

信息安全漏洞周报

2015 年 11 月 09 日-2015 年 11 月 15 日

2015 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**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 181 个，其中高危漏洞 53 个、中危漏洞 116 个、低危漏洞 12 个。上述漏洞中，可利用来实施远程攻击的漏洞有 158 个。本周收录的漏洞中，已有 149 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“WinRAR SFX 'Text and Icon'函数远程代码执行漏洞”、“Joomla! jNews 组件'index.php' SQL 注入漏洞”等零日代码攻击，请使用相关产品的用户注意加强防范。

本周，安全业界对涉及众多 Web 容器软件的“Apache Commons Components InvokerTransformer 反序列化任意代码执行漏洞”(CNVD-2015-07556)进行了分析和重点关注，针对上述漏洞暂时没有统一的官方补丁，CNVD 建议参考如下措施（见下表）采取临时修复措施：

Web 容器	影响版本	建议解决方案
jboss	JBoss Enterprise Application Platform 6.4.4, 5.2.0, 4.3.0_CP10 JBoss AS (Wildfly) 6 and earlier JBoss A-MQ 6.2.0 JBoss Fuse 6.2.0 JBoss SOA Platform (SOA-P) 5.3.1 JBoss Data Grid (JDG) 6.5.0 JBoss BRMS (BRMS) 6.1.0 JBoss BPMS (BPMS) 6.1.0 JBoss Data Virtualization (JDV) 6.1.0 JBoss Fuse Service Works (FSW) 6.0.0 JBoss Enterprise Web Server (EWS) 2.1, 3.0	删除 commons-collections jar 中的 InvokerTransformer, InstantiateFactory, 和 InstantiateTransformer class 文件
WebSphere		使用 SerialKiller 替换进行序

WebLogic	9.2.3.0\9.2.4.0\10.0.0.0\10.0.1.0\10.0.2.0\10.2.6.0\10.3.0.0\10.3.1.0\10.3.2.0\10.3.4.0\10.3.5.0\12.1.1.0	列化操作的 <code>ObjectInputStream</code> 类； 在不影响业务的情况下，临时删除项目里的 “org/apache/commons/collections/functors/InvokerTransformer.class” 文件；
Jenkins		

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 181 个漏洞。报送情况如表 1 所示。其中，奇虎(补天平台)、天融信、安天实验室、启明星辰等单位报送数量较多。补天平台、乌云、漏洞盒子、河北翎贺计算机信息技术有限公司及白帽子向 CNVD 提交了 776 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)	556	556
天融信	178	0
安天实验室	163	0
启明星辰	143	0
绿盟科技	67	0
恒安嘉新	52	0
H3C	8	0
乌云	180	180
漏洞盒子	15	15
河北翎贺计算机信息技术有限公司	1	1
CNCERT 宁夏分中心	1	1
个人	23	23
报送总计	1387	776

录入总计	181（去重）	776
------	---------	-----

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Mozilla、IBM、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	Mozilla	23	13%
2	IBM	22	12%
3	Cisco	16	9%
4	MediaWiki	9	5%
5	TYPO3	7	4%
6	SAP	7	4%
7	Samsung	7	4%
8	Microsoft	6	3%
9	Linux	4	2%
10	其他	80	44%

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 181 个漏洞。其中应用程序漏洞 132 个，网络设备漏洞 16 个，Web 应用漏洞 13 个，操作系统漏洞 11 个，数据库漏洞 5 个，安全产品漏洞 4 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	132
网络设备漏洞	16
Web 应用漏洞	13
操作系统漏洞	11
数据库漏洞	5
安全产品漏洞	4

表 3 漏洞按影响类型统计表

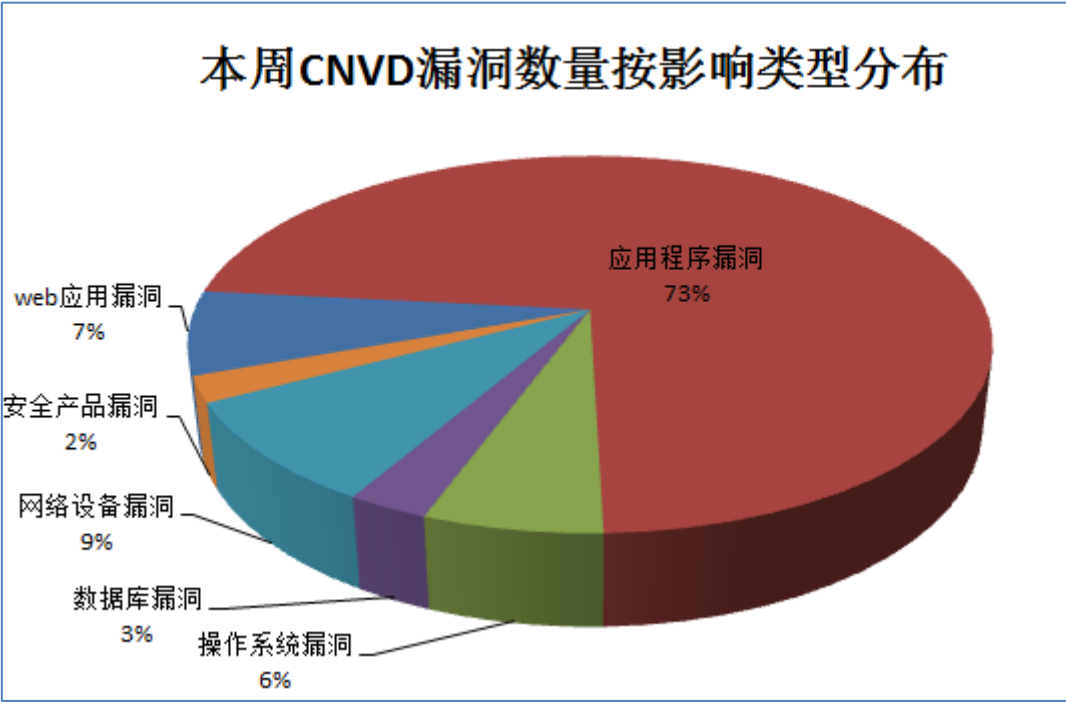


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 10 个电信行业漏洞、8 个移动互联网行业漏洞（如下图表所示）。其中，“IBM Tivoli Storage Manager 权限提升漏洞（CNVD-2015-07342）、Lenovo Switch Center 本地提权漏洞、Android 远程权限提升漏洞（CNVD-2015-07366、CNVD-2015-07367、CNVD-2015-07368、CNVD-2015-07369）”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-2015-07342	IBM Tivoli Storage Manager 权限提升漏洞（CNVD-2015-07342）	高	是
电信	CNVD-2015-07410	Samsung Galaxy S6 目录遍历漏洞	中	否
电信	CNVD-2015-07446	Huawei AR Routers 信息泄露漏洞	中	是
电信	CNVD-2015-07462	IBM WebSphere Commerce Enterprise 信息泄露漏洞	中	是
电信	CNVD-2015-07463	多款 IBM 产品访问权限漏洞	中	是
电信	CNVD-2015-07473	多款 IBM 产品存在漏洞	中	是
电信	CNVD-2015-07474	多款 Huawei 产品目录遍历漏洞	低	是
电信	CNVD-2015-07485	IBM WebSphere Application Server CRLF 注入漏洞	中	是
电信	CNVD-2015-07513	Lenovo Switch Center 远程提权漏洞	中	是
电信	CNVD-2015-07514	Lenovo Switch Center 本地提权漏洞	高	是
移动互联网	CNVD-2015-07341	Android 拒绝服务漏洞（CNVD-2015-07341）	中	是

		1)		
移动互联网	CNVD-2015-07351	Android 信息泄露漏洞 (CNVD-2015-07351)	中	是
移动互联网	CNVD-2015-07365	Android 远程权限提升漏洞 (CNVD-2015-07365)	中	是
移动互联网	CNVD-2015-07366	Android 远程权限提升漏洞 (CNVD-2015-07366)	高	是
移动互联网	CNVD-2015-07367	Android 远程权限提升漏洞 (CNVD-2015-07367)	高	是
移动互联网	CNVD-2015-07368	Android 任意代码执行漏洞 (CNVD-2015-07368)	高	是
移动互联网	CNVD-2015-07369	Android 任意代码执行漏洞 (CNVD-2015-07369)	高	是
移动互联网	CNVD-2015-07409	Samsung Fimg2d 本地竞争条件漏洞	中	否

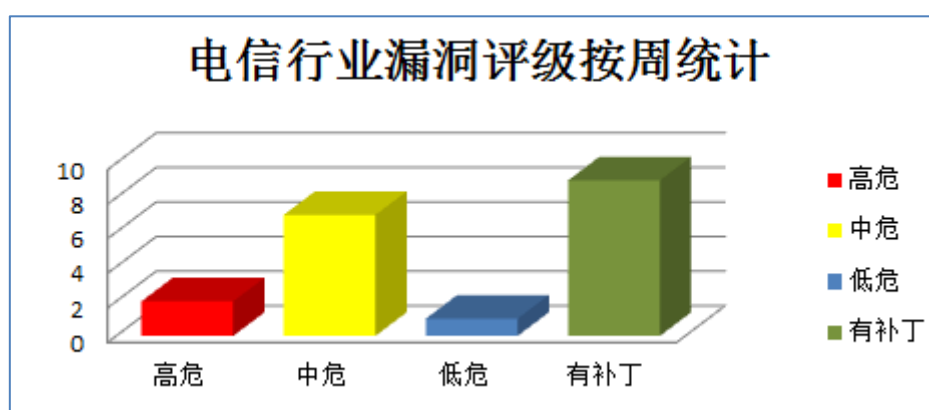


图 1 电信行业漏洞统计

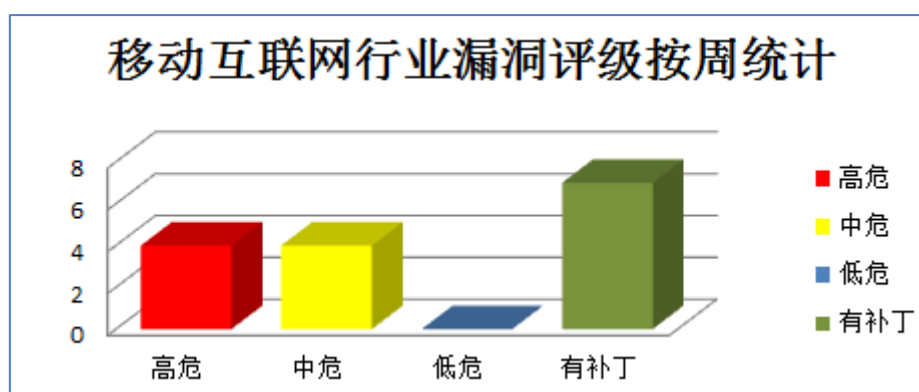


图 2 移动互联网行业漏洞统计

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10日，微软发布了2015年11月份的月度例行安全公告，共含12项更新，修复了Microsoft Windows、Explorer、Edge、Office、Office Services、Skype、Lync、Web Apps和.NETFramework中存在的53个安全漏洞。其中，4项远程代码更新的综合评级为最高级“严重”级别。利用上述漏洞，攻击者可提升权限，绕过安全功能限制，执行远程代码。

CNVD收录的相关漏洞包括：Microsoft Office 内存破坏漏洞（CNVD-2015-07511、CNVD-2015-07510）、Microsoft Internet Explorer 内存破坏漏洞（CNVD-2015-07509、CNVD-2015-07508、CNVD-2015-07507）、Microsoft exfat ‘mount.c’ 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/webinfo/show/3737>

2、IBM 产品安全漏洞

IBM Security QRadar Incident Forensics 是美国 IBM 公司的一套安全取证调查软件。该软件支持对疑似恶意网络安全事件进行深入取证调查，及修复网络安全漏洞。IBM WebSphere Application Server (WAS) 是美国 IBM 公司开发并发行的一款应用服务器产品，它是 Java EE 和 Web 服务应用程序的平台，也是 IBM WebSphere 软件平台的基础。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、注入任意 Web 脚本或 HTML 和执行任意 SQL 命令等。

CNVD收录的相关漏洞包括：IBM Security QRadar Incident Forensics 中间人攻击漏洞（CNVD-2015-07484、CNVD-2015-07479）、IBM Security QRadar Incident Forensics 跨站请求伪造漏洞、IBM Security QRadar Incident Forensics 缓存 SSL 页面漏洞、IBM Security QRadar Incident Forensics 跨站脚本漏洞（CNVD-2015-07481）、IBM Security QRadar Incident Forensics 会话劫持漏洞、IBM Security QRadar Incident Forensics SQL 注入漏洞、IBM WebSphere Application Server CRLF 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-2015-07484>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07479>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07483>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07482>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07481>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07480>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07478>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07485>

3、Mozilla 产品安全漏洞

Mozilla Firefox 是一款开源 Web 浏览器。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、进行跨站脚本攻击和发起拒绝服务攻击等。

Mozilla NSS/Firefox 整数溢出漏洞、Mozilla Firefox 跨站脚本漏洞 (CNVD-2015-07411)、Mozilla Firefox 功能拒绝服务漏洞、Mozilla Firefox 地址栏伪造漏洞 (CNVD-2015-07429)、Mozilla Firefox 信息泄露漏洞 (CNVD-2015-07432)、Mozilla Firefox Add-on SDK 跨站脚本漏洞、Mozilla Firefox 信息泄露漏洞 (CNVD-2015-07430)、Mozilla Firefox Reader View 功能跨站脚本漏洞。其中,“Mozilla NSS/Firefox 整数溢出漏洞、Mozilla Firefox 功能拒绝服务漏洞”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-2015-07441>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07411>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07412>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07429>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07432>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07431>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07430>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07428>

4、TYPO3 产品安全漏洞

TYP03 是瑞士 TYP03 协会维护的一套免费开源的内容管理系统(框架)(CMS/CMF)。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、进行跨站脚本和跨站请求伪造攻击、访问任意文件和执行任意代码等。

CNVD 收录的相关漏洞包括: TYP03 Zend Framework Integration 扩展任意文件访问漏洞、TYP03 MK Forms 扩展任意代码执行漏洞、TYP03 http:BL Blocking 扩展 SQL 注入漏洞、TYP03 LDAP 扩展信息泄露漏洞、TYP03 News system 扩展跨站脚本漏洞、TYP03 Adminer 扩展信息泄露漏洞、TYP03 Typo3Quixplorer 扩展跨站请求伪造漏洞。其中,“TYP03 MK Forms 扩展任意代码执行漏洞、TYP03 http:BL Blocking 扩展 SQL 注入漏洞”的综合评级为“高危”。目前,厂商已发布了除“TYP03 http:BL Blocking 扩展 SQL 注入漏洞、TYP03 LDAP 扩展信息泄露漏洞”外,其余漏洞的修补程序。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-2015-07449>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07450>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07451>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07452>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07453>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07454>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07455>

5、Google Picasa 堆缓冲区溢出漏洞

Google Picasa 是一套应用软件，用于整理和编辑数字相片。本周，Google Picasa 被披露存在堆缓冲区溢出漏洞。攻击者利用该漏洞可执行任意代码。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-2015-07528>

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-2015-07333	Palo Alto Networks Panorama VM Appliance 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这个安全问题，请到厂商的主页下载： https://www.paloaltonetworks.com/
CNVD-2015-07332	GNOME NetworkManager ‘ipv6/addrconf.c’拒绝服务漏洞	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://wiki.gnome.org/Projects/NetworkManager
CNVD-2015-07390	Accentis ‘SIDX’参数 SQL 注入漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： http://www.accentis.com.au/
CNVD-2015-07385	Commvault Edge Server Web 控制台 OS 命令注入漏洞	高	暂无
CNVD-2015-07439	PHP Server Monitor 存在多个漏洞	高	暂无
CNVD-2015-07440	Python ‘Modules\audioop.c’存在多个内存破坏漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： http://www.python.org/
CNVD-2015-07458	OpenSMTPD 存在多个漏洞（CNVD-2015-07458）	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.opensmtpd.org/
CNVD-2015-07515	SAP HANA DB SQL 接口任意代码执行漏洞	高	用户可联系供应商获得补丁信息： http://www.sap.com
CNVD-2015-07516	SAP HANA DB Extended Application Services 任意代码执行漏洞	高	用户可联系供应商获得补丁信息： http://www.sap.com

CNVD-2015-07519	SAP HANA Database 任意代码执行漏洞	高	用户可联系供应商获得补丁信息： http://www.sap.com
-----------------	----------------------------	---	--

表 3 部分高危漏洞列表

小结：本周，微软发布了 2015 年 11 月份的月度例行安全公告，共含 12 项更新，修复了 Microsoft Windows、Explorer、Edge、Office、Office Services、Skype、Lync、Web Apps 和 .NETFramework 中存在的 53 个安全漏洞。此外，IBM、Mozilla、TYPO3 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、进行跨站脚本和跨站请求伪造攻击、执行任意 SQL 命令、发起拒绝服务攻击和执行任意代码等。另外，Google Picasa 被披露存在一个高危漏洞，攻击者利用该漏洞可执行任意代码。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、Apache 修补 Ambari 产品漏洞

Apache Ambari 是规定、管理、监控 Apache Hadoop 集群的工具。

本周，Apache 修补了上述产品存在的开放重定向漏洞，避免攻击者利用漏洞将用户重定向到任意网站，并进行钓鱼攻击。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/66316>

本周要闻速递

1. 三星 Galaxy 手机通话可被黑客远程监听和记录

旧金山的 Daniel Komaromy 和柏林的 NicoGolde 两个安全研究人员发现三星 Galaxy 手机—S6、S6 Edge、特别是 Note 4 存在 MITM 攻击。这两位研究人员在一个刚开箱的、最新升级的三星设备上演示了这个中间人（MITM）攻击，此攻击允许他们通过将设备连接到伪基站来截获语音通话内容。此外，两位研究人员已经将他们的发现报告给了三星，且目前他们未向公众公布该攻击的细节信息。

参考链接：<http://www.freebuf.com/news/85614.html>

2. iBackDoor：疑似后门，影响 iOS 应用的高风险代码

近期，FireEye 的移动安全研究人员发现了嵌入到 iOS 应用中的疑似“后门”行为的 mobiSage 广告库，并且这些应用都是由 App Store 发布的。研究人员将该潜在的后门称为 iBackDoor，允许黑客访问敏感的用户数据和设备功能。截止目前，已经发现 2,846 款 iOS 应用受到影响，检测到 900 次使用 JavaScript 代码控制后门的尝试。幸运的

是，目前还没有发现广告服务器发送任何恶意的命令（例如录音或窃取敏感数据）。

参考链接：<http://www.freebuf.com/news/85143.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