收录的相关漏洞包括：Microsoft Windows OLE 包管理器远程代码执行漏洞、Microsoft Internet Explorer 存在未明内存破坏漏洞（CNVD-2014-06867、CNVD-2014-06864、CNVD-2014-06866、CNVD-2014-06865、CNVD-2014-06868、CNVD-2014-06869、CNVD-2014-06870）。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/3517>

<http://www.cnvd.org.cn/webinfo/show/3515>

3、Oracle 产品安全漏洞

10月14日，Oracle 发布了2014年10月份的安全更新，修复了其多款产品存在的154个安全漏洞。受影响的产品包括 Oracle 数据库（31个）、中间件产品 Fusion Middleware（18个）；电子商务套装软件 Oracle E-Business Suite（10个）、供应链套装软件 Oracle Supply Chain Products Suite（5个）、企业管理器网格控制产品 Oracle Enterprise Manager Grid Control（2个）；Virtualization（7个）、PeopleSoft 产品（5个）、Primavera 产品（2个）、JD Edwards 产品（1个）、Retail Applications（4个）、Health Sciences Applications（3个）、Communications Applications（2个）、Java SE（25个）、Oracle Sun 系统产品（15个）和 MySQL 数据库（24个）。本次安全更新提供了针对32个高危漏洞的补丁，有138个漏洞可被远程利用。

CNVD 收录的相关漏洞包括：Oracle Database Server 远程代码执行漏洞、Oracle Java SE/Java SE Embedded AWT 子件存在未明远程代码执行漏洞、Oracle Java SE 存在远程漏洞（CNVD-2014-06751）、Oracle Supply Chain Products Suite 存在远程漏洞（CNVD-2014-06810、CNVD-2014-06811、CNVD-2014-06812）、Oracle Java SE/Java SE Embedded/JRockit Libraries 子件存在未明漏洞、Oracle PeopleSoft Products 存在远程漏洞（CNVD-2014-06802）。其中“Oracle Database Server 远程代码执行漏洞、Oracle Java SE/Java SE Embedded AWT 子件存在未明远程代码执行漏洞、Oracle Java SE 存在远程漏洞（CNVD-2014-06751）”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/webinfo/show/3516>

4、Cisco 产品安全漏洞

Cisco Adaptive Security Appliance 是一款自适应安全设备，可提供安全和 VPN 服务的模块。本周，上述产品被披露存在拒绝服务和信息泄露漏洞，攻击者可利用漏洞获取敏感信息或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco ASA Software 拒绝服务漏洞（CNVD-2014-06771、CNVD-2014-06770、CNVD-2014-06768、CNVD-2014-06769、CNVD-2014-06767、CNVD-2014-06766、CNVD-2014-06765）、Cisco ASA Software 信息泄露漏洞（CNVD-2014-06764）。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-2014-06771>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06770>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06768>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06769>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06767>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06766>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06765>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06764>

5、vBulletin 'breadcrumbs_create.php' SQL 注入漏洞

vBulletin 是款论坛程序套件。本周，vBulletin 被披露存在综合评级为“高危”的 SQL 注入漏洞。攻击者可利用漏洞危及应用程序，访问或修改数据。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-2014-06792>

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-2014-06742	Sophos Cyberoam 'add_guest_user' SQL 注入漏洞	高	请安装厂商已发布的最新版本或补丁： http://kb.cyberoam.com/default.asp?id=3049
CNVD-2014-06743	Sophos Cyberoam 远程代码执行漏洞	高	请安装厂商已发布的最新版本或补丁： http://kb.cyberoam.com/default.asp?id=3049
CNVD-2014-06744	Sophos Cyberoam 堆栈缓冲区溢出漏洞	高	请安装厂商已发布的最新版本或补丁： http://kb.cyberoam.com/default.asp?id=3049
CNVD-2014-06788	Mozilla Firefox/Thunderbird 内存错误引用内存破坏漏洞	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.mozilla.org/en-US/ https://www.mozilla.org/zh-CN/thunderbird/
CNVD-2014-06786	Mozilla Firefox/Thunderbird 越界内存破坏漏洞（CNVD-2014-06786）	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.mozilla.org/en-US/ https://www.mozilla.org/zh-CN/thunderbird/
CNVD-2014-06784	Mozilla Firefox/Thunderbird 存在多个内存破坏漏洞（CNVD-2014-06784）	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.mozilla.org/en-US/ https://www.mozilla.org/zh-CN/thunderbird/

CNVD-2014-06782	Adobe Flash Player / AIR 存在未明内存破坏漏洞 (CNVD-2014-06782)	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.adobe.com/products/air.html
CNVD-2014-06781	Adobe Flash Player / AIR 存在未明整数溢出漏洞	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.adobe.com/products/air.html
CNVD-2014-06780	Adobe Flash Player / AIR 存在未明内存破坏漏洞 (CNVD-2014-06780)	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.adobe.com/products/air.html
CNVD-2014-06738	Joomla! CMS SQL 注入漏洞	高	请安装厂商已发布的最新版本或补丁： http://developer.joomla.org/security/578-20140301-core-sql-injection.html

表 3 部分高危漏洞列表

小结：本周，移动互联网行业漏洞数相对较多，主要原因是收录了多个 Android 应用程序存在的 SSL 证书验证漏洞，攻击者可利用漏洞获取敏感信息，请各应用软件方注意防范 Android SSL 证书验证漏洞。10 月 14 日，Oracle 发布了 2014 年 10 月份的安全更新，修复了其多款产品存在的 154 个安全漏洞。10 月 15 日，微软发布了 2014 年 10 月份的月度例行安全公告，共含 8 项更新，修复了 Microsoft Windows、Internet Explorer、.NET Framework 等存在的 24 个安全漏洞，同时，CNVD 收录了 Windows OLE 远程代码执行漏洞及 SSL V3 信息泄露漏洞。此外，Cisco 多款产品被批露存在拒绝服务和信息泄露漏洞，允许攻击者利用漏洞执行代码、提升权限、获取敏感信息或发起拒绝服务攻击。另外，vBulletin 被披露存在一个高危零日漏洞。攻击者可利用漏洞危及应用程序，访问或修改数据。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、Huawei 修补 E5332 Router 产品漏洞

Huawei E5332 Router 是中国华为(Huawei)公司的一款联通 3G 无线路由器产品。

本周，Huawei 修补了上述产品存在拒绝服务漏洞，避免攻击者利用漏洞通过构建一个 API 服务请求的参数发起拒绝服务攻击。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/51019>

本周要闻速递

1. 国内 iCloud 服务器遭遇中间人攻击，对中国苹果用户隐私构成威胁

iCloud.com 有多个 IP，当使用国内 IP 直接访问国外 IP 时，访问的目标证书会被替换为自签名的证书，这意味着用户访问到的 iCloud 服务器不是真正的 iCloud 服务器，存在帐号信息被第三方获取的风险，换句话说 iCloud 服务器在中国可被利用发起 SSL 中间人攻击，导致中国苹果用户隐私泄露。

参考链接：<http://www.freebuf.com/news/47744.html>

2. 苹果发布 114 个安全补丁修复 Mountain Lion、iTunes 等漏洞

10 月 19 日国际报道：当地时间周四，除发布 OSX10.10Yosemite 外，苹果还发布了其他一些软件更新，其中大部分为安全补丁。这些安全补丁针对 OSXMMountainLionv10.8.5、OSXMavericksv10.9.5、OSXServerversions2.2.5 版本和 3.3.2 版本以及 4.0 以及 iTunes12.0.1。并预计 10 月 20 日发布 iOS8.1 系统时一并发布这些安全补丁，而其中一些补丁将被嵌入到新发布的 Yosemite 系统和 iOS 系统当中。其中 Yosemite 系统包含了 45 个安全补丁，包括 9 月末单独发布的 Shellshock 漏洞补丁。同时还包括 SSL3 协议设计上的 POODLE 漏洞等。此外还包括一些旨在封堵允许获得特权、执行任意代码的漏洞补丁。

参考链接：<http://www.shuland.com/roll/times/2014-10-19/28526.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