国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2015 年 11 月 23 日-2015 年 11 月 29 日 **2015 年第 48 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**低**。

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 146 个，其中高危漏洞 38 个、中危漏洞 99 个、低危漏洞 9 个。上述漏洞中，可利用来实施远程攻击的漏洞有 123 个。本周收录的漏洞中，已有 114 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“Kaspersky Antivirus 存在多个内存破坏漏洞”、“Kaspersky Anti-Virus 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 6 家成员单位、合作伙伴及个人报送了本周收录的全部 146 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、启明星辰、天融信等单位报送数量较多。补天平台、乌云、漏洞盒子、习科网络安全及白帽子向 CNVD 提交了 970 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)	521	521
安天实验室	155	0
启明星辰	74	0
天融信	70	0
恒安嘉新	59	0
绿盟科技	46	0

乌云	426	426
漏洞盒子	14	14
习科网络安全	1	1
CNCERT 上海分中心	2	2
CNCERT 安徽分中心	1	1
个人	5	5
报送总计	1374	970
录入总计	146（去重）	970

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、Huawei、Moodle 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	14	10%
2	Huawei	12	8%
3	Moodle	10	7%
4	CloudBees	10	7%
5	IBM	6	4%
6	Adobe	4	3%
7	CSL DualCom	4	3%
8	Kaspersky Labs	4	3%
9	ARRIS	4	3%
10	其他	78	52%

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 146 个漏洞。其中应用程序漏洞 87 个，网络设备漏洞 28 个，Web 应用漏洞 16 个，操作系统漏洞 7 个，安全产品漏洞 7 个，数据库漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	87
网络设备漏洞	28

Web 应用漏洞	16
操作系统漏洞	7
安全产品漏洞	7
数据库漏洞	1

表 3 漏洞按影响类型统计表

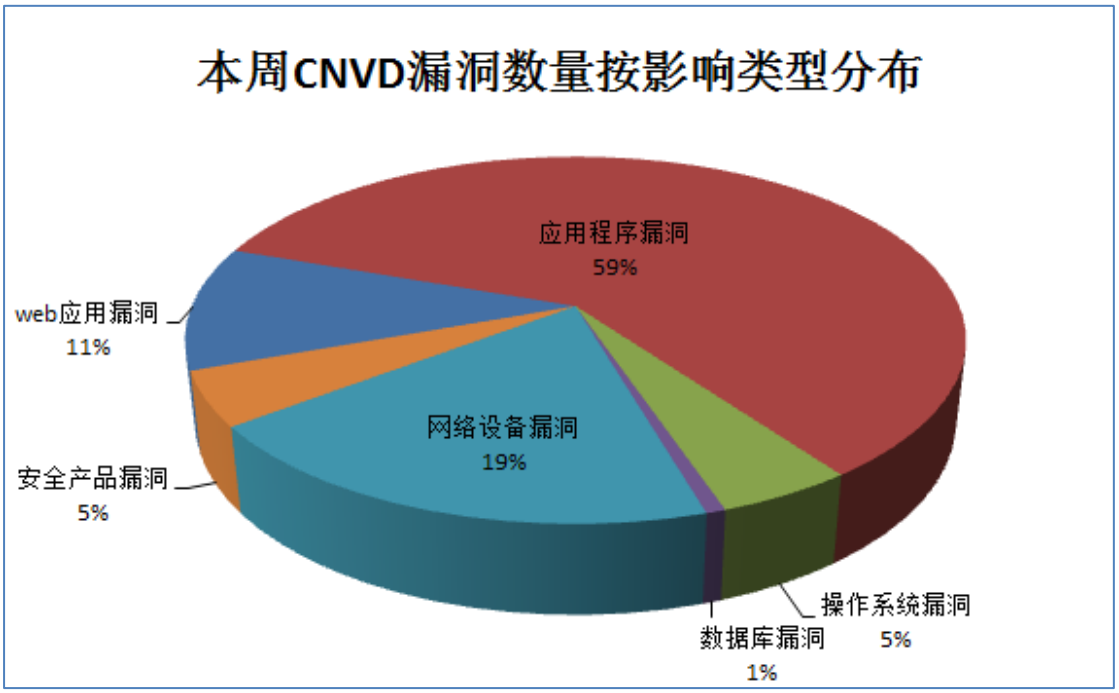

图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 13 个电信行业漏洞、4 个移动互联网行业漏洞（如下图表所示）。其中，“IBM WebSphere Application Server 远程代码执行漏洞”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-2015-07696	D-Link DIR-601 命令注入漏洞	高	否
电信	CNVD-2015-07695	D-Link DIR-615 ’ PING ‘和 ‘Send Email’ 缓冲区溢出漏洞	高	否
电信	CNVD-2015-07713	D-Link DIR-816L 跨站请求伪造漏洞	中	是
电信	CNVD-2015-07707	Oracle WebLogic Server 远程代码执行漏洞	中	是
电信	CNVD-2015-07738	Cisco Firepower 9000 Series Switches 点击劫持漏洞	中	否
电信	CNVD-2015-07742	Cisco Firepower 9000 Series Switches HTML 注入漏洞	中	否
电信	CNVD-2015-07749	IBM WebSphere Application Server 远程	高	是

		代码执行漏洞		
电信	CNVD-2015-07748	Huawei 路由器 VPN 路由转发跳跃漏洞	中	是
电信	CNVD-2015-07756	多款 Huawei eSpace 交换机拒绝服务漏洞	中	是
电信	CNVD-2015-07754	多款 Huawei 路由器信息泄露漏洞	低	是
电信	CNVD-2015-07773	Huawei AR 路由器目录遍历漏洞	中	是
电信	CNVD-2015-07772	Huawei eSpace U2980 和 U2990 拒绝服务漏洞	中	是
电信	CNVD-2015-07794	Huawei AR 路由器 SFTP 服务器目录遍历漏洞	中	是
移动互联网	CNVD-2015-07769	Apple iOSCFNetworkHTTPProtocol 组件存在漏洞	中	是
移动互联网	CNVD-2015-07768	Apple iOS kernel 安全绕过漏洞	中	是
移动互联网	CNVD-2015-07764	Newphoriaapplican 框架跨站脚本漏洞（CNVD-2015-07764）	中	是
移动互联网	CNVD-2015-07763	Newphoriaapplican 框架跨站脚本漏洞	中	是

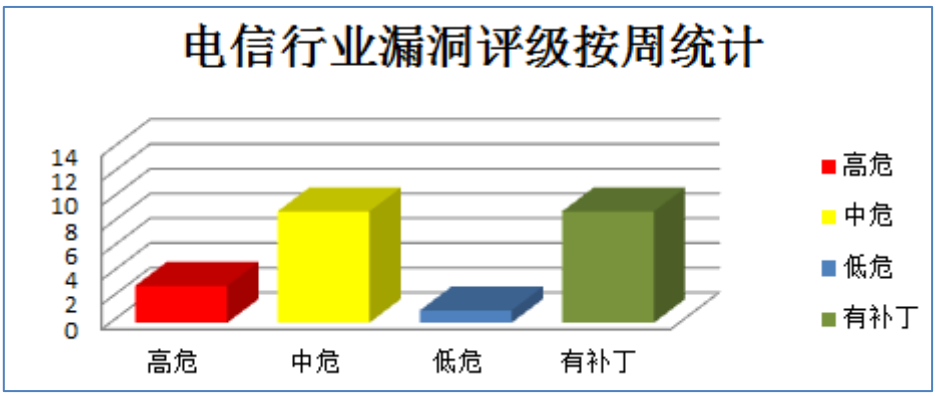

图 1 电信行业漏洞统计

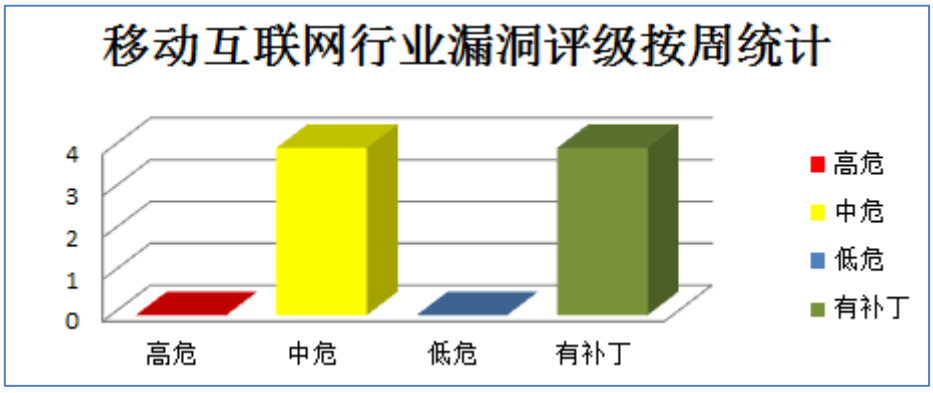

图 2 移动互联网行业漏洞统计

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、 Moodle 产品安全漏洞

Moodle 是一套免费、开源的电子学习软件平台。本周，上述产品被披露存在跨站脚本、安全绕过和拒绝服务漏洞。攻击者利用漏洞可进行跨站脚本攻击、执行未授权操作和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Moodle 拒绝服务漏洞（CNVD-2015-07725）、Moodle 安全绕过漏洞（CNVD-2015-07730、CNVD-2015-07731、CNVD-2015-07732、CNVD-2015-07733、CNVD-2015-07729）、Moodle 跨站脚本漏洞（CNVD-2015-07727、CNVD-2015-07728）。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-2015-07725

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07730

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07731

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07732

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07733

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07729

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07727

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07728

2、 Cisco 产品安全漏洞

Cisco Firepower 9000 是美国思科（Cisco）公司的一套运行于 9000 系列防火墙设备中的操作系统。Cisco Firepower 9000 Series Switches 是美国思科公司（Cisco）9000 系列交换机产品。本周，上述产品被披露存在多个安全漏洞。攻击者利用漏洞可执行命令注入、读取任意文件、进行跨站请求伪造和发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Cisco Firepower 9000 Firepower Extensible 操作系统命令注入漏洞、Cisco Firepower 9000 Firepower Extensible Operating System 文件读取漏洞、Cisco Firepower 9000 Series Switches 点击劫持漏洞、Cisco Firepower 9000 Series 本地拒绝服务漏洞、Cisco Firepower 9000 跨站请求伪造漏洞、Cisco Firepower 9000 Series Switches HTML 注入漏洞、Cisco Firepower 9000 Series 本地命令注入漏洞、Cisco Firepower 9000 Series 存在多个任意文件读取漏洞。目前，厂商已经发布了“Cisco Firepower 9000 Firepower Extensible Operating System 文件读取漏洞、Cisco Firepower 9000 跨站请求伪造漏洞”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-2015-07806

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07760

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07738

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07739

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07740

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07742

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07743

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07744

3、Huawei 产品安全漏洞

Huawei VP9660 是华为视频会议系统的多点控制器。 Huawei AR 系列路由器是基于华为专有 VRP 的下一代企业级路由器，集成了路由、交换、3G、WLAN、语音和安全功能。Huawei eSpace U2980、U2990 是统一网关系列产品。Huawei VP9660 是中国华为（Huawei）公司的一款新一代专业型全高清视频会议终端产品。Huawei eSpace 8950 是中国华为（Huawei）公司的一款智能视频话机产品。Huawei eSpace U2980 和 U2990 都是中国华为(Huawei)公司的电话交换机产品。Huawei AR Routers 是中国华为(Huawei)公司的 AR 系列路由器产品。Huawei eSpace U1900 是统一网关系列产品。本周，上述产品被披露存在信息泄露、目录遍历、安全绕过和拒绝服务漏洞。攻击者利用漏洞可获得敏感信息、执行未授权操作和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Huawei VP9660 信息泄露漏洞、Huawei AR 路由器 SFTP 服务器目录遍历漏洞、Huawei eSpace U2980/2990 拒绝服务漏洞、Huawei VP9660 远程安全绕过漏洞、Huawei eSpace 8950 IP Phone 拒绝服务漏洞、Huawei eSpace U2980 和 U2990 拒绝服务漏洞、Huawei AR 路由器目录遍历漏洞、Huawei eSpace 统一网关拒绝服务漏洞。其中，“Huawei VP9660 信息泄露漏洞、Huawei eSpace 统一网关拒绝服务漏洞”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-2015-07795

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07794

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07793

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07799

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07771

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07772

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07773

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07750

4、IBM 产品安全漏洞

IBM Sterling B2B Integrator 是美国 IBM 公司的一套集成了重要的 B2B 流程、交易和关系的软件。IBM i Access for Windows 是美国 IBM 公司的一套提供访问和使用各种不同的 Windows 操作系统的桌面资源的客户端解决方案。IBM Installation Manager 是美国 IBM 公司的一套可运行在多种平台（如 IBM i、OS、Windows、Linux、Unix）上的通用软件管理工具。WebSphere 是 IBM 的集成软件平台。IBM Java SDK 是一款 Java 实

现平台。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、执行任意代码和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：IBM Sterling B2B Integrator 跨站脚本漏洞（CNVD-2015-07814）、IBM i Access for Windows 本地拒绝服务漏洞、IBM i Access for Windows 本地缓冲区溢出漏洞、IBM Installation Manager ‘/tmp’本地命令注入漏洞、IBM WebSphere Application Server 远程代码执行漏洞、IBM Java SDK 本地信息泄露漏洞。其中，“IBM WebSphere Application Server 远程代码执行漏洞”的综合评级为“高危”。目前，厂商已发布了除“IBM Installation Manager ‘/tmp’本地命令注入漏洞”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-2015-07814

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07816

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07815

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07770

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07749

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07714

5、D-Link DIR-601 命令注入漏洞

D-Link DIR-601 是友讯\公司的一款无线路由器产品。本周，D-Link DIR-601 被披露存在命令注入漏洞。攻击者利用该漏洞可执行任意 OS 命令。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-2015-07696

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-2015-07715	Jenkins 远程代码执行漏洞	高	用户可联系供应商获得补丁信息：http://jenkins-ci.org/
CNVD-2015-07722	Adobe Premiere Clip 存在未明漏洞	高	用户可联系供应商获得补丁信息：http://www.adobe.com/
CNVD-2015-07753	SQLite fts3_tokenizer 远程代码执行漏洞	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.sqlite.org
CNVD-2015-07757	Novell openSUSEdracut 程序包符号链接漏洞	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://lists.opensuse.org/opensuse-updates/2015-11/msg00098.html

CNVD-2015-07767	Tibbo Technology AggreGate 权限提升漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：http://aggregate.tibbo.com/downloads.html
CNVD-2015-07766	Tibbo Technology AggreGate 远程代码执行漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：http://aggregate.tibbo.com/downloads.html
CNVD-2015-07775	AlienVault Unified Security Management 远程代码执行漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页：http://www.alienvault.com/
CNVD-2015-07789	CSL DualCom GPRS CS2300-R SPT 任意命令执行漏洞	高	暂无
CNVD-2015-07798	Proftpd 堆溢出漏洞	高	暂无
CNVD-2015-07797	Arista EOS 远程任意代码执行漏洞	高	用户可联系供应商获得补丁信息：https://www.arista.com

表 3 部分高危漏洞列表

小结：本周，Moodle 产品被披露存在跨站脚本、安全绕过和拒绝服务漏洞。攻击者利用漏洞可进行跨站脚本攻击、执行未授权操作和发起拒绝服务攻击。Cisco、Huawei、IBM 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、执行任意代码和发起拒绝服务攻击等。此外，D-Link DIR-601 被披露存在一个高危漏洞，攻击者利用该漏洞可执行任意 OS 命令。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、Red Hat 修补 Enterprise Linux (RHEL)产品漏洞

Red Hat Enterprise Linux（RHEL）是美国红帽（Red Hat）公司维护和发布的一套面向企业用户的 Linux 操作系统。

本周，Red Hat 修补了上述产品存在的代码执行漏洞，避将攻击者利用漏洞执行 non-verified 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/67210

本周要闻速递

1. 谷歌可远程更改安卓设备密码，影响 74%设备

根据纽约地区检察官办公室的一份报告所述，只要有法院命令，谷歌能够非常容易地远程重置旧版本 Android 系统的密码，调查人员可以轻易地查看设备上的内容。这份报告同时指出运行 Android 5.0（及更新的系统）的设备将无法进行远程重置，因为新系统采用全盘加密，虽然很多设备上这项功能不会默认开启，而早期的 Android 版本就可以进行远程重置。根据 Android Developer Dashboard 的最新数据，约有 74.1%的设备还在运行 Android 4.4 及更早版本的 Android 系统。也就是说，谷歌有能力对 74.1%的 Android 设备进行远程的密码重置操作。

参考链接：http://www.freebuf.com/news/86821.html

2. Chrome 第三方扩展程序被曝光可记录隐私信息

瑞典的安全公司 Detectify 实验室目前表示有些 Chrome 扩展程序会追踪用户的上网历史记录，甚至还包括 Facebook Connect 的私密访问令牌、连接到私有 Dropbox 和 Google Drive 文件。Detectify 实验室安全研究人员称这些 Chrome 扩展程序并未经过用户的同意就开始追踪用户的上网历史记录，甚至有些追踪功能都是默认打开的。也有一些是在隐藏在隐私保护协议里面的。

参考链接：http://www.freebuf.com/news/86932.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