国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2015 年 09 月 14 日-2015 年 09 月 20 日 **2015 年第 38 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 107 个，其中高危漏洞 52 个、中危漏洞 51 个、低危漏洞 4 个。上述漏洞中，可利用来实施远程攻击的漏洞有 92 个。本周收录的漏洞中，已有 86 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“Montala Limited ResourceSpace SQL 注入漏洞”、“SiteFactory CMS 绝对路径遍历漏洞”等零日代码攻击，请使用相关产品的用户注意加强防范。

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 107 个漏洞。报送情况如表 1 所示。其中，启明星辰、奇虎、绿盟科技、安天实验室等单位报送数量较多。此外，CNCERT 各分中心、乌云、漏洞盒子及白帽子向 CNVD 提交了 641 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
启明星辰	287	0
奇虎（补天平台）	243	243
绿盟科技	87	0
安天实验室	63	0
天融信	52	0
恒安嘉新	33	0

乌云	350	350
漏洞盒子	38	38
CNCERT 安徽分中心	2	2
CNCERT 河南分中心	1	1
CNCERT 四川分中心	1	1
个人	6	6
报送总计	1163	641
录入总计	107（去重）	641

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、WordPress、Synology 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	28	26%
2	WordPress	5	5%
3	Synology	5	5%
4	Cisco	4	4%
5	yokogawa	3	3%
6	Seagate Technology	3	3%
7	libvdpau	3	3%
8	Impero	2	2%
9	IBM	2	2%
10	其他	52	47%

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 107 个漏洞。其中应用程序漏洞 69 个，Web 应用漏洞 21 个，操作系统漏洞 11 个，网络设备漏洞 3 个，安全产品漏洞 2 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	69
Web 应用漏洞	21
操作系统漏洞	11
网络设备漏洞	3
安全产品漏洞	2
数据库漏洞	1

表 3 漏洞按影响类型统计表

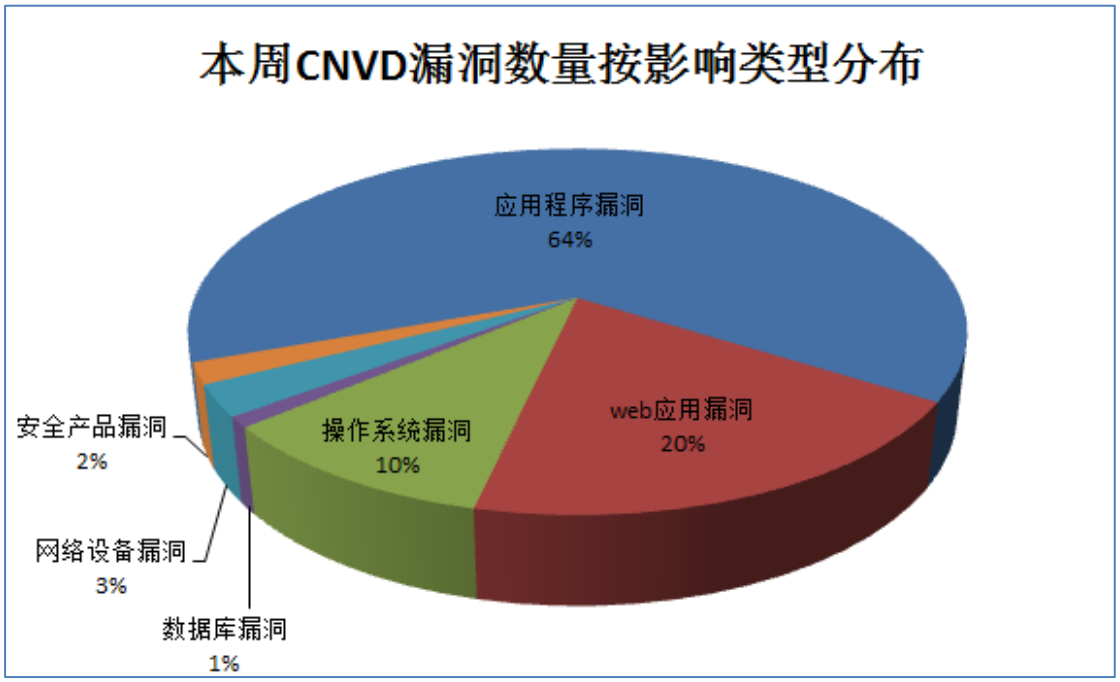

图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 2 个电信行业漏洞、2 个移动互联网行业漏洞、3 个工控系统行业漏洞（如下图表所示）。其中，“Yokogawa 多个产品栈缓冲区溢出漏洞、Yokogawa 多个产品栈缓冲区溢出漏洞（CNVD-2015-05996、CNVD-2015-05995）”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-2015-06026	ASUS TM-AC1900 缓冲区溢出漏洞	高	否
电信	CNVD-2015-06033	IBM WebSphere Portal 拒绝服务漏洞（CNVD-2015-06033）	中	是
移动互联网	CNVD-2015-06049	NTT Broadband Platform Japan Connected-free Wi-Fi 应用程序跨站脚本漏洞	中	是
移动互联网	CNVD-2015-06048	NTT Broadband Platform Japan Connected-free Wi-Fi 应用程序安全绕过漏洞	中	是
工控系统	CNVD-2015-05997	Yokogawa 多个产品栈缓冲区溢出漏洞	高	是

工控系统	CNVD-2015-05996	Yokogawa 多个产品栈缓冲区溢出漏洞（CNVD-2015-05996）	高	是
工控系统	CNVD-2015-05995	Yokogawa 多个产品栈缓冲区溢出漏洞（CNVD-2015-05995）	高	是

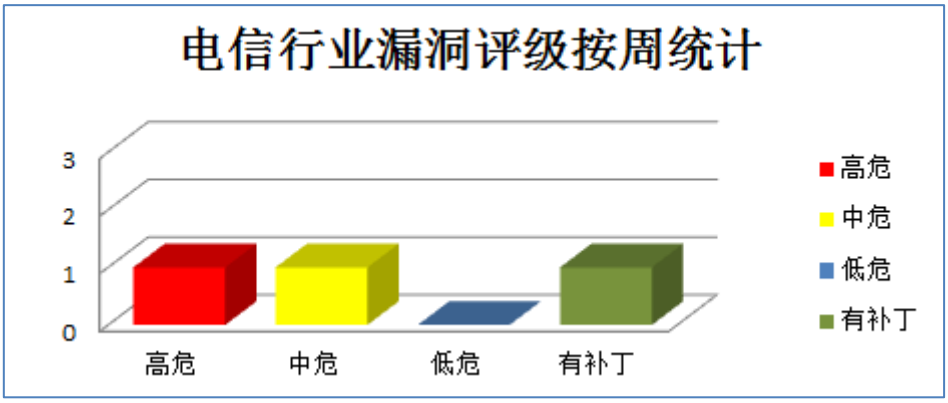

图 1 电信行业漏洞统计

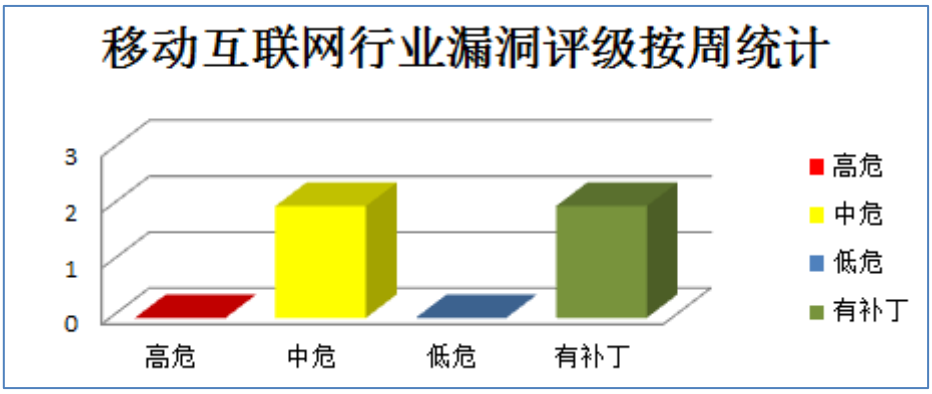

图 2 移动互联网行业漏洞统计

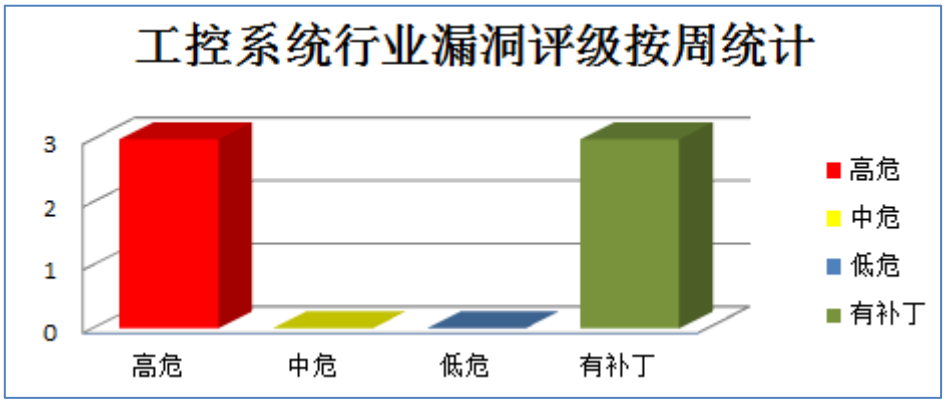

图 3 工控系统行业漏洞统计

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

Microsoft Windows 是美国微软（Microsoft）公司发布的一系列操作系统。本周，上述产品被披露存在权限提升漏洞。攻击者利用漏洞可提升权限。

CNVD 收录的相关漏洞包括：Microsoft Windows 任务管理权限提升漏洞（CNVD-2015-05976、CNVD-2015-05975）、Microsoft Windows Task Scheduler 权限提升漏洞、Microsoft Windows Win32k 权限提升漏洞、Microsoft Windows 字体驱动程序权限提升漏洞（CNVD-2015-05948）、Microsoft Windows Win32k 权限提升漏洞（CNVD-2015-05972、CNVD-2015-05971）、Microsoft Windows 字体驱动程序权限提升漏洞。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/flaw/show/CNVD-2015-05976

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05975

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05974

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05973

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05948

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05972

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05971

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05950

2、 Cisco 产品安全漏洞

Cisco Application Visibility and Control 是应用层分类、监控、流量控制网络设备系列服务；Cisco Web Security Appliance（WSA）是美国思科（Cisco）公司的一套 Web 安全设备；Cisco Content Security Management Appliance 是一款内容安全管理应用。本周，上述产品被披露存在拒绝服务漏洞。攻击者利用漏洞可发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco Application Visibility and Control 拒绝服务漏洞、Cisco Web Security Appliance 拒绝服务漏洞（CNVD-2015-06006）、Cisco Web Security Appliance 拒绝服务漏洞、Cisco Content Security Management Appliance 日志翻转拒绝服务漏洞。目前，厂商已经发布了“Cisco Application Visibility and Control 拒绝服务漏洞、Cisco Web Security Appliance 拒绝服务漏洞”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-2015-06016

http://www.cnvd.org.cn/flaw/show/CNVD-2015-06006

http://www.cnvd.org.cn/flaw/show/CNVD-2015-06005

http://www.cnvd.org.cn/flaw/show/CNVD-2015-05977

3、 Synology 产品安全漏洞

Synology Download Station 是群晖（Synology）公司的一套基于 Web 的下载应用程序；Synology Video Station 是群晖（Synology）公司的一款视频管理器。本周，上述产

品被披露存在 SQL 注入、跨站脚本和任意命令执行漏洞。攻击者利用漏洞可获得敏感信息、进行跨站脚本攻击和执行任意命令。

CNVD 收录的相关漏洞包括：Synology Download Station 跨站脚本漏洞（CNVD-2015-06011）、Synology Video Station 任意命令执行漏洞、Synology Video Station SQL 注入漏洞（CNVD-2015-06009、CNVD-2015-06008）、Synology Download Station 跨站脚本漏洞。其中，除“Synology Download Station 跨站脚本漏洞（CNVD-2015-06011）、Synology Download Station 跨站脚本漏洞”外，其余漏洞的综合评级为“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-2015-06011
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06010
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06009
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06008
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06012

4、 IBM 产品安全漏洞

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 WebSphere Application Server（WAS）是美国 IBM 公司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；IBM HTTP Server 是一款附带在 IBM WAS 产品中的免费 Web 服务器。本周，上述产品被披露存在拒绝服务和缓冲区溢出漏洞。攻击者利用漏洞可发起拒绝服务攻击和执行任意代码。

CNVD 收录的相关漏洞包括：IBM WebSphere Portal 拒绝服务漏洞（CNVD-2015-06033）、IBM HTTP Server Administration Server 栈缓冲区溢出漏洞。其中，“IBM HTTP Server Administration Server 栈缓冲区溢出漏洞”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-2015-06033
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06034

5、 Nibbleblog 任意文件上传漏洞

NibbleBlog 是一套博客引擎。本周，NibbleBlog 被披露存在综合评级为“高危”的任意文件上传漏洞。攻击者利用该漏洞可上传文件，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-2015-06053

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-2015-05957	Microsoft Internet Explorer 权限提升漏洞（CNVD-2015-05957）	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://technet.microsoft.com/library/security/ms15-094
CNVD-2015-05958	Microsoft Internet Explorer 脚本引擎内存破坏漏洞	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://technet.microsoft.com/library/security/ms15-094
CNVD-2015-05953	Microsoft .NET Framework 权限提升漏洞（CNVD-2015-05953）	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://technet.microsoft.com/library/security/ms15-101
CNVD-2015-05963	Adobe Shockwave Player 内存破坏漏洞（CNVD-2015-05963）	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://helpx.adobe.com/security/products/shockwave/apsb15-22.html
CNVD-2015-05961	Seagate 及 LaCie 多个无线存储产品硬编码凭证漏洞	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://apps1.seagate.com/downloads/request.html
CNVD-2015-05960	Seagate 及 LaCie 多个无线存储产品直接请求漏洞	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://apps1.seagate.com/downloads/request.html
CNVD-2015-05962	Seagate 及 LaCie 多个无线存储产品无限制上传文件漏洞	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://apps1.seagate.com/downloads/request.html
CNVD-2015-05980	libvdpau 目录遍历漏洞	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.x.org/archives/xorg-announce/2015-August/002630.html

CNVD-2015-05981	libvdpau 权限提升漏洞	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.ubuntu.com/usn/USN-2729-1
CNVD-2015-05991	Adobe Shockwave Player 内存破坏漏洞（CNVD-2015-05991）	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://helpx.adobe.com/security/products/shockwave/apsb15-22.html

表 3 部分高危漏洞列表

小结：本周，Microsoft Windows 产品被披露存在权限提升漏洞。攻击者利用漏洞可提升权限。此外，Cisco、Synology、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、执行任意命令、发起拒绝服务攻击和执行任意代码。另外，NibbleBlog 被披露存在一个高危零日漏洞，攻击者利用该漏洞可上传文件，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。

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 OpenStack Platform/OpenShift Origin 产品漏洞

Red Hat Enterprise Linux OpenStack Platform 是一款企业级的解决方案。Red Hat OpenShift Origin 是美国红帽（Red Hat）公司的一款开源平台即服务（PaaS）产品。

本周，Red Hat 修补了上述产品存在的缓冲区溢出和拒绝服务漏洞，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/64070

http://www.cnvd.org.cn/patchInfo/show/63830

本周要闻速递

1. AirDrop 漏洞：数百万苹果设备可被默默安装恶意应用

AirDrop 是苹果公司开发出来用于在设备间直接快速传输文件的技术，但是安全研究人员 Mark Dowd 却在 iOS 和 OS X 系统中发现了一个严重漏洞，攻击者可以利用该漏洞重写目标设备上的任意文件，即便用户没有选择接收该文件，还可以向设备推送安装恶意应用程序。另外，攻击者还可利用该漏洞执行一个目录遍历攻击，在任意文件系统中书写文件。Dowd 已经向苹果官方报告了该漏洞，苹果也发布了修复措施，但最新的 iOS 9 操作系统还未完全修复该问题。

参考链接：http://www.freebuf.com/news/78625.html

2. 星巴克官网曝严重漏洞

埃及的独立安全研究员 Mohamed M.表示，他在星巴克上发现了三个严重漏洞。黑客可以通过利用其中简单的点击劫持漏洞，获取受害用户账号的权限。这三个漏洞分别是：远程代码执行、远程文件包含（钓鱼攻击）、CSRF（跨站请求伪造）。

参考链接：http://www.freebuf.com/news/78947.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