

信息安全漏洞周报

2015 年 10 月 12 日-2015 年 10 月 18 日

2015 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 206 个，其中高危漏洞 84 个、中危漏洞 103 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 170 个。本周收录的漏洞中，已有 192 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“BisonWare BisonFTP 信息泄露漏洞”、“PCMan FTP Server 信息泄露漏洞”等零日代码攻击，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 6 家成员单位、合作伙伴及个人报送了本周收录的全部 206 个漏洞。报送情况如表 1 所示。其中，乌云、奇虎(补天平台)、天融信、启明星辰、安天实验室等单位报送数量较多。此外，漏洞盒子、腾讯玄武实验室及白帽子向 CNVD 提交了 782 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
乌云	343	343
奇虎(补天平台)	314	314
漏洞盒子	26	26
天融信	173	0
启明星辰	144	5
安天实验室	120	0

绿盟科技	21	0
腾讯玄武实验室	6	6
CNCERT 宁夏分中心	1	1
个人	87	87
报送总计	1235	782
录入总计	206（去重）	782

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Google、Apple、Cisco 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	Google	52	25%
2	Apple	28	14%
3	Cisco	19	9%
4	IBM	10	5%
5	Refbase	8	4%
6	WordPress	6	3%
7	Microsoft	4	2%
8	EMC	3	1%
9	Schneider Electric	2	1%
10	其他	74	36%

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 206 个漏洞。其中应用程序漏洞 105 个，操作系统漏洞 74 个，Web 应用漏洞 15 个，网络设备漏洞 6 个，安全产品漏洞 3 个，数据库漏洞 3 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	105
操作系统漏洞	74
Web 应用漏洞	15
网络设备漏洞	6
安全产品漏洞	3

数据库漏洞	3
-------	---

表 3 漏洞按影响类型统计表

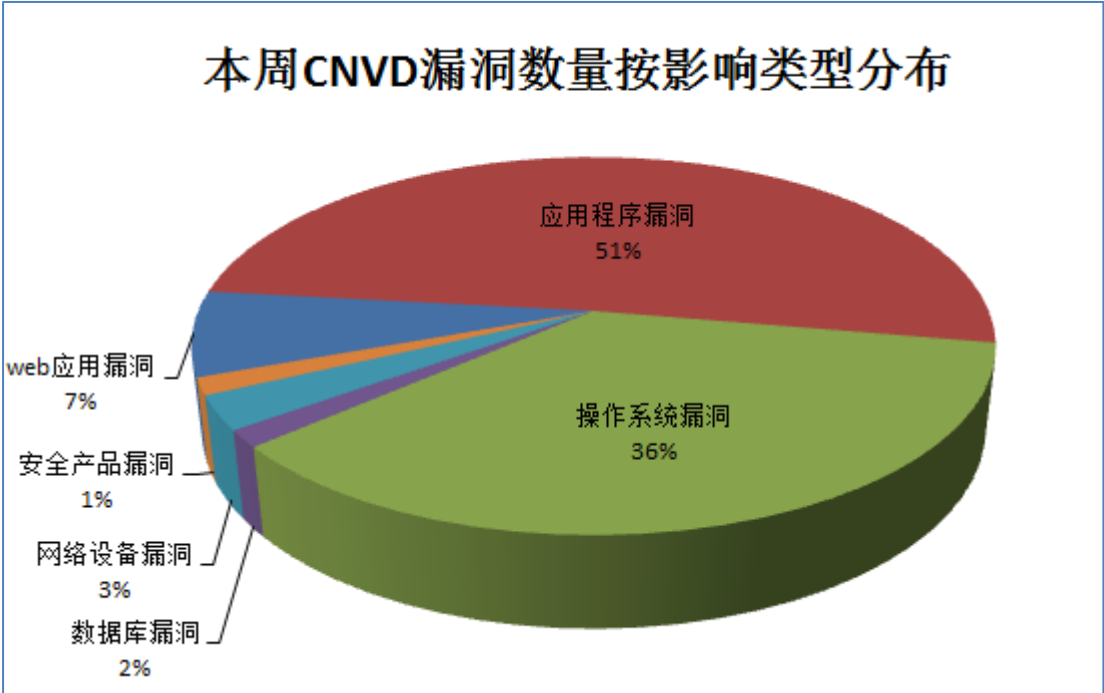


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 12 个电信行业漏洞、48 个移动互联网行业漏洞、3 个工系统行业漏洞（如下图表所示）。其中，“PostgreSQL 内存读取漏洞、PostgreSQL json 或 jsonb 数据拒绝服务漏洞、Android 任意代码执行漏洞、Android 缓冲区溢出漏洞、Android 整数溢出漏洞（CNVD-2015-06524、CNVD-2015-06604）、Android 任意代码执行漏洞（CNVD-2015-06534、CNVD-2015-06577、CNVD-2015-06514）、Android 权限提升漏洞（CNVD-2015-06566、CNVD-2015-06567、CNVD-2015-06568、CNVD-2015-06569、CNVD-2015-06578）、Android 安全限制绕过漏洞（CNVD-2015-06575）、Android 拒绝服务漏洞（CNVD-2015-06580、CNVD-2015-06589、CNVD-2015-06588、CNVD-2015-06587、CNVD-2015-06586、CNVD-2015-06585、CNVD-2015-06584、CNVD-2015-06583、CNVD-2015-06582、CNVD-2015-06581、CNVD-2015-06592、CNVD-2015-06591、CNVD-2015-06597、CNVD-2015-06596、CNVD-2015-06595、CNVD-2015-06594、CNVD-2015-06593、CNVD-2015-06606）、Android 缓冲区溢出漏洞（CNVD-2015-06605）、Android 存在多个缓冲区溢出漏洞、Android 安全限制绕过漏洞、Android libstagefright 数字错误漏洞（CNVD-2015-06611、CNVD-2015-06610、CNVD-2015-06609）、Schneider Electric InduSoft Web Studio Remote Agent 组件代码执行漏洞、Schneider Electric InduSoft Web Studio 任意代码执行漏洞、Mitsubishi Electric MELSEC FX3G PLC 设备资源管理错

误漏洞”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-2015-06447	Cisco Wireless LAN Controller RADIUS 实现漏洞	中	是
电信	CNVD-2015-06448	Cisco AnyConnect Secure Mobility Client 搜索路径处理漏洞	中	是
电信	CNVD-2015-06451	Cisco Nexus 3000 Series NX-OS SNMP 服务停止响应漏洞	中	是
电信	CNVD-2015-06507	多款 IBM 产品 SQL 注入漏洞	中	是
电信	CNVD-2015-06512	多款 IBM 产品信息泄露漏洞（CNVD-2015-06512）	中	是
电信	CNVD-2015-06520	Cisco AnyConnect Secure Mobility Client 权限提升漏洞（CNVD-2015-06520）	中	是
电信	CNVD-2015-06531	IBM Content Template Catalog for WebSphere Portal 跨站脚本漏洞	中	是
电信	CNVD-2015-06546	PostgreSQL 内存读取漏洞	高	是
电信	CNVD-2015-06545	PostgreSQL json 或 jsonb 数据拒绝服务漏洞	高	是
电信	CNVD-2015-06555	Cisco IOS Software RADIUS 客户端拒绝服务漏洞	中	是
电信	CNVD-2015-06556	Cisco Wireless LAN Controller 802.11i 管理帧处理拒绝服务漏洞	中	是
电信	CNVD-2015-06558	Cisco Unified Communications Manager IM and Presence Service REST 拒绝服务漏洞	中	是
移动互联网	CNVD-2015-06461	Apple iOS 锁屏绕过漏洞	低	是
移动互联网	CNVD-2015-06504	Android 任意代码执行漏洞	高	是
移动互联网	CNVD-2015-06505	ILegendSoft Mercury Browser For Android 存在多个漏洞	中	否
移动互联网	CNVD-2015-06514	Android 任意代码执行漏洞（CNVD-2015-06514）	高	是
移动互联网	CNVD-2015-06527	Android 缓冲区溢出漏洞	高	是
移动互联网	CNVD-2015-06528	Android 权限提升漏洞（CNVD-2015-06528）	中	是
移动互联网	CNVD-2015-06524	Android 整数溢出漏洞（CNVD-2015-06524）	高	是
移动互联网	CNVD-2015-06534	Android 任意代码执行漏洞（CNVD-2015-06534）	高	是
移动互联网	CNVD-2015-06535	Android 拒绝服务漏洞（CNVD-2015-06535）	中	是
移动互联网	CNVD-2015-06550	Android SMS 消息任意删除漏洞	中	是
移动互联网	CNVD-2015-06566	Android 权限提升漏洞（CNVD-2015-06566）	高	是

		6)		
移动互联网	CNVD-2015-06567	Android 权限提升漏洞 (CNVD-2015-06567)	高	是
移动互联网	CNVD-2015-06568	Android 权限提升漏洞 (CNVD-2015-06568)	高	是
移动互联网	CNVD-2015-06569	Android 权限提升漏洞 (CNVD-2015-06569)	高	是
移动互联网	CNVD-2015-06579	Android 权限提升漏洞 (CNVD-2015-06579)	中	是
移动互联网	CNVD-2015-06576	Android 安全限制绕过漏洞 (CNVD-2015-06576)	中	是
移动互联网	CNVD-2015-06575	Android 安全限制绕过漏洞 (CNVD-2015-06575)	高	是
移动互联网	CNVD-2015-06577	Android 任意代码执行漏洞 (CNVD-2015-06577)	高	是
移动互联网	CNVD-2015-06578	Android 权限提升漏洞 (CNVD-2015-06578)	高	是
移动互联网	CNVD-2015-06580	Android 拒绝服务漏洞 (CNVD-2015-06580)	高	是
移动互联网	CNVD-2015-06589	Android 拒绝服务漏洞 (CNVD-2015-06589)	高	是
移动互联网	CNVD-2015-06588	Android 拒绝服务漏洞 (CNVD-2015-06588)	高	是
移动互联网	CNVD-2015-06587	Android 拒绝服务漏洞 (CNVD-2015-06587)	高	是
移动互联网	CNVD-2015-06586	Android 拒绝服务漏洞 (CNVD-2015-06586)	高	是
移动互联网	CNVD-2015-06585	Android 拒绝服务漏洞 (CNVD-2015-06585)	高	是
移动互联网	CNVD-2015-06584	Android 拒绝服务漏洞 (CNVD-2015-06584)	高	是
移动互联网	CNVD-2015-06583	Android 拒绝服务漏洞 (CNVD-2015-06583)	高	是
移动互联网	CNVD-2015-06582	Android 拒绝服务漏洞 (CNVD-2015-06582)	高	是
移动互联网	CNVD-2015-06581	Android 拒绝服务漏洞 (CNVD-2015-06581)	高	是
移动互联网	CNVD-2015-06592	Android 拒绝服务漏洞 (CNVD-2015-06592)	高	是
移动互联网	CNVD-2015-06591	Android 拒绝服务漏洞 (CNVD-2015-06591)	高	是
移动互联网	CNVD-2015-06590	Android 拒绝服务漏洞 (CNVD-2015-06590)	高	是

移动互联网	CNVD-2015-06597	Android 拒绝服务漏洞（CNVD-2015-06597）	高	是
移动互联网	CNVD-2015-06596	Android 拒绝服务漏洞（CNVD-2015-06596）	高	是
移动互联网	CNVD-2015-06598	Android 信息泄露漏洞	中	是
移动互联网	CNVD-2015-06595	Android 拒绝服务漏洞（CNVD-2015-06595）	高	是
移动互联网	CNVD-2015-06594	Android 拒绝服务漏洞（CNVD-2015-06594）	高	是
移动互联网	CNVD-2015-06593	Android 拒绝服务漏洞（CNVD-2015-06593）	高	是
移动互联网	CNVD-2015-06608	Android 整数溢出漏洞（CNVD-2015-06608）	中	是
移动互联网	CNVD-2015-06606	Android 拒绝服务漏洞（CNVD-2015-06606）	高	是
移动互联网	CNVD-2015-06605	Android 缓冲区溢出漏洞（CNVD-2015-06605）	高	是
移动互联网	CNVD-2015-06604	Android 整数溢出漏洞（CNVD-2015-06604）	高	是
移动互联网	CNVD-2015-06603	Android 安全限制绕过漏洞（CNVD-2015-06603）	中	是
移动互联网	CNVD-2015-06601	Android 存在多个缓冲区溢出漏洞	高	是
移动互联网	CNVD-2015-06617	Android 安全限制绕过漏洞	高	是
移动互联网	CNVD-2015-06611	Android libstagefright 数字错误漏洞（CNVD-2015-06611）	高	是
移动互联网	CNVD-2015-06610	Android libstagefright 数字错误漏洞（CNVD-2015-06610）	高	是
移动互联网	CNVD-2015-06609	Android libstagefright 数字错误漏洞（CNVD-2015-06609）	高	是
工控系统	CNVD-2015-06460	Schneider Electric InduSoft Web Studio Remote Agent 组件代码执行漏洞	高	是
工控系统	CNVD-2015-06464	Schneider Electric InduSoft Web Studio 任意代码执行漏洞	高	是
工控系统	CNVD-2015-06525	Mitsubishi Electric MELSEC FX3G PLC 设备资源管理错误漏洞	高	是

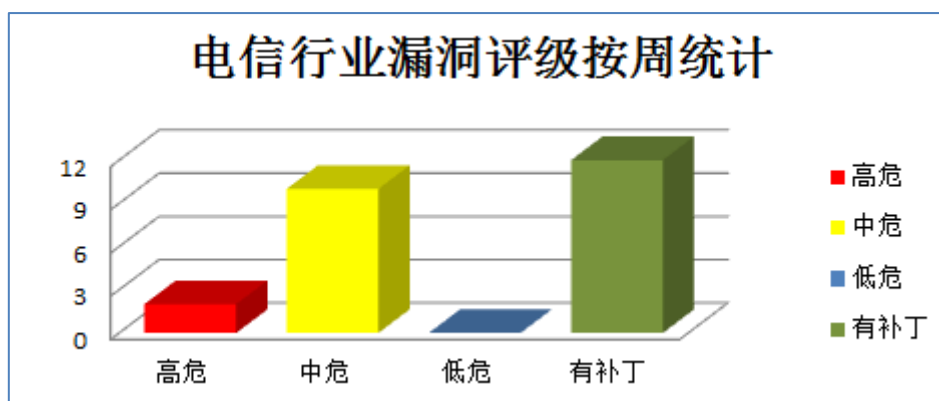


图 1 电信行业漏洞统计

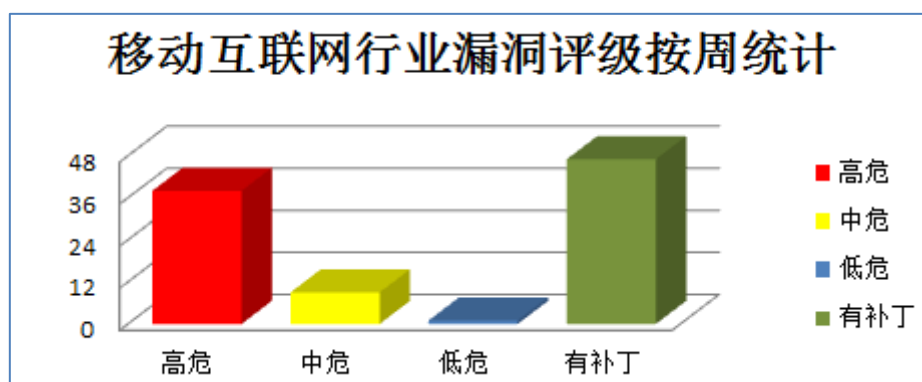


图 2 移动互联网行业漏洞统计

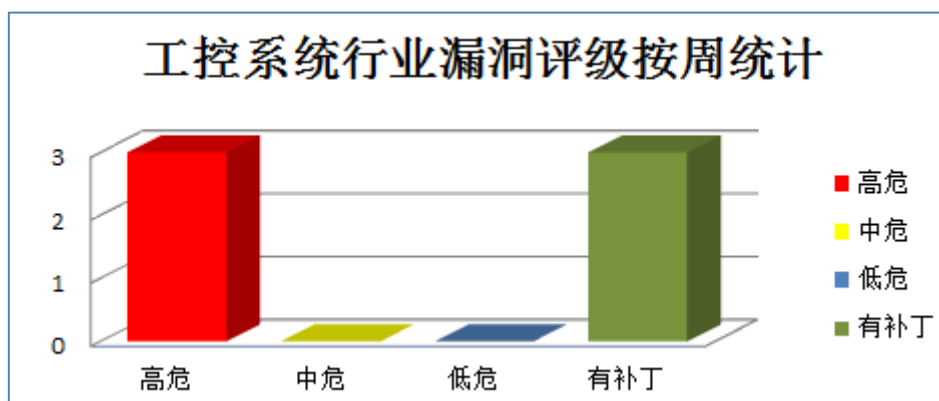


图 3 工控系统行业漏洞统计

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、Google 产品安全漏洞

Android 是美国谷歌（Google）公司和开放手机联盟领导及开发的基于 Linux 开放性内核的移动操作系统。本周，该产品被披露存在拒绝服务漏洞。攻击者利用漏洞可发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Android 拒绝服务漏洞（CNVD-2015-06581、CNVD-

2015-06580、CNVD-2015-06585、CNVD-2015-06584、CNVD-2015-06583、CNVD-2015-06582、CNVD-2015-06594、CNVD-2015-06593）。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-2015-06581>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-06580>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-06585>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-06584>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-06583>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-06582>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-06594>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-06593>

2、Apple 产品安全漏洞

Apple OS X 是一款苹果公司开发的操作系统。本周，该产品被披露存在权限提取、内存破坏漏洞。攻击者利用漏洞可提取权限和执行任意代码。

CNVD 收录的相关漏洞包括：Apple OS X 内核内存破坏漏洞、Apple OS X IOHIDFamily 内存破坏漏洞、Apple OS X 内核内存破坏漏洞（CNVD-2015-06427、CNVD-2015-06428、CNVD-2015-06429）、Apple OS X root 权限提取漏洞、Apple OS X intel 图形驱动内存破坏漏洞、Apple OS X intel 图形驱动内存破坏漏洞（CNVD-2015-06431）。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-2015-06422>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-06425>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-06427>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-06428>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-06429>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-06430>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-06432>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-06431>

3、IBM 产品安全漏洞

IBM Business Process Manager 是一个综合的业务流程管理平台。IBM Maximo Asset Management 是美国 IBM 公司的一套 IT 资产管理解决方案。IBM UrbanCode Deploy 是美国 IBM 公司的应用自动化部署工具。该工具基于一个完善的应用部署自动化管理信息模型,提供可视化的部署逻辑设计手段,并通过远程代理技术,实现对复杂应用在不同环境下的自动化部署。IBM Emptoris Supplier Lifecycle Management 是美国 IBM 公司的

一套供应链生命周期管理方案。IBM Emptoris Sourcing 是美国 IBM 公司的一套供应商寻源决策、考察成本、风险和绩效的平台，帮助企业从供应商那里获得实惠的价格和更大的价值。IBM Multi-Enterprise Integration Gateway 是美国 IBM 公司的一款跨企业集成通信网关产品。IBM Emptoris Strategic Supply Management Platform 是美国 IBM 公司战略供应管理解决方案，有助于企业最大程度地节省成本、提高供应商绩效并降低风险。本周，该产品被披露存在信息泄露、跨站脚本、权限提升和 SQL 注入漏洞。攻击者利用漏洞可获得敏感信息、进行跨站攻击和提升权限。

CNVD 收录的相关漏洞包括：IBM Business Process Manager 跨站脚本漏洞（CNVD-2015-06513）、多款 IBM 产品信息泄露漏洞（CNVD-2015-06512）、IBM UrbanCode Deploy 权限提升漏洞、IBM Emptoris Supplier Lifecycle Management 和 Emptoris Program Management 跨站脚本漏洞、IBM Emptoris Sourcing 信息泄露漏洞、IBM Multi-Enterprise Integration Gateway_2 信息泄露漏洞、IBM Emptoris Strategic Supply Management Platform 和 Emptoris Program Management 跨站脚本漏洞、多款 IBM 产品 SQL 注入漏洞。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-2015-06513>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-06512>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-06511>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-06510>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-06509>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-06508>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-06506>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-06507>

4、Cisco 产品安全漏洞

Cisco Prime 是一款以服务为中心从终端、网络设备和应用整合管理有线与无线 LAN、WAN 与数据中心，并筛选信息的解决方案。Cisco VPN Client 是一套跨平台的客户端软件。Cisco TelePresence VCS Expressway 是一款视频会议应用。Cisco AnyConnect Secure Mobility 是一个安全的企业移动解决方案。Cisco Aironet 3600 access points 是一款思科推出的无线接入点产品。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得敏感信息、提升权限和发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Cisco Prime Collaboration Assurance SQL 注入漏洞（CNVD-2015-06574）、Cisco Prime Collaboration Assurance SQL 注入漏洞、Cisco Prime Infrastructure SSL 重协商请求处理拒绝服务漏洞、Cisco Prime Collaboration Assurance 文件查看漏洞、Cisco VPN Client 权限提升漏洞、Cisco TelePresence VCS Expressway 进程管理权限提升漏洞、Cisco AnyConnect Secure Mobility Client IPC 命令文件

修改漏洞、Cisco Aironet 1850 CLI 输入权限获取漏洞。目前，厂商已发布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-2015-06574>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-06573>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-06561>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-06559>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-06564>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-06563>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-06560>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-06562>

5、Perl Email-Address 模块拒绝服务漏洞

Perl 是跨平台编程语言，Email-Address 是其中的一个电子邮件地址模块。本周，Perl Email-Address 模块被披露存在综合评级为“高危”的拒绝服务漏洞。攻击者利用该漏洞可发起拒绝服务攻击。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-2015-06548>

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-2015-06442	ZOHO ManageEngine EventLog Analyzer 安全绕过 SQL 注入漏洞	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://bonitas2.zohocorp.com/zipUploads/2015_14_07_17_52_30_o_19q686iqs1sfemdf19e05sqre61.tar.gz
CNVD-2015-06455	vtiger 公司 logo 上传任意命令执行漏洞	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.vtiger.com/
CNVD-2015-06456	Web Reference Database 跨站请求伪造漏洞	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.refbase.net/index.php/Web_Reference_Database
CNVD-2015-06457	Web Reference Database 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.refbase.net/index.php/Web_Reference_Database
CNVD-2015-06458	Web Reference Database SQL 注入漏洞（CNVD-2015-06458）	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.refbase.net/index.php/Web_Reference_Database

CNVD-2015-06466	RSA Web Threat Detection 权限提升漏洞	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.emc.com/
CNVD-2015-06464	Schneider Electric InduSoft Web Studio 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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2015-251-01
CNVD-2015-06479	GLPI 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://forge.glpi-project.org/issues/5217
CNVD-2015-06492	Kaspersky Internet Security 文件脱壳缓冲区溢出漏洞	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://support.kaspersky.com/vulnerability.aspx?el=12430
CNVD-2015-06499	EasyIO EasyIO-30P-SF 控制器硬编码漏洞	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.easyio.com/

表 3 部分高危漏洞列表

小结：本周，Google 产品被披露存在拒绝服务漏洞。攻击者利用漏洞可发起拒绝服务攻击。此外，Apple、IBM、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、进行跨站脚本攻击、提升权限、执行任意代码和发起拒绝服务攻击。另外，Perl Email-Address 模块被披露存在一个高危零日漏洞，攻击者利用该漏洞可发起拒绝服务攻击。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、Apache 修补 Commons Components HttpClient 产品漏洞

Apache Commons 包含了很多开源的工具，用于解决平时编程经常会遇到的问题，减少重复劳动。

本周，Apache 修补了上述产品存在的拒绝服务漏洞，避免攻击者利用漏洞发起拒绝服务攻击。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/65139>

本周要闻速递

1. iOS 核心应用设计漏洞，暴露用户 Apple ID 凭证

Check Point 的安全研究员 Kasif Dekel 上个月在 iOS 核心功能中发现了一个软件设计漏洞（CVE-2015-5832），这个软件是用来管理核心应用程序的凭证。即使用户已经注销了，这个漏洞也会保存下用户的登录凭证，从而导致设备上存储的敏感数据泄漏出去。苹果已经核实确认该安全问题，并已发布了一个安全公告。

参考链接：<http://www.freebuf.com/news/81621.html>

2. 谷歌 AdMob 过滤器漏洞

来自悉尼的两款公交安卓应用（Arrivo 和 TripView 公交时间表）的开发人员告诉我们，谷歌应用收费服务 AdMob 的过滤器，并没有能抓到偷偷潜进他们应用的恶意广告。恶意广告是一种新兴的问题，大多数用户信任广告拦截的安全预防措施，觉得它们能保护自己不受恶意软件和垃圾广告侵害。然而，像上面所提到的 Arrivo 和 TripView 公交时间表应用，都遭受了垃圾广告的入侵。

参考链接：<http://www.freebuf.com/news/81614.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