

信息安全漏洞周报

2015 年 05 月 11 日-2015 年 05 月 17 日

2015 年第 20 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 173 个，其中高危漏洞 61 个、中危漏洞 99 个、低危漏洞 13 个。上述漏洞中，可利用来实施远程攻击的漏洞有 150 个。本周收录的漏洞中，已有 142 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“Mediacoder 缓冲区溢出漏洞”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 173 个漏洞。报送情况如表 1 所示。其中，奇虎、安天科技、启明星辰、天融信等单位报送数量较多。此外，CNCERT 各分中心、乌云、漏洞盒子、安徽讯成创安科技有限公司、中国电子科技集团公司第三十研究所及白帽子向 CNVD 提交了 883 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	550	550
安天实验室	191	0
启明星辰	176	0
天融信	144	1
绿盟科技	44	0
乌云	265	265

漏洞盒子	35	35
安徽讯成创安科技有限公司	1	1
中国电子科技集团公司第三十研究所	1	1
CNCERT 宁夏分中心	5	5
CNCERT 甘肃分中心	4	4
个人	21	21
报送总计	1437	883
录入总计	173（去重）	883

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、Mozilla 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	45	26%
2	Adobe	10	6%
3	Mozilla	8	5%
4	WordPress	8	5%
5	IBM	7	4%
6	Apple	6	3%
7	Google	4	2%
8	Docker	4	2%
9	Cisco	3	2%
10	其他	78	45%

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 173 个漏洞。其中应用程序漏洞 122 个，操作系统漏洞 23 个，WEB 应用漏洞 19 个，网络设备漏洞 5 个，安全产品漏洞 3 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	122
操作系统漏洞	23
WEB 应用漏洞	19
网络设备漏洞	5
安全产品漏洞	3
数据库漏洞	1

表 3 漏洞按影响类型统计表

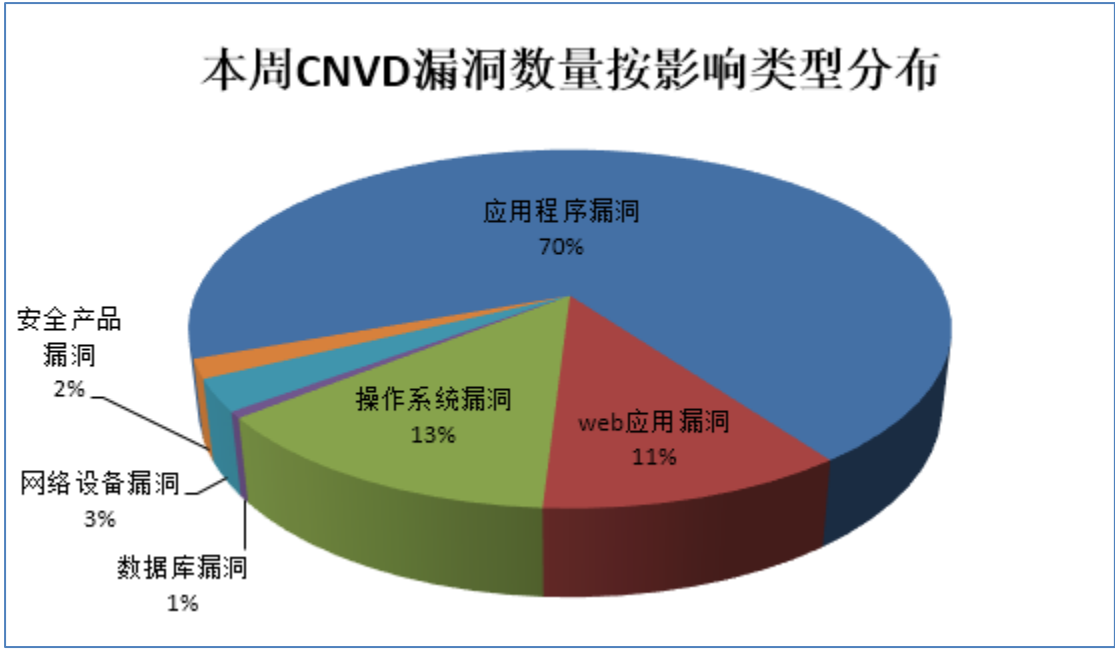


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周,CNVD 收录了 7 个电信行业漏洞,9 个移动互联网行业漏洞(如下图表所示)。其中,“IBM WebSphere Application Server 存在未明任意代码执行漏洞、Google Android 'bindBackupAgent()'函数远程代码执行漏洞”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-2015-02957	IBM WebSphere Application Server 存在未明任意代码执行漏洞	高	是
电信	CNVD-2015-02970	IBM WebSphere Commerce 调试记录本地信息泄露漏洞	低	是
电信	CNVD-2015-02990	Cybertec Series 2000 3G Modem/Router WEB 接口默认管理密码漏洞	中	否
电信	CNVD-2015-03031	Cisco Wireless LAN Controller 存在未明拒绝服务漏洞	中	是
电信	CNVD-2015-03042	Cisco Unified Communications Manage	中	是

		r 存在未明权限提升漏洞		
电信	CNVD-2015-03047	Cisco Unity Connection CUCReports Web 接口跨站请求伪造漏洞	中	是
电信	CNVD-2015-03056	F5 BIG-IP Application Security Manager JSON 内容处理 ASM 过滤绕过漏洞	中	否
移动互联网	CNVD-2015-02960	Siemens HomeControl for Room Automation for Android SSL 证书中间人攻击漏洞	中	是
移动互联网	CNVD-2015-02967	wpa_supplicant/hostapd 零长度处理空指针引用拒绝服务漏洞	中	是
移动互联网	CNVD-2015-02966	wpa_supplicant/hostapd eap_peer/eap_pwd.c eap_pwd_perform_confirm_exchange()函数越界读漏洞	中	是
移动互联网	CNVD-2015-02965	wpa_supplicant/hostapd eap_server/eap_server_pwd.c eap_pwd_process_confirm_response()函数越界读漏洞	中	是
移动互联网	CNVD-2015-02964	wpa_supplicant/hostapd ap/wmm.c hostapd_wmm_action() WMM action 帧处理整数溢出漏洞	中	是
移动互联网	CNVD-2015-02963	wpa_supplicant/hostapd eap_server/eap_server_pwd.c eap_pwd_process_commit_response()越界读漏洞	中	是
移动互联网	CNVD-2015-03002	Google Android 'bindBackupAgent()'函数远程代码执行漏洞	高	是
移动互联网	CNVD-2015-03001	Google Android adb backup 'server/BackupManagerService.java'目录遍历漏洞	中	是
移动互联网	CNVD-2015-03000	Google Android 目录遍历漏洞	中	否

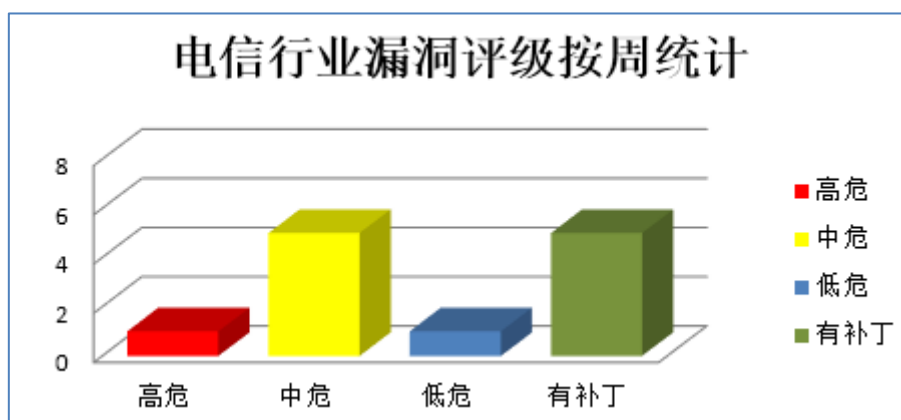


图 1 电信行业漏洞统计

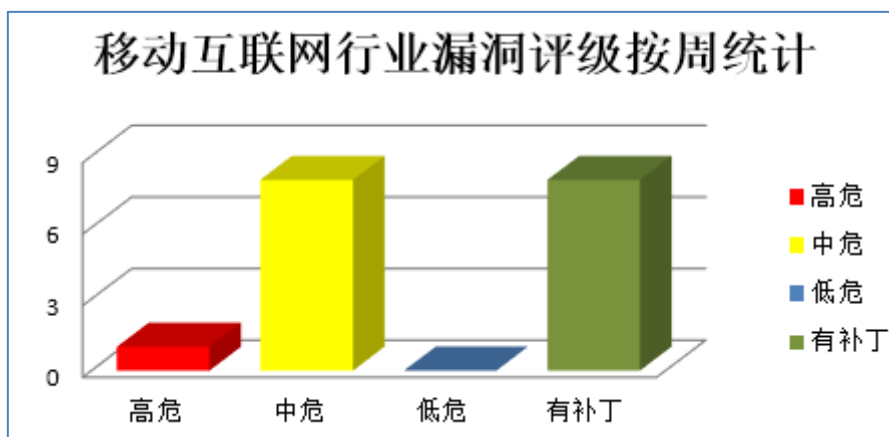


图 2 移动互联网系统行业漏洞统计

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、Microsoft 产品安全漏洞

5 月 12 日，微软发布了 2015 年 5 月份的月度例行安全公告，共含 13 项更新，修复了 Microsoft Windows、Internet Explorer、Office、.NET Framework、Lync、Silverlight 和 Server 软件中存在的 48 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，获得敏感信息，或进行拒绝服务攻击。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer 内存破坏漏洞（CNVD-2015-03096、CNVD-2015-03097、CNVD-2015-03098、CNVD-2015-03099、CNVD-2015-03090、CNVD-2015-03091、CNVD-2015-03092、CNVD-2015-03093）。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/3629>

2、IBM 产品安全漏洞

IBM Java 是一款 JRE 运行时环境。IBM WebSphere Application Server 是一款商业性质的 WEB 应用服务程序。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：IBM JDK Java 信息泄露漏洞、IBM JDK Java 拒绝服务漏洞、IBM JDK Java 虚拟机权限提升漏洞、IBM WebSphere Application Server 存在未明任意代码执行漏洞。其中，“IBM WebSphere Application Server 存在未明任意代码执行漏洞”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-2015-03030>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03032>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03033>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02957>

3、Mozilla 产品安全漏洞

Mozilla Firefox 是一款流行的开源 WEB 浏览器。本周, 上述产品被披露存在多个安全漏洞。攻击者可利用漏洞执行未授权操作、获取敏感信息、提升权限或执行任意代码。

CNVD 收录的相关漏洞包括: Mozilla Firefox 'WebChannel.jsm'同源策略绕过漏洞、Mozilla Firefox 'updater.exe'进程权限提升漏洞、Mozilla Firefox 条件竞争内存错误引用漏洞、Mozilla Firefox MP4 文件解析越界读漏洞、Mozilla Firefox referrer 策略绕过漏洞、Mozilla Firefox 'asm.js'越界读写漏洞、Mozilla Firefox 存在未明内存破坏漏洞 (CNVD-2015-03121、CNVD-2015-03122)。其中, “Mozilla Firefox 'asm.js'越界读写漏洞、Mozilla Firefox 存在未明内存破坏漏洞 (CNVD-2015-03121、CNVD-2015-03122)” 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-2015-03115>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03116>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03117>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03118>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03119>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03120>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03121>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03122>

4、Adobe 产品安全漏洞

Adobe Reader/Acrobat 是流行的处理 PDF 文件的应用程序。本周, 上述产品被披露存在 Javascript API 执行限制绕过漏洞。攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括: Adobe Reader/Acrobat Javascript API 执行限制绕过漏洞 (CNVD-2015-03077、CNVD-2015-03078、CNVD-2015-03079、CNVD-2015-03080、CNVD-2015-03081、CNVD-2015-03082、CNVD-2015-03083、CNVD-2015-03084)。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-2015-03077>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03078>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03079>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03080>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03081>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03082>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03083>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03084>

5、HP ThinPro OS /usr/bin/hpobl 权限提升漏洞

HP ThinPro OS 是瘦客户端操作系统。本周，HP ThinPro OS 被披露存在综合评级为“高危”的权限提升漏洞。攻击者利用该漏洞可以 root 权限访问设备。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-2015-02959>

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-2015-02948	phpMyBackupPro 存在未明代码注入漏洞（CNVD-2015-02948）	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.phpmybackuppro.net/
CNVD-2015-02947	phpMyBackupPro 存在未明代码注入漏洞（CNVD-2015-02947）	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.phpmybackuppro.net/
CNVD-2015-02946	phpMyBackupPro 存在未明代码注入漏洞（CNVD-2015-02946）	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.phpmybackuppro.net/
CNVD-2015-02950	phpMyBackupPro 多用户模式 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://www.phpmybackuppro.net/
CNVD-2015-02982	Module::Signature Module for Perl Test Phase 存在未明任意代码执行漏洞	高	暂无
CNVD-2015-03034	AlienVault OSSIM Plugin ID SQL 注入漏洞	高	暂无
CNVD-2015-03035	AlienVault OSSIM NBE hostname/IP 处理命令执行漏洞	高	暂无
CNVD-2015-03036	AlienVault OSSIM NBE 协议 SQL 注入漏洞	高	暂无
CNVD-2015-03016	Pimcore /misc/http-error-log _dc 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://pimcore.org/
CNVD-2015-03015	Pimcore /reports/newsletter/send HOST 参数命令执行漏洞	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://pimcore.org/
--	--	--	---

表 3 部分高危漏洞列表

小结：本周，微软发布了 2015 年 5 月份的月度例行安全公告，共含 13 项更新，修复了 Microsoft Windows、Internet Explorer、Office、.NET Framework、Lync、Silverlight 和 Server 软件中存在的 48 个安全漏洞。此外，IBM、Mozilla、Adobe 多款产品被披露存在多个安全漏洞，允许攻击者利用漏洞获取敏感信息、提升权限、发起拒绝服务攻击或者执行任意代码。另外，HP ThinPro OS 被披露存在一个高危零日漏洞，攻击者利用该漏洞可以 root 权限访问设备。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 Struts 产品漏洞

Apache Struts 是一款建立 Java web 应用程序的开放源代码架构。

本周，Apache 修补了上述产品存在的安全漏洞，避免攻击者利用漏洞对内部应用程序状态进行攻击。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/58390>

本周要闻速递

1. PHP Hash 比较存在缺陷，影响大量 Web 网站登录认证、忘记密码等关键业务

最近一个被称为“Magic Hash”的 PHP 漏洞可以使得攻击者非法获取用户的账号信息。该漏洞源于 PHP 在处理哈希字符串时，会利用“!=”或“==”来对哈希值进行比较，它把每一个以“0E”开头的哈希值都解释为 0，所以如果两个不同的密码经过哈希以后，其哈希值都是以“0E”开头的，那么 PHP 将会认为他们相同，都是 0。攻击者可以利用这一漏洞，通过输入一个经过哈希后以“0E”开头的字符串，即会被 PHP 解释为 0，如果数据库中存在这种哈希值以“0E”开头的密码的话，他就可以以这个用户的身份登录进去，尽管并没有真正的密码。

参考链接：<http://www.freebuf.com/news/67007.html>

2. 美电信巨头 Verizon 曝有重大安全漏洞，泄露客户所有信息

近日，美电信巨头 Verizon 曝有重大安全漏洞，泄露客户所有信息。该漏洞之所以存在，主要因为 Verizon 的客服网站是通过客户的计算机 IP 地址来区分每一个客户。而这个 IP 地址是由客户的互联网服务提供商提供。因此客服网站判断的依据是，客户是

否以一个 Verizon 可以识别的 IP 地址来访问他们的网站。因为这些 IP 地址对于每个家庭网络客户来说都是独一无二的，所以当它遇到一个可识别的 IP 地址时，它将知道该 IP 地址对应的用户的信息，并且会自动显示客户位置信息、姓名、电话号码以及邮箱地址，而这些信息正是控制 Verizon 账户所需要的。目前，该漏洞已经修复。

参考链接：<http://www.freebuf.com/news/67398.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