国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2014 年 11 月 10 日-2014 年 11 月 16 日 **2014 年第 46 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 152 个，其中高危漏洞 75 个、中危漏洞 70 个、低危漏洞 7 个。上述漏洞中，可利用来实施远程攻击的漏洞有 139 个。本周收录的漏洞中，已有 118 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“IP.Board 'ipsconnect.php' SQL 注入漏洞”、“JExperts Channel 存在多个远程权限提升漏洞”等零日攻击代码，请使用相关产品的用户注意加强防范。

上周，微软发布月度例行安全公告，其中修复了一个标注为“严重”级的漏洞，“Microsoft Windows OLE 远程代码执行漏洞（CNVD-2014-08252）”，根据 CNCERT 监测情况和 WOOYUN 白帽子报送结果，互联网上已经出现针对漏洞的网页挂马攻击。

成员单位报送漏洞统计

本周，共 7 家成员单位及个人报送了本周收录的全部 152 个漏洞。报送情况如表 1 所示。其中，安天实验室、恒安嘉新、天融信、启明星辰等单位报送数量较多。此外，CNCERT 各分中心、北京数字认证股份有限公司及白帽子向 CNVD 提交了 36 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
安天实验室	161	0
恒安嘉新	119	0
天融信	117	0
启明星辰	115	0

绿盟科技	25	0
奇虎 360	4	4
北京数字认证股份有限公司	2	2
CNCERT 江西分中心	13	13
CNCERT 河南分中心	5	5
CNCERT 山西分中心	3	3
CNCERT 福建分中心	3	3
CNCERT 宁夏分中心	1	1
个人	5	5
报送总计	573	36
录入总计	152（去重）	36

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Microsoft、Adobe、SAP 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	Microsoft	32	21%
2	Adobe	18	12%
3	SAP	13	9%
4	Aruba Networks	8	5%
5	Cisco	7	4%
6	IBM	4	3%
7	Joomla!	4	3%
8	Linux	3	2%
9	WordPress	3	2%
10	其他	60	39%

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 152 个漏洞。其中应用程序漏洞 108 个，WEB 应用漏洞 19 个，网络设备漏洞 9 个，操作系统漏洞 9 个，安全产品漏洞 5 个，数据库漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	108
WEB 应用漏洞	19
网络设备漏洞	9
操作系统漏洞	9
安全产品漏洞	5
数据库漏洞	2

表 3 漏洞按影响类型统计表

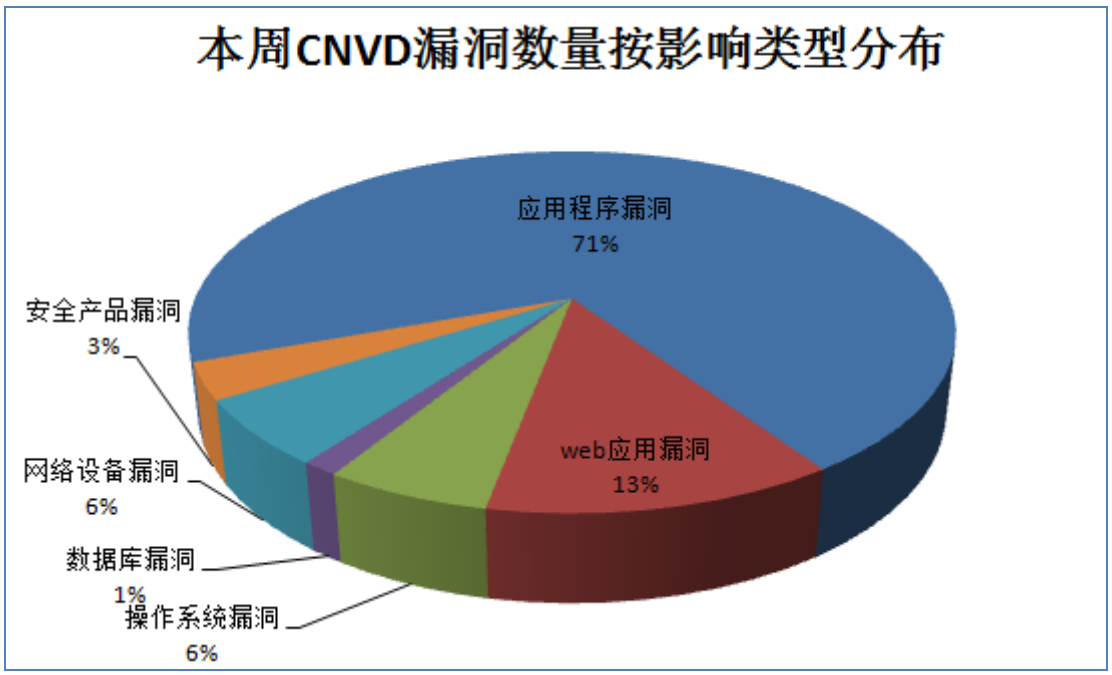

图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 9 个电信行业漏洞，3 个移动互联网漏洞（如下图表所示）。其中，“Cisco RV router firmware 任意代码执行漏洞、Cisco RV router firmware 跨站请求伪造漏洞”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-2014-08179	IBM Tivoli Netcool/Impact 跨站脚本漏洞	中	是
电信	CNVD-2014-08188	Cisco RV router firmware 任意代码执行漏洞	高	是
电信	CNVD-2014-08191	Cisco Unity Connection 信息泄露漏洞	中	是
电信	CNVD-2014-08192	Cisco IOS XE 软件本地安全绕过漏洞	中	否
电信	CNVD-2014-08196	Belkin N750 DB Wi-Fi Gigabit Router	高	否

		缓冲区溢出漏洞		
电信	CNVD-2014-08189	Cisco RV router firmware 任意文件上传漏洞	中	是
电信	CNVD-2014-08200	Cisco RV router firmware 跨站请求伪造漏洞	高	是
电信	CNVD-2014-08206	D-Link DAP-1360 存在多个漏洞	中	否
电信	CNVD-2014-08230	Cisco Unified Communications Manager TLS 证书验证安全绕过漏洞	中	否
移动互联网	CNVD-2014-08194	GWT Mobile PhoneGap Showcase application for Android 跨站脚本漏洞	中	否
移动互联网	CNVD-2014-08193	RewardingYourself application for Android and BlackBerry OS 跨站脚本漏洞	中	否
移动互联网	CNVD-2014-08224	Apple iOS 捆绑标识符验证安全绕过漏洞	中	否

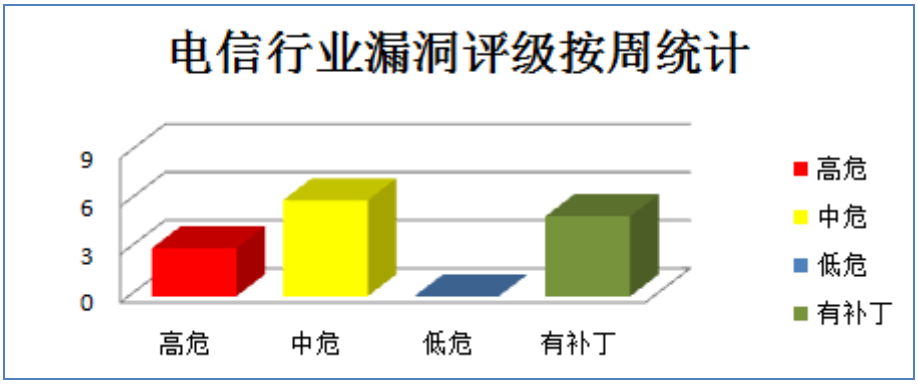

图 1 电信行业漏洞统计

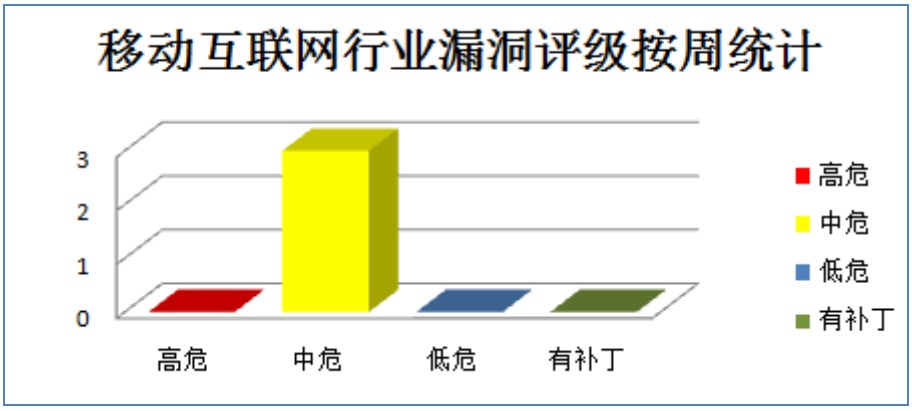

图 2 移动互联网行业漏洞统计

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、 Microsoft 产品安全漏洞

11 月 11 日，微软发布了 2014 年 11 月份的月度例行安全公告，共含 15 项更新，修复了 Microsoft Windows、Internet Explorer、.NETFramework、Office、Exchange 和 Server 软件中存在的 37 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，攻击者可以远程执行代码，提升权限，绕过安全功能限制，获得敏感信息，或发起拒绝服务攻击。其中，Microsoft Windows OLE 远程代码执行漏洞（CNVD-2014-08252），根据 CNCERT 监测情况和 WOOYUN 白帽子报送结果，已经出现针对该漏洞的攻击。

CNVD 收录的相关漏洞包括：Microsoft Windows OLE 远程代码执行漏洞（CNVD-2014-08252）、Microsoft Internet Explorer 内存破坏漏洞（CNVD-2014-08277、CNVD-2014-08270、CNVD-2014-08269、CNVD-2014-08268、CNVD-2014-08267、CNVD-2014-08266、CNVD-2014-08265）。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/webinfo/show/3532

2、 Adobe 产品安全漏洞

Adobe Flash Player 是一款 Flash 文件处理程序。Adobe AIR 是 Adobe 公司出品的跨操作系统的运行时库，通过它开发者可利用现有的 Web 开发技术。本周，上述产品被披露存在内存破坏和远程代码执行漏洞，攻击者可利用漏洞发起拒绝服务或执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Flash Player and AIR 内存错误引用远程代码执行漏洞（CNVD-2014-08234、CNVD-2014-08233、CNVD-2014-08232）、Adobe Flash Player and AIR 存在未明内存破坏漏洞（CNVD-2014-08228、CNVD-2014-08227）、Adobe Flash Player and AIR 内存破坏漏洞（CNVD-2014-08241、CNVD-2014-08242）、Adobe Flash Player And AIR 类型混乱远程代码执行漏洞（CNVD-2014-08240）。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/flaw/show/CNVD-2014-08234
http://www.cnvd.org.cn/flaw/show/CNVD-2014-08233
http://www.cnvd.org.cn/flaw/show/CNVD-2014-08232
http://www.cnvd.org.cn/flaw/show/CNVD-2014-08228
http://www.cnvd.org.cn/flaw/show/CNVD-2014-08227
http://www.cnvd.org.cn/flaw/show/CNVD-2014-08241
http://www.cnvd.org.cn/flaw/show/CNVD-2014-08242
http://www.cnvd.org.cn/flaw/show/CNVD-2014-08240

3、 SAP 产品安全漏洞

SAP 为“Systems Applications and Products in Data Processing”的简称，是 SAP 公司的产品——企业管理解决方案的软件名称。SAP GRC 是治理、风险管理及合规解决方案。SAP NetWeaver 是一款 SAP 业务套件解决方案、SAP xApps 组合应用、合作伙伴解决方案以及客户定制应用的技术基础。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取敏感信息、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：SAP GRC 存在多个未明漏洞、SAP Document Management Services 任意代码执行漏洞、SAP CRM Internet Sales module 任意代码执行漏洞、SAP Payroll Process 拒绝服务漏洞、SAP NetWeaver Business Warehouse SQL 注入漏洞、SAP Product Safety (EHS-SAF) SQL 注入漏洞、SAP Contract Accounting SQL 注入漏洞、SAP CRM Promotion Guidelines (CRM-MKT-MPL-TPM-PPG)模块远程代码执行漏洞。上述漏洞的综合评级为“高危”。其中“SAP GRC 存在多个未明漏洞、SAP Document Management Services 任意代码执行漏洞、SAP CRM Internet Sales module 任意代码执行漏洞、SAP Payroll Process 拒绝服务漏洞”厂商已经发布了修补程序。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-2014-08291

http://www.cnvd.org.cn/flaw/show/CNVD-2014-08163

http://www.cnvd.org.cn/flaw/show/CNVD-2014-08146

http://www.cnvd.org.cn/flaw/show/CNVD-2014-08162

http://www.cnvd.org.cn/flaw/show/CNVD-2014-08144

http://www.cnvd.org.cn/flaw/show/CNVD-2014-08148

http://www.cnvd.org.cn/flaw/show/CNVD-2014-08147

http://www.cnvd.org.cn/flaw/show/CNVD-2014-08145

4、Cisco 产品安全漏洞

Cisco Unified Communications Manager（CUCM，Unified CM）是美国思科（Cisco）公司的一款统一通信系统中的呼叫处理组件。该组件提供了一种可扩展、可分布和高可用的企业 IP 电话呼叫处理解决方案。Cisco RV router firmware 是思科 RV 180 系列 VPN 路由器固件。Cisco IOS 是多数思科系统路由器和网络交换机上使用的互联网络操作系统。Cisco Unified Computing System 通过将统一计算、网络、存储访问和虚拟化整合到一个系统中，简化 IT 管理并提高灵活性。Cisco Unity Connection 是一个由语音、视频、数据和移动产品及应用组成的全面 IP 通信系统。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取敏感信息、提升权限、绕过安全限制执行任意未授权操作。

CNVD 收录的相关漏洞包括：Cisco Unified Communications Manager TLS 证书验证安全绕过漏洞、Cisco RV router firmware 任意代码执行漏洞、Cisco RV router firmware 跨站请求伪造漏洞、Cisco RV router firmware 任意文件上传漏洞、Cisco IOS XE

软件本地安全绕过漏洞、Cisco Unified Computing System 存在多个本地权限提升漏洞、Cisco Unity Connection 信息泄露漏洞。其中“Cisco RV router firmware 任意代码执行漏洞、Cisco RV router firmware 跨站请求伪造漏洞”的综合评级为“高危”。目前，除“Cisco Unified Communications Manager TLS 证书验证安全绕过漏洞、Cisco IOS XE 软件本地安全绕过漏洞”外，厂商已经发布其余漏洞的修补程序。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-2014-08230

http://www.cnvd.org.cn/flaw/show/CNVD-2014-08188

http://www.cnvd.org.cn/flaw/show/CNVD-2014-08200

http://www.cnvd.org.cn/flaw/show/CNVD-2014-08189

http://www.cnvd.org.cn/flaw/show/CNVD-2014-08192

http://www.cnvd.org.cn/flaw/show/CNVD-2014-08183

http://www.cnvd.org.cn/flaw/show/CNVD-2014-08191

5、PHP-Fusion 存在多个 SQL 注入漏洞（CNVD-2014-08293）

PHP-Fusion 是一套基于 MySql 和 PHP 的开源轻量级内容管理系统。该系统包含新闻、文章和论坛等模块。本周，PHP-Fusion 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受影响的应用程序，访问或修改数据库数据。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-2014-08293

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-2014-08152	KDE Workspace 任意命令执行漏洞	高	KDE Workspace 4.14.3 已经修复该漏洞，建议用户下载更新：https://git.reviewboard.kde.org/r/120977/
CNVD-2014-08161	RSA Web Threat Detection SQL 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：http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-4627
CNVD-2014-08165	French National Commission on Informatics and Liberty (aka CNIL) CookieViz SQL 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：http://seclists.org/fulldisclosure/2014/Nov/3

CNVD-2014-08177	Open-XchangeAppSuite 'ExtractValue()'函数 SQL 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：http://www.open-xchange.com/home.html
CNVD-2014-08190	LibreOffice 释放后重利用漏洞	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.libreoffice.org/
CNVD-2014-08199	ManageEngine 产品任意文件上传漏洞	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.manageengine.com/network-monitoring/
CNVD-2014-08198	ManageEngine 产品存在多个 SQL 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：http://www.manageengine.com/network-monitoring/
CNVD-2014-08213	MantisBTXmlImportExport 插件 'ImportXml.php'任意 PHP 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://www.mantisbt.org/
CNVD-2014-08207	MODX Evolution 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://modx.com/
CNVD-2014-08218	Aruba ClearPass 权限提升漏洞（CNVD-2014-08218）	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.arubanetworks.com/

表 3 部分高危漏洞列表

小结：本周，微软发布了 2014 年 11 月份的月度例行安全公告，共含 15 项更新，修复了 Microsoft Windows、Internet Explorer、.NETFramework、Office、Exchange 和 Server 软件中存在的 37 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，攻击者可以远程执行代码，提升权限，绕过安全功能限制，获得敏感信息，或进行拒绝服务攻击。此外， Adobe、SAP、Cisco 多款产品被批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、发起拒绝服务攻击或提升权限执行未授权操作。另外，PHP-Fusion 被披露存在一个高危零日漏洞。攻击者可利用漏洞危及受影响的应用程序，访问或修改数据库数据。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、Apache 修补 Qpid/Traffic Server 产品漏洞

Apache Qpid(Open Source AMQP Messaging)是一个跨平台的企业通讯解决方案，实现了高级消息队列协议。Traffic Server 是 Apache 软件基金会所研发的开放源码代理服务器和 Web 缓存服务器。

本周，Apache 修补了上述产品存在的 XML 外部实体注入和跨站脚本漏洞，避免攻击者利用漏洞执行未授权操作或在受影响用户的浏览器上下文中执行任意 HTML 和脚本代码。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/51785

http://www.cnvd.org.cn/patchInfo/show/51729

本周要闻速递

1. 贝尔金路由器（Belkin router）存在 ROOT 访问权限漏洞

安全研究员 Marco Vaz 在贝尔金 n750 型号的路由器中发现一个严重的漏洞，该漏洞可以使攻击者在受害者的设备上获得 Root 访问权限（也就是管理员权限）。该公司已经发布了该漏洞的修复补丁，但遗憾的是，进行固件更新修补该漏洞的用户却很少。该漏洞的编码为 CVE-2014-1635，主要攻击的是路由器的 Web 界面，受攻击的路由器型号为 N750 DB WIFI 双频 N+千兆型，运行的固件版本为 F9K1103_WW_1.10.16m。

参考链接：http://www.freebuf.com/news/50811.html

2. 微软披露影响所有 Windows 版本的高危漏洞

微软披露了一个存在于所有 Windows 版本的高危漏洞。建议所有 Windows 用户，尤其是运行网站的用户应尽快安装微软周二发布的补丁。据微软的公告称，该高危漏洞存在于微软的安全传输层协议（TLS）和安全套接层协议（SSL）中。因为它不能正确的过滤特殊形式的数据包，这就使得攻击者可以向 Windows 服务器发送恶意流量远程执行攻击代码。

参考链接：http://www.freebuf.com/news/51382.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