国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2016 年 01 月 04 日-2016 年 01 月 10 日 **2016 年第 2 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 109 个，其中高危漏洞 32 个、中危漏洞 70 个、低危漏洞 7 个。上述漏洞中，可利用来实施远程攻击的漏洞有 98 个。本周收录的漏洞中，已有 89 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“Joomla! com_informations 组件'themeid'参数 SQL 注入漏洞”、“Joomla com_memorix 组件'index.php' SQL 注入漏洞”等零日代码攻击漏洞，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 108 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、习科网络安全及白帽子向 CNVD 提交了 1022 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)	688	688
天融信	190	0
安天实验室	153	0
启明星辰	115	0
恒安嘉新	113	0
绿盟科技	55	0

H3C	5	0
乌云	288	288
漏洞盒子	18	18
习科网络安全	1	1
CNCERT 甘肃分中心	1	1
个人	24	24
报送总计	1651	1020
录入总计	109（去重）	1020

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Wireshark、IBM、Adobe 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	Wireshark	32	29%
2	IBM	18	17%
3	Adobe	10	9%
4	TheHostingTool	4	4%
5	Silicon Graphics, Inc.	4	4%
6	QEMU	4	4%
7	Samsung	3	3%
8	Wordpress	2	2%
9	Joomla!	2	2%
10	其他	30	26%

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 109 个漏洞。其中应用程序漏洞 93 个，网络设备漏洞 7 个，Web 应用漏洞 7 个，操作系统漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	93
网络设备漏洞	7

Web 应用漏洞	7
操作系统漏洞	2

表 3 漏洞按影响类型统计表

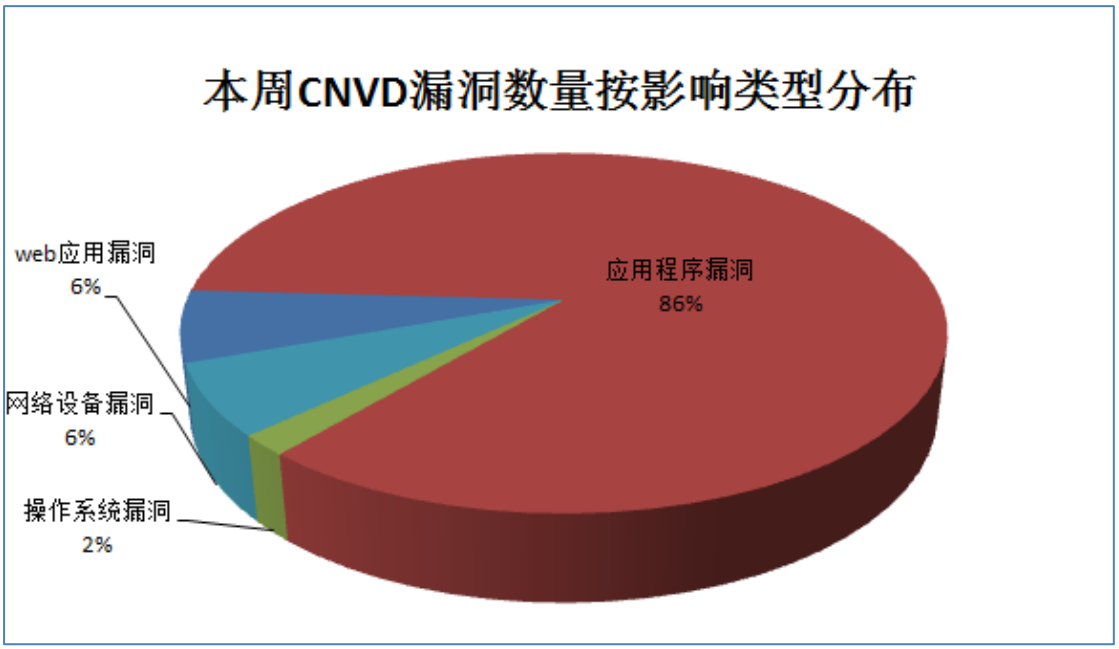

图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 7 个电信行业漏洞（如下图表所示）。其中，“HPE Network Switches 本地安全绕过漏洞”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-2016-00018	ASUS Japan WL-330NUL 设备跨站脚本漏洞	中	是
电信	CNVD-2016-00036	Belkin N600 欺骗漏洞	中	否
电信	CNVD-2016-00078	IBM Cognos Business Intelligence Tivoli Common Reporting 安全绕过漏洞	低	是
电信	CNVD-2016-00077	IBM Cognos Business Intelligence Tivoli Common Reporting 权限提升漏洞	中	是
电信	CNVD-2016-00096	Cisco IOS XR 资源管理错误漏洞	中	是
电信	CNVD-2016-00113	HPE Network Switches 本地安全绕过漏洞	高	是
电信	CNVD-2016-00112	HPE Network Switches 本地安全绕过漏洞（CNVD-2016-00112）	中	是

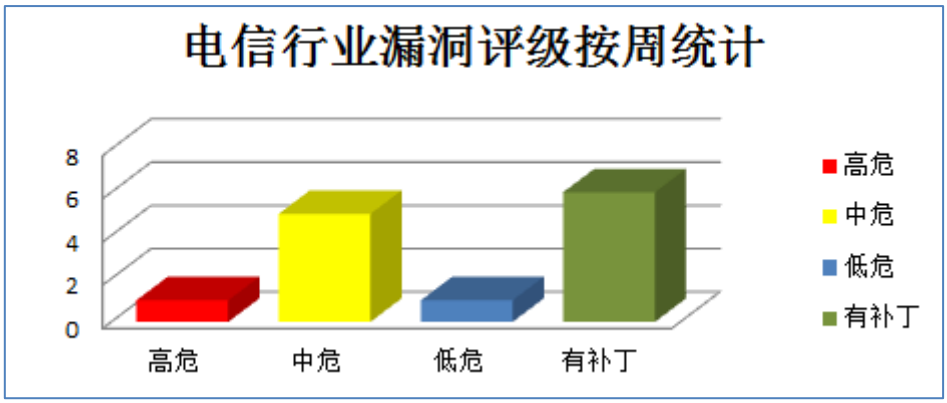

图 1 电信行业漏洞统计

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 是一款多媒体程序播放器。本周，该产品被披露存在内存错误引用和内存破坏漏洞，攻击者利用漏洞可执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Flash Player 内存错误引用漏洞（CNVD-2016-00009、CNVD-2016-00008、CNVD-2016-00007、CNVD-2016-00006、CNVD-2016-00017、CNVD-2016-00015）、Adobe Flash Player 内存破坏漏洞（CNVD-2016-00005、CNVD-2016-00003）。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-2016-00009

http://www.cnvd.org.cn/flaw/show/CNVD-2016-00008

http://www.cnvd.org.cn/flaw/show/CNVD-2016-00007

http://www.cnvd.org.cn/flaw/show/CNVD-2016-00006

http://www.cnvd.org.cn/flaw/show/CNVD-2016-00017

http://www.cnvd.org.cn/flaw/show/CNVD-2016-00015

http://www.cnvd.org.cn/flaw/show/CNVD-2016-00005

http://www.cnvd.org.cn/flaw/show/CNVD-2016-00003

2、 Wireshark 产品安全漏洞

Wireshark 是一款网络协议解析器。本周，该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：Wireshark SCTP 解析器拒绝服务漏洞、Wireshark 802.11 解析器拒绝服务漏洞、Wireshark DIAMETER 解析器拒绝服务漏洞、Wireshark RSVP 解析器拒绝服务漏洞、Wireshark VeriWave 解析器拒绝服务漏洞、Wireshark Mobile

Identity 解析器拒绝服务漏洞、Wireshark Ascend 解析器拒绝服务漏洞、Wireshark BER 解析器拒绝服务漏洞。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-2016-00054

http://www.cnvd.org.cn/flaw/show/CNVD-2016-00056

http://www.cnvd.org.cn/flaw/show/CNVD-2016-00057

http://www.cnvd.org.cn/flaw/show/CNVD-2016-00058

http://www.cnvd.org.cn/flaw/show/CNVD-2016-00059

http://www.cnvd.org.cn/flaw/show/CNVD-2016-00060

http://www.cnvd.org.cn/flaw/show/CNVD-2016-00061

http://www.cnvd.org.cn/flaw/show/CNVD-2016-00062

3、 MediaWiki 产品安全漏洞

MediaWiki 是美国维基媒体（Wikimedia）基金会和 MediaWiki 志愿者共同开发维护的一套免费的基于网络的 Wiki 引擎，它可用于部署内部的知识管理和内容管理系统。本周，该产品被披露存在信息泄露和安全绕过漏洞，攻击者利用漏洞可获得敏感信息和绕过安全限制，执行未授权操作。

CNVD 收录的相关漏洞包括：MediaWiki 安全绕过漏洞（CNVD-2016-00110、CNVD-2016-00111）、MediaWiki 信息泄露漏洞（CNVD-2016-00108）、MediaWiki 远程漏洞、MediaWiki ‘includes/User.php’安全绕过漏洞。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-2016-00110

http://www.cnvd.org.cn/flaw/show/CNVD-2016-00111

http://www.cnvd.org.cn/flaw/show/CNVD-2016-00108

http://www.cnvd.org.cn/flaw/show/CNVD-2016-00109

http://www.cnvd.org.cn/flaw/show/CNVD-2016-00091

4、 QEMU 产品安全漏洞

QEMU 是法国程序员法布里斯-贝拉（Fabrice Bellard）所研发的一套模拟处理器软件。本周，该产品被披露存在缓冲区溢出和拒绝服务漏洞，攻击者利用漏洞可执行任意代码，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：QEMU ‘rocker.c’栈缓冲区溢出漏洞、QEMU 栈缓冲区溢出漏洞、QEMU ‘net/vmxnet3.c’拒绝服务漏洞（CNVD-2016-00106）、QEMU ‘net/vmxnet3.c’拒绝服务漏洞。其中，“QEMU ‘rocker.c’栈缓冲区溢出漏洞、QEMU 栈缓冲区溢出漏洞”的综合评级均为“高危”。目前，厂商已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-2016-00100

http://www.cnvd.org.cn/flaw/show/CNVD-2016-00104

http://www.cnvd.org.cn/flaw/show/CNVD-2016-00106

http://www.cnvd.org.cn/flaw/show/CNVD-2016-00107

5、 Silicon Graphics LibTiff 堆缓冲区溢出漏洞

Silicon Graphics LibTiff 是美国 Silicon Graphics 公司的一个读写 TIFF（标签图像文件格式）文件的库。该库包含一些处理 TIFF 文件的命令行工具。本周，Silicon Graphics LibTiff 被披露存在堆缓冲区溢出漏洞，攻击者可利用漏洞执行任意代码。目前，厂商尚未发布漏洞修补程序。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-2016-00101

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-2016-00010	FreeType 'sfnt/ttsbit.c'堆缓冲区溢出漏洞	高	用户可联系供应商获得补丁信息：http://www.freetype.org/
CNVD-2016-00012	Lepide Software Active Directory Self Service 密码重置漏洞	高	暂无
CNVD-2016-00031	Lenovo Service Engine 远程代码执行漏洞	高	用户可联系供应商获得补丁信息：https://www.lenovo.com/
CNVD-2016-00023	TheHostingTool 任意文件上传漏洞	高	暂无
CNVD-2016-00041	PycURL 远程代码执行漏洞	高	用户可联系供应商获得补丁信息：https://pypi.python.org/pypi/pycurl
CNVD-2016-00040	Samsung LibQjpeg 远程内存破坏漏洞	高	用户可联系供应商获得补丁信息：http://www.samsung.com/
CNVD-2016-00039	Samsung LibQjpeg 远程内存破坏漏洞（CNVD-2016-00039）	高	用户可联系供应商获得补丁信息：http://www.samsung.com/
CNVD-2016-00073	FTPShell client 缓冲区溢出漏洞	高	暂无
CNVD-2016-00105	Ubuntu Vivid 本地提权漏洞	高	暂无
CNVD-2016-00113	HPE Network Switches 本地安全绕过漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c04920918

表 3 部分高危漏洞列表

小结：本周，Adobe 产品被披露存在内存错误引用和内存破坏漏洞，攻击者利用漏洞可执行任意代码。此外，Wireshark、MediaWiki、QEMU 等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、绕过安全限制、执行任意代码和发起拒绝服务攻击等。另外，Silicon Graphics LibTiff 被披露存在一个高危漏洞，攻击者可利用该漏洞执行任意代码。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、Linux 修补 Kernel 产品漏洞

Linux kernel 是 Linux 操作系统所使用的内核。

本周，Linux 修补了 kernel 存在的信息泄露漏洞，避免攻击者利用漏洞获得敏感信息。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/69673

本周要闻速递

1. Joomla 漏洞每天受到黑客 16600 次扫描攻击

据研究人员介绍， Joomla 反序列化远程命令执行漏洞（CVE-2015-8562），每天被黑客发动 16600 次扫描攻击，企图破坏带有该漏洞的网站。由此可见，该漏洞被网络犯罪分子广泛利用，也给互联网造成了严重的经济损失。目前，Joomla 的反序列漏洞，已经在 15 年的 12 月 14 日发布的 3.4.6 版本中修复了该漏洞。

参考链接：http://www.freebuf.com/news/92306.html

2. Comcast Xfinity 家庭安全系统被曝严重漏洞

Comcast（康卡斯特）是美国有线电视公司，也是宽带网络及 IP 电话服务供应商。Xfinity 家庭安全系统是一套月租型的智能家庭监控系统解决方案，提供住宅报警的功能，还可以提供使用者收看有线电视，互联网和电话的服务等服务。近日，研究人员发现 Comcast Xfinity 家庭安全系统中存在一个安全漏洞，攻击者可以在不触发警报的前提下进入用户住宅。厂商尚未发布漏洞修复方案。

参考链接：http://www.freebuf.com/news/92500.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