

信息安全漏洞周报

2015 年 07 月 13 日-2015 年 07 月 19 日

2015 年第 29 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 229 个，其中高危漏洞 103 个、中危漏洞 120 个、低危漏洞 6 个。上述漏洞中，可利用来实施远程攻击的漏洞有 222 个。本周收录的漏洞中，已有 193 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“HansoPlayer '.wav'文件处理内存破坏漏洞”、“MantisBT SQL 注入漏洞（CNVD-2015-04521）”等零日攻击代码，请使用相关产品的用户注意加强防范。

本周，意大利软件开发商 Hacking Team 公司信息泄露事件的影响持续发酵，其中涉及 Abode Flash 被披露存在三个高危 0day 漏洞（分别对应 CVE-2015-5119、CVE-2015-5122、CVE-2015-5123），攻击者利用漏洞执行任意代码或者发起拒绝服务攻击，目前，Adobe 已经发布补丁及新版本修复了目前存在的三个 0day 漏洞。请相关用户紧急更新。

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 229 个漏洞。报送情况如表 1 所示。其中，天融信、启明星辰、奇虎、安天实验室等单位报送数量较多。此外，CNCERT 各分中心、北京国舜科技有限公司、乌云、漏洞盒子及白帽子向 CNVD 提交了 527 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
天融信	214	0
奇虎	200	200
启明星辰	165	0

安天实验室	99	0
绿盟科技	76	0
恒安嘉新	56	0
乌云	267	267
漏洞盒子	42	42
北京国舜科技有限公司	1	1
CNCERT 福建分中心	4	4
CNCERT 山西分中心	1	1
CNCERT 天津分中心	1	1
个人	11	11
报送总计	1137	527
录入总计	229（去重）	527

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Adobe、Microsoft、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	Adobe	57	25%
2	Microsoft	30	13%
3	Cisco	17	7%
4	IBM	16	7%
5	WordPress	14	6%
6	TYPO3	6	3%
7	Drupal	4	2%
8	Pivotx	3	1%
9	OpenStack	3	1%
10	其他	79	35%

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 229 个漏洞。其中应用程序漏洞 165 个, WEB 应用漏洞 40 个, 网络设备漏洞 19 个, 操作系统漏洞 4 个, 安全产品漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	165
WEB 应用漏洞	40
网络设备漏洞	19
操作系统漏洞	4
安全产品漏洞	1

表 3 漏洞按影响类型统计表

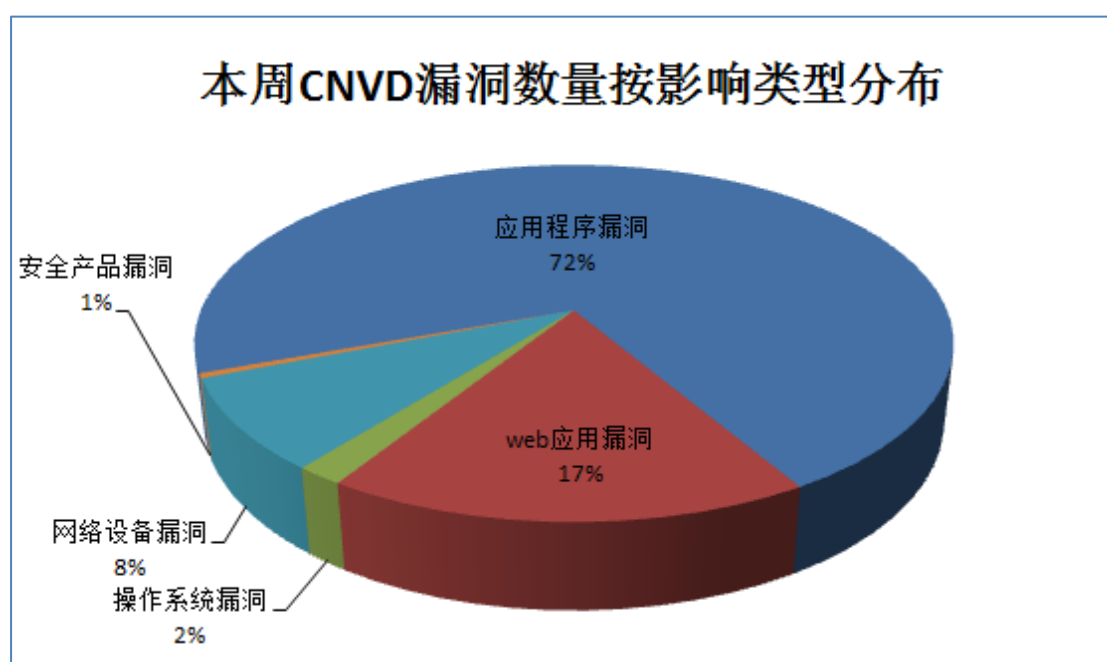


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周, CNVD 收录了 12 个电信行业漏洞 (如下图表所示)。其中, “IBM WebSphere Application Server 和 WebSphere Virtual Enterprise 本地提权漏洞”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。本周末收录移动互联网和工业控制系统行业相关的漏洞。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2015-04402	IBM Business Process Manager 和 WebSphere Lombardi Edition 安全绕过漏洞	中	是

电信	CNVD-2015-04412	IBM WebSphere Application Server 和 WebSphere Virtual Enterprise 本地提权漏洞	高	是
电信	CNVD-2015-04437	Cisco ASR 1000 IOS XE PPPoE 进程拒绝服务漏洞	中	是
电信	CNVD-2015-04445	Cisco TelePresence MCU 4500 设备跨站请求伪造漏洞	中	否
电信	CNVD-2015-04451	Cisco TelePresence IP Gateway 设备跨站请求伪造漏洞	中	否
电信	CNVD-2015-04452	Cisco TelePresence Serial Gateway 设备跨站请求伪造漏洞	中	否
电信	CNVD-2015-04463	IBM WebSphere Portal 信息泄露漏洞(CNVD-2015-04463)	中	是
电信	CNVD-2015-04462	IBM WebSphere Portal 跨站脚本漏洞(CNVD-2015-04462)	中	是
电信	CNVD-2015-04461	IBM WebSphere Portal 跨站脚本漏洞(CNVD-2015-04461)	中	是
电信	CNVD-2015-04505	IBM WebSphere Application Server 会话劫持漏洞	中	是
电信	CNVD-2015-04580	Cisco NX-OS 'tar'命令校验权限提升漏洞	中	是
电信	CNVD-2015-04576	IBM Tivoli Federated Identity Manager 跨站脚本漏洞 (CNVD-2015-04576)	中	是

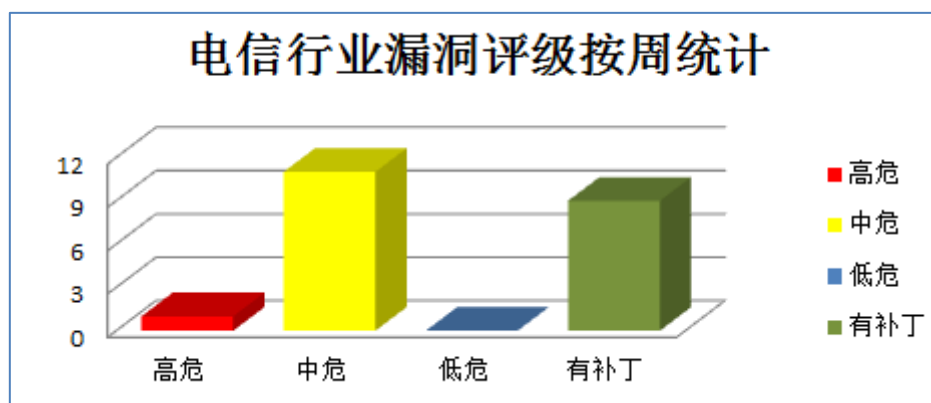


图 1 电信行业漏洞统计

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、Adobe 产品安全漏洞

Adobe Flash Player 是一个解析 SWF 内容的播放器。Adobe AIR 是针对网络与桌面应用的结合所开发出来的技术，可以不必经由浏览器而对网络上的云端程式做控制。

本周，上述产品被披露存在任意代码执行和内存错误引用漏洞，攻击者可利用漏洞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：Adobe Flash Player ActionScript 3 内存错误引用漏洞、Adobe Flash Player 及 AIR 内存错误引用任意代码执行漏洞、Adobe Flash Player 及 AIR 内存错误引用代码执行漏洞（CNVD-2015-04509、CNVD-2015-04510、CNVD-2015-04511、CNVD-2015-04512、CNVD-2015-04513、CNVD-2015-04514）。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-2015-04438>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04500>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04509>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04510>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04511>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04512>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04513>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04514>

2、Microsoft 产品安全漏洞

7 月 14 日，微软发布了 2015 年 7 月份的月度例行安全公告，共含 14 项更新，修复了 Microsoft Windows、Internet Explorer、Office 和 SQL Server 中存在的 59 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，涉及的产品主要为：Internet Explorer、Microsoft Windows。利用上述漏洞，攻击者可以执行远程代码，提升权限。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer 内存破坏漏洞（CNVD-2015-04620、CNVD-2015-04619、CNVD-2015-04618、CNVD-2015-04617、CNVD-2015-04616、CNVD-2015-04615、CNVD-2015-04614、CNVD-2015-04613）。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/3661>

3、IBM 产品安全漏洞

IBM WebSphere Application Server 是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。IBM WebSphere Portal 是美国 IBM 公司的一套企业门户软件。该软件能够创建一个联接企业内部和外部的平台，可让员工、客户和供应商等通过该平台访问企业内部数据。IBM InfoSphere Master Data Management (MDM) 是美国 IBM 公司的一套用于帮助组织管理整个企业范围内的主数据（关于客户、供应商、产品和帐户的信息）的解决方案。该方案支持通过协作、操作和分析这三种主数据使用风格集中多个数据领域。本周，上述产品被披露存在会话劫持、

权限提升、跨站脚本和信息泄露漏洞。攻击者可利用漏洞劫持会话、提升权限、进行跨站攻击或获得敏感信息。

CNVD 收录的相关漏洞包括：IBM WebSphere Application Server 会话劫持漏洞、IBM WebSphere Application Server 远程权限提升漏洞（CNVD-2015-04409）、IBM WebSphere Application Server 和 WebSphere Virtual Enterprise 本地提权漏洞、IBM WebSphere Portal 跨站脚本漏洞（CNVD-2015-04461、CNVD-2015-04462、CNVD-2015-04463）、IBM InfoSphere Master Data Management 信息泄露漏洞（CNVD-2015-04440、CNVD-2015-04439）。其中“IBM WebSphere Application Server 远程权限提升漏洞（CNVD-2015-04409）、IBM WebSphere Application Server 和 WebSphere Virtual Enterprise 本地提权漏洞”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-2015-04505>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04409>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04412>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04461>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04462>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04463>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04440>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04439>

4、Cisco 产品安全漏洞

Cisco TelePresence Advanced Media Gateway device 是美国思科（Cisco）公司一款“网真”系统中的高清晰度（HD）媒体网关。Cisco TelePresence MSE 8000 devices 是一套高容量的语音和视频会议媒体服务引擎设备。Cisco TelePresence MCU 4500 是一款多媒体会议网桥产品。Cisco TelePresence IP VCR devices 是一款网真 IP 录像机设备。Cisco TelePresence IP Gateway 是一款网真 IP 网关设备。Cisco TelePresence Serial Gateway 是一款集成了网络和串行视频网络的网关设备。Cisco TelePresence ISDN Gateway 是一款网真 ISDN 视频网关解决方案。该方案提供高清晰度视频、内容共享和加密等功能。Cisco Unified Computing System（UCS）C server 是美国思科（Cisco）公司的统一计算系统（UCS）C 系列服务器。Integrated Management Controller（IMC）是用于其中的一套管理工具，它支持 HTTP、SSH 访问等，并可对服务器进行开机、关机和重启等操作。本周，上述产品被披露存在跨站请求伪造和安全绕过漏洞。攻击者可利用漏洞绕过安全限制和进行跨站请求伪造攻击。

CNVD 收录的相关漏洞包括：Cisco TelePresence Advanced Media Gateway 设备跨站请求伪造漏洞、Cisco TelePresence MSE 8000 设备跨站请求伪造漏洞、Cisco TelePresence MCU 4500 设备跨站请求伪造漏洞、Cisco TelePresence IP VCR 设备跨站请求伪造漏洞、

Cisco TelePresence IP Gateway 设备跨站请求伪造漏洞、Cisco TelePresence Serial Gateway 设备跨站请求伪造漏洞、Cisco TelePresence ISDN Gateway 设备跨站请求伪造漏洞、Cisco Unified Computing System C Integrated Management Controller 安全绕过漏洞。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-2015-04472>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04444>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04445>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04446>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04451>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04452>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04453>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04471>

5、KMPlayer 栈缓冲区溢出漏洞

KMPlayer 是一款基于 Linux、UNIX 操作系统的视频播放器。本周，KMPlayer 被披露存在综合评级为“高危”的栈缓冲区溢出漏洞。攻击者利用该漏洞构建恶意文件，诱使用户解析，可使应用程序崩溃或执行任意代码。目前，互联网上已经出现了针对该漏洞的攻击代码，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-2015-04499>

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-2015-04404	ANTlabsInnGate 固件 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.antlabs.com/products/ig-3100/
CNVD-2015-04413	OpenSSH 'x11_open_helper()' 函数安全绕过漏洞	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.openssh.com/txt/release-6.9
CNVD-2015-04419	Pivotx 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： http://blog.pivotx.net/archive/2015/06/21/pivotx-2311-released

CNVD-2015-04415	WordPress Easy2Map 插件 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： https://wordpress.org/plugins/easy2map/changelog/
CNVD-2015-04426	redcarpet 栈缓冲区溢出漏洞	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://github.com/vmg/redcarpet/blob/master/CHANGELOG.md
CNVD-2015-04424	cups-filters 'texttopdf'堆缓冲区溢出漏洞	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://bzi.linuxfoundation.org/loggerhead/openprinting/cups-filters/revisions/7363
CNVD-2015-04421	ZOHO ManageEngine Password Manager Pro 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： https://www.manageengine.com/products/passwordmanagerpro/release-notes.html
CNVD-2015-04434	Citrix NetScaler ADC and NetScaler Gateway 远程任意命令执行漏洞	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://support.citrix.com/article/CTX201149
CNVD-2015-04441	SolarWinds Storage Manager AuthenticationFilter 远程命令执行漏洞	高	暂无
CNVD-2015-04448	WordPress ACF Frontend Display 插件任意文件上传漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，Adobe 产品被披露存在任意代码执行和内存错误引用漏洞，攻击者可利用漏洞执行任意代码或发起拒绝服务攻击。此外，Microsoft、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取敏感信息、提升权限、执行任意代码、绕过安全限制、进行跨站脚本和跨站请求伪造攻击或发起拒绝服务攻击。另外，KMPlayer 被披露存在一个高危零日漏洞，攻击者利用该漏洞构建恶意文件，诱使用户解析，可使应用程序崩溃或执行任意代码。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。

CNVD 整理和发布以下重要安全修补信息。

1、Linux 修补 kernel 产品漏洞

Linux kernel 是一款开源的操作系统。

本周，Linux 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/60927>
<http://www.cnvd.org.cn/patchInfo/show/60707>



本周要闻速递

1. Java 曝高危 0day 漏洞，已被俄罗斯黑客组织利用

近日 Java 曝高危 0day 漏洞。攻击者首先会向受害者们发送一封含有 Java 0day 漏洞链接的邮件。一旦用户打开了链接，漏洞利用代码就会释放一个最基本的木马程序 TROJ_DROPPR.CXC，该程序进而会在 "/login user" 文件夹中释放一个名为 TSPY_FAKEMS.C 的 payload。之后恶意程序会在 Java 默认设置的情况下执行恶意代码从而入侵系统。

参考链接：<http://www.freebuf.com/news/72484.html>

2. Flash 紧急修复 3 个 Flash 0day 漏洞

13 日，Flash 被爆出三个 0day，分别是 CVE-2015-5119、CVE-2015-5122、CVE-2015-5123，惊到了各家浏览器，Firefox 开发人员在最新版火狐浏览器中将 Flash Player 插件列入屏蔽名单，这就意味着网站上所有 Flash 内容将被禁用，用户不得不自行手动开启 Flash。其中，CVE-2015-5119 在 Flash 18.0.0.203 版本中已得到修复。14 日 Adobe 发布了最新的 18.0.0.209 版本，修复了 CVE-2015-5122 和 CVE-2015-5123 中提到的漏洞。目前，三枚 0day 已经全部修复。

参考链接：<http://www.freebuf.com/news/72387.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