国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2013 年 01 月 28 日-2013 年 02 月 03 日 **2013 年 第5 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 132 个，其中高危漏洞 46 个、中危漏洞 77 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 126 个。本周收录的漏洞中，已有 102 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。本周互联网上出现“Microsoft Internet Explorer 地址栏 URI 欺骗漏洞”、“多个 Hunt CCTV 设备信息泄露漏洞”等的零日攻击代码，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 6 家成员单位和个人报送了本周收录的全部 132 个漏洞。各单位报送情况如表 1 所示。其中，启明星辰、绿盟科技、恒安嘉新、安天实验室、天融信等单位报送数量较多，个人漏洞研究者向 CNVD 提交了 3 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
启明星辰	120	0
绿盟科技	97	0
恒安嘉新	50	0
安天实验室	44	0
天融信	40	0
东软	3	0
个人	3	3
报送总计	357	3
录入总计	132（去重）	3

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Apple、IBM、WordPress、JBOSS、Wireshark 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	Apple	17	13%
2	IBM	11	8%
3	WordPress	9	7%
4	Wireshark	9	7%
5	JBoss	6	5%
6	Cisco	4	3%
7	Opera	3	2%
8	SAP	3	2%
9	Microsoft	2	1%
10	Novell	2	1%
11	其它	66	51%

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 132 个漏洞。其中应用程序漏洞 90 个，WEB 应用漏洞 21 个，操作系统漏洞 16 个，网络设备漏洞 5 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	90
WEB 应用漏洞	21
网络设备漏洞	5
操作系统漏洞	16
数据库漏洞	0
安全产品漏洞	0

表 3 漏洞按影响类型统计表

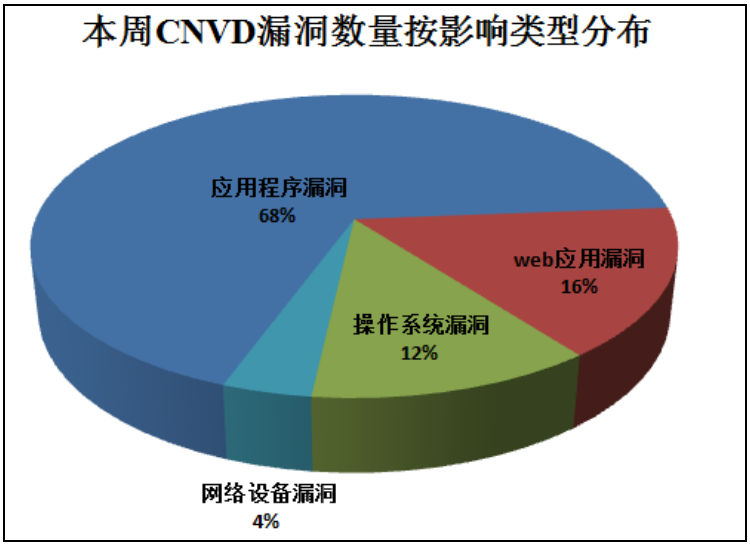

图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 5 个网络设备漏洞：BT Home Hub 'uuid'字段缓冲区溢出漏洞、Cisco Carrier Routing System 存在未明拒绝服务漏洞、D-Link DCS Cameras 验证绕过漏洞、多个 Hunt CCTV 设备信息泄露漏洞、Netgear SPH200D 存在多个漏洞。上述漏洞的综合评级为“中危”。目前，互联网上已经出现了针对“BT Home Hub 'uuid'字段缓冲区溢出漏洞”、“多个 Hunt CCTV 设备信息泄露漏洞”和“Netgear SPH200D 存在多个漏洞”的攻击代码，Dlink 和 Cisco 已经发布了漏洞的修补程序。

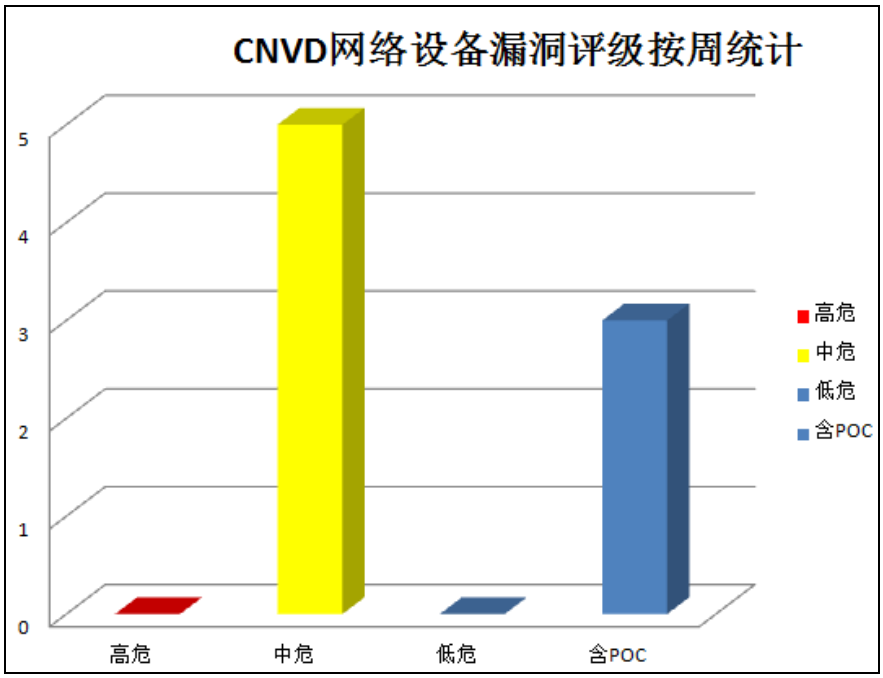

图 2 网络设备漏洞统计

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、Apple 产品安全漏洞

Apple iOS 是一款运行在苹果 iPhone 和 iPod touch 等移动设备上的操作系统。本周，苹果公司发布安全公告，修复了 iOS 系统的多个漏洞。攻击者利用漏洞可获得敏感信息，绕过安全验证，发起拒绝服务攻击或以应用程序上下文执行任意代码。

CNVD 收录的相关漏洞包括：Apple iPhone/iPad/iPod touch webkit 跨站脚本漏洞、Apple iPhone/iPad/iPod touch 内存破坏漏洞（CNVD-2013-19604）、Apple iPhone/iPad/iPod touch 内存破坏漏洞（CNVD-2013-19602）、Apple iPhone/iPad/iPod touch 内存破坏漏洞（CNVD-2013-19600）、Apple iPhone/iPad/iPod touch Safari Javascript 启用漏洞等。除“Apple iPhone/iPad/iPod touch webkit 跨站脚本漏洞”的综合评级为“中危”外，其他均为高危。CNVD 提醒相关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。

此外，Apple QuickTime 本周出现了一个零日拒绝服务漏洞，主要影响其 7.7.3 版本。Apple QuickTime 是一款多媒体播放器，攻击者可以利用该产品漏洞使受影响的应用程序崩溃，拒绝服务合法用户。目前，互联网上已经出现了针对该漏洞的攻击代码，CNVD 提醒相关用户随时关注厂商主页获取最新版本。

参考链接：

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19606

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19604

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19602

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19600

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19589

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19665

2、UPnP 协议 libupnp 函数库安全漏洞

libupnp 是 UPnP 设备可移植的 SDK，提供了 API 和开源代码。本周，该产品被披露存在多个综合评级为“高危”的缓冲区溢出漏洞，攻击者利用漏洞可在受影响设备内执行任意代码。

CNVD 收录的相关漏洞包括：UPnP 协议 libupnp 函数库缓冲区溢出漏洞（CNVD-2013-19636）、UPnP 协议 libupnp 函数库缓冲区溢出漏洞（CNVD-2013-19635）、UPnP 协议 libupnp 函数库缓冲区溢出漏洞（CNVD-2013-19634）、UPnP 协议 libupnp 函数库缓冲区溢出漏洞（CNVD-2013-19633）、UPnP 协议 libupnp 函数库缓冲区溢出漏洞（CNVD-2013-19632）。上述漏洞的综合评级均为“高危”。厂商已发布了上述漏洞的修补程序。CNVD 提醒相关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/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19636

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19635

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19634

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19633

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19632

3、IBM 产品安全漏洞

IBM InfoSphere Information Server 是一款数据集成软件平台。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可提升权限，未授权访问应用，获得敏感信息或执行任意命令。

CNVD 收录的相关漏洞包括：IBM InfoSphere Information Server Suite 密码字段自动完成漏洞、IBM InfoSphere Information Server Suite 存在多个跨站脚本漏洞、IBM InfoSphere Information Server Suite 输入验证漏洞、IBM InfoSphere Information Server Suite 开放重定向漏洞、IBM InfoSphere Information Server Suite 权限提升漏洞（CNVD-2013-19679）、IBM InfoSphere Information Server Suite 权限提升漏洞（CNVD-2013-19678）。其中，“IBM InfoSphere Information Server Suite 输入验证漏洞”的综合评级为“高危”。厂商已发布了上述漏洞的修补程序。CNVD 提醒相关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/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19686

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19684

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19682

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19680

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19679

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19678

4、Wireshark 产品安全漏洞

Wireshark 是一款开源的网络协议分析工具。本周，该产品被披露存在多个漏洞，攻击者利用漏洞可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：Wireshark DTLS 解码器拒绝服务漏洞、Wireshark NTLMSSP 解码器缓冲区溢出漏洞、Wireshark MS-MMC 解码器拒绝服务漏洞、Wireshark PER 解码器拒绝服务漏洞、Wireshark DTN 解码器拒绝服务漏洞。其中，“Wireshark NTLMSSP 解码器缓冲区溢出漏洞”的综合评级为“高危”。厂商已发布了上述漏洞的修补程序。CNVD 提醒相关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/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19661

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19660

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19658

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19657

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19656

5、Microsoft Internet Explorer 零日漏洞

Microsoft Internet Explorer 是一款流行的 WEB 浏览器。本周，该产品被披露存在两个零日漏洞：Microsoft Internet Explorer 信息泄露漏洞（CNVD-2013-19702）、Microsoft Internet Explorer 地址栏 URI 欺骗漏洞。攻击者利用漏洞获得敏感信息或通过发送 HTTP 请求欺骗 WEB 站点。目前，互联网上已经出现了针对上述漏洞的攻击代码，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/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19702

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19699

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/publish/main/52/index.html

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2013-19705	Novell Groupwise Client 不可信指针引用漏洞	高	Novell GroupWise 8.0.3 Hot Patch 2 或 2012 SP1 Hot Patch 1 已经修复此漏洞，建议用户下载使用：http://www.novell.com
CNVD-2013-19692	HP XP P9000 Command View Advanced Edition 存在未明拒绝服务漏洞	高	HP XP P9000 Command View Advanced Edition 7.4.0-00 已经修复此漏洞，建议用户下载使用：http://www.hp.com
CNVD-2013-19691	VLC Media Player ASF 文件处理缓冲区溢出漏洞	高	VLC Media Player 2.0.6 将修复此漏洞，建议用户下载使用：http://www.videolan.org/
CNVD-2013-19689	Broadcom UPnP Stack 'SetConnectionType()'函数格式串漏洞	高	暂无
CNVD-2013-19683	Opera Web Browser SVG 文档处理任意代码执行漏洞	高	Opera Web Browser 12.13 将修复此漏洞，建议用户下载使用：http://www.opera.com
CNVD-2013-19682	IBM InfoSphere Information Server Suite 输入验证漏洞	高	IBM InfoSphere Information Server 8.5 Fix Pack 3 将修复此漏洞，建议用户下载使用：http://www.ibm.com/support/docview.wss?uid=swg24033513

CNVD-2013-19673	GNU glibc 'regexec.c'缓冲区溢出漏洞	高	用户可参考如下厂商提供的安全公告获得补丁信息：http://sourceware.org/ml/libc-alpha/2013-01/msg00967.html
CNVD-2013-19671	Buffalo TeraStation 'dynamic.pl'任意命令注入漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，苹果公司发布安全更新，修复 iOS 系统的多个安全漏洞，建议相关用户尽快更新。本周，UPnP 协议 libupnp 函数库被披露存在多个漏洞，影响涉及目前常用的即插即用设备，包括：网络打印机、路由器、存储设备以及个人电子产品。IBM InfoSphere Information Server 和 Wireshark 也存在多个安全漏洞。CNVD 提醒使用相关产品的用户注意加强防范。此外，Microsoft IE 浏览器被披露存在两个零日漏洞，且攻击代码已在互联网公开，相关用户应随时关注厂商主页，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、 FFmpeg 发布升级程序，修补多个漏洞

FFmpeg 是一款用于录制、转换和流化音频和视频的完整解决方案。本周，FFmpeg 修补了多个漏洞。攻击者可以破坏内存、执行任意代码或发起拒绝服务攻击。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安全事件。

补丁下载链接：

http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=31256

http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=31253

http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=31257

http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=31255

本周要闻速递

1. JetDirect 存漏洞 打印机安全问题再升温

比特网 ChinaByte 1 月 30 日编译报道 打印机并不是网络罪犯入侵企业网络的典型路径。但是最近，该设备却成为安全专家们关注的焦点，他们认为打印机是网络防御中一个被忽略的薄弱环节。最近，英国移动 app 开发者 Andrew Howard 爆料，谷歌发现 8 6800 台 HP 公共打印机可能促使网络罪犯渗透到企业网络或窃取敏感文件，这让打印机安全话题进一步升温。Howard 表示，许多型号的打印机漏洞是已知的，这些漏洞可能会用作私人网络的入口。本月早些时候，viaForensics 研究人员 Sebastian Guerrero 发现

了 JetDirect 中的漏洞，它可能被用于入侵 HP 打印机。JetDirect 技术用于将打印机添加到本地网络，因此很多人能进到设备中。Guerrero 表示，这些漏洞能使人检索到之前打印过的文件。HP 建议用户将打印机置于防火墙之后，并只为那些可信的合作方提供认证。

参考链接：http://sec.chinabyte.com/206/12535706.shtml

2. UPnP 漏洞爆发 数千万个人设备受威胁

网络安全软件厂商 Rapid7 在即将于周二发布的一份白皮书中表示，目前市场上广泛使用的网络技术存在很多漏洞，而这些漏洞使数千万台个人电脑、打印机和存储设备在常规网络环境中就非常容易受到黑客的攻击。计算机路由器和其他网络设备是导致用户个人设备极易受到攻击的根源，因为它们都普遍采用了即插即用（Universal Plug and Play, UPnP）技术。该技术能够让网络更加便捷地识别外部设备并与之进行通讯，这大大节省了网络调试时间。Rapid7 在这份白皮书中指出，该公司研究人员已经从即插即用技术标准中发现了三种相互独立的漏洞，而正是这些漏洞导致全球 4,000 万到 5,000 万台设备极易受到攻击。这些设备的名单中包括数家全球知名网络设备生产商的产品，比如 Belkin、D-Link 以及思科旗下的 Linksys 和 Netgear。

参考链接：http://www.enet.com.cn/article/2013/0130/A20130130239791.shtml

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

国家互联网应急中心的全称是国家计算机网络应急技术处理协调中心（英文简称是 CNCERT 或 CNCERT/CC）成立于 1999 年 9 月，是工业和信息化部领导下的国家级网络安全应急机构，致力于建设国家级的网络安全监测中心、预警中心和应急中心，以支撑政府主管部门履行网络安全相关的社会管理和公共服务职能，支持基础信息网络的安全防护和安全运行，支援重要信息系统的网络安全监测、预警和处置；国家互联网应急中心在我国大陆 31 个省、自治区、直辖市设有分中心。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82990999