国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2012 年 12 月 31 日-2013 年 01 月 06 日 **2013 年第 1 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 116 个，其中高危漏洞 30 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 110 个。本周收录的漏洞中，已有 59 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“Simple Webserver 目录遍历漏洞”、“WordPress TwentyTen Theme 'loo.php'任意文件上传漏洞”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 4 家成员单位和多个合作伙伴报送了本周收录的全部 116 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、安天实验室、恒安嘉新等单位报送数量较多。此外，个人报送者向 CNVD 提交了 1 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	100	0
绿盟科技	36	0
安天实验室	23	0
恒安嘉新	17	0
个人报送者	1	1
报送总计	177	1
录入总计	116（去重）	1

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 WordPress、MoinMoin 、IBM、Opera、Adobe 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	WordPress	16	14%
2	MoinMoin	4	3%
3	IBM	4	3%
4	Opera	3	3%
5	Adobe	3	3%
6	MyBB	3	3%
7	Samsung	2	2%
8	Ruby on Rails	2	2%
9	ownCloud	2	2%
10	Cisco	1	1%
11	其它	76	64%

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 116 个漏洞。其中应用程序漏洞 75 个，WEB 应用漏洞 38 个，网络设备漏洞 3 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	75
WEB 应用漏洞	38
网络设备漏洞	3
操作系统漏洞	0
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

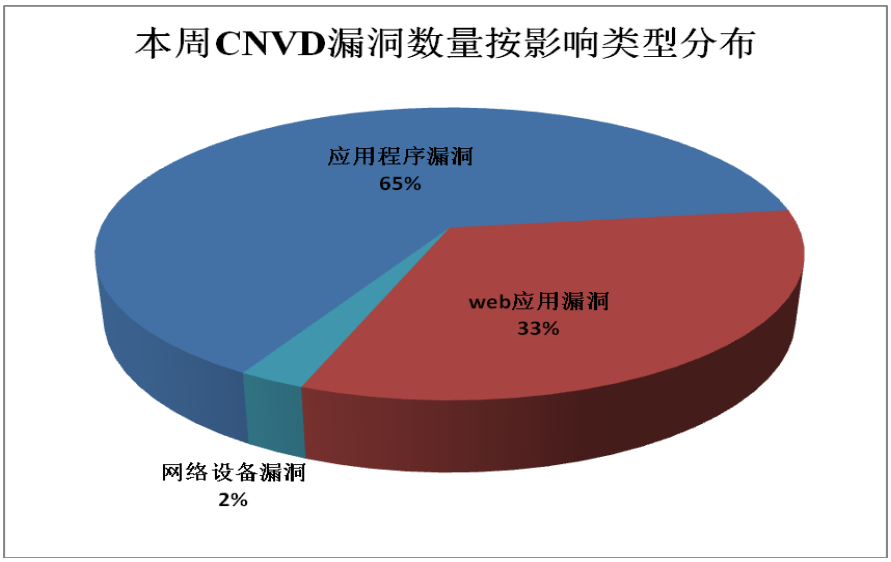

图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 3 个网络设备漏洞：Cisco Unified IP Phone 7900 任意代码执行漏洞、Belkin N900 F9K1104v1 路由器 WPA2 实现漏洞、Aastra 6753i '.tug 配置文件信息泄露漏洞。其中，“Cisco Unified IP Phone 7900 任意代码执行漏洞”的综合评级为“高危”。相关厂商已经发布了漏洞修补程序。

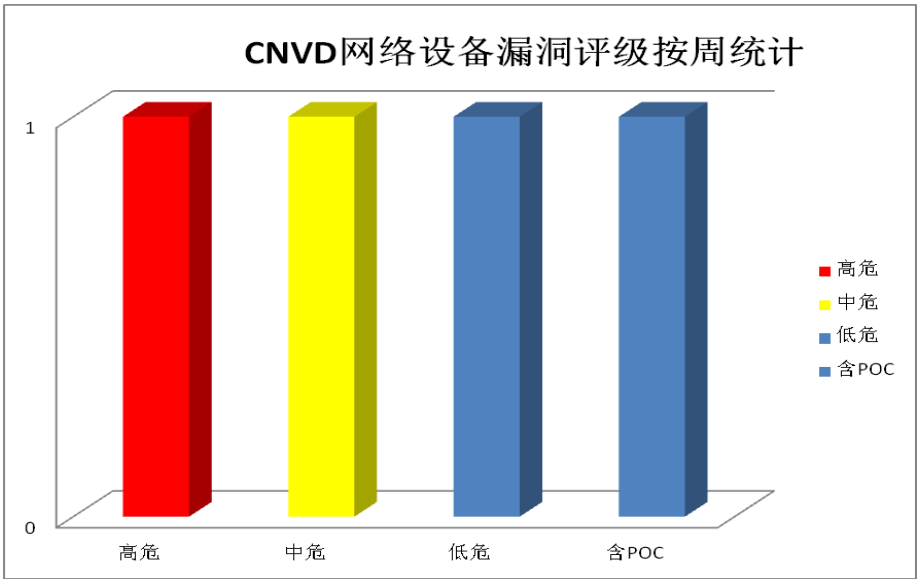

图 2 网络设备漏洞统计

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、Microsoft 产品安全漏洞

Internet Explorer 是微软公司推出的网页浏览器软件。由于 Internet Explorer 在处理 mshtml!CButton 对象时存在内存释放后重用缺陷，攻击者可通过诱使用户访问特定构造的恶意网页（即网页挂马攻击方式），进而在用户主机上执行页面中包含的恶意代码，远程控制用户主机操作系统。受影响版本包括 IE6、7、8。

本周，CNVD 收录了微软公司浏览器软件 Internet Explorer 存在的一个远程代码执行零日漏洞：Microsoft IE mshtml!CButton 对象释放后重用代码执行漏洞（CNVD-2012-18980），该漏洞的综合评级为“高危”。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-2012-18980

2、IBM 产品安全漏洞

IBM InfoSphere Guardium 是一款数据库安全软件，提供企业数据中心中可信信息的安全性和完整性保障功能；IBM SPSS Modeler 是一款数据挖掘平台。本周，上述产品被披露存在多个安全漏洞，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：IBM SPSS Modeler XML 解析存在未明漏洞、IBM InfoSphere Guardium 存在未明漏洞、IBM InfoSphere Guardium 'diag'存在未明漏洞、IBM InfoSphere Guardium 'Dojo'存在漏洞。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-2013-19012

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-18996

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-18994

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-18995

3、Opera 安全漏洞

Opera Web Browser 是一款开源的 WEB 浏览器。本周，该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，构建恶意 WEB 页，诱使用户解析，发起钓鱼等攻击。

CNVD 收录的相关漏洞包括：Opera Web Browser Internet 快捷方式处理错误漏洞、Opera Web Browser 不正确 WebP 图像处理信息泄露漏洞、Opera Web Browser 证书校验状态错误漏洞。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-2013-19027

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19022

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19025

4、Adobe 产品安全漏洞

Adobe ColdFusion 是 Adobe 公司提供的网络应用服务器开发环境套件。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可绕过权限，获取敏感信息。

CNVD 收录的相关漏洞包括：Adobe ColdFusion 受限目录访问漏洞、Adobe ColdFusion 敏感信息泄露漏洞、Adobe ColdFusion 验证绕过漏洞。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-2013-19074

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19075

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19072

5、WordPress TwentyTen Theme 'loo.php'任意文件上传漏洞

WordPress 是一款基于 PHP 的内容管理系统。本周，该产品被披露存在一个综合评级为“高危”的文件上传漏洞。由于 WordPress TwentyTen Theme 插件未能正确处理用户提交的输入，攻击者利用漏洞可上传任意文件并以 WEB 权限执行。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/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19030

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-2013-19070	Ruby on Rails Active Record 组件 SQL 注入漏洞	高	Ruby on Rails 3.0.18，3.1.9 和 3.2.10 已经修复此漏洞，建议用户下载使用：http://www.ruby-lang.org
CNVD-2013-19082	MyBB Profile Wii Friend Code 插件 SQL 注入漏洞	高	暂无
CNVD-2013-19076	WHMCompleteSolution Google Checkout SQL 注入漏洞	高	WHMCompleteSolution 4.5.3 已经修复此漏洞，建议用户下载使用：http://www.whmcs.com
CNVD-2013-19048	osTicket 存在多个输入验证漏洞（CNVD-2013-19048）	高	暂无

CNVD-2013-19045	Ubiquiti AirOS 命令执行漏洞	高	暂无
CNVD-2013-19056	SWI-Prolog 文件名处理缓冲区溢出漏洞	高	用户可参考如下厂商提供的安全公告获得补丁信息：http://www.swi-prolog.org/git/pl.git/commitdiff/b2c88972e7515ada025e97e7d3ce3e34f81cf33e
CNVD-2013-19005	Astium PBX 'logon.php' SQL 注入漏洞	高	暂无
CNVD-2013-19006	Dedecms plus\feedback.php SQL 注入漏洞	高	暂无
CNVD-2012-18989	opLYNX 验证绕过漏洞	高	i-GEN opLYNX 2.01.9 已经修复此漏洞，建议用户下载使用：http://www.cybertech.ca/igen/products_oplynx.html
CNVD-2012-18987	Joomla Content 组件'cont'参数任意文件上传漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，IBM 多款产品以及 Adobe ColdFusion 被披露存在多个漏洞，攻击者利用漏洞可发起拒绝服务攻击或窃取敏感信息，企业用户和开发者用户需加强防范措施；本周，微软 IE 浏览器和 Opera 浏览器被披露存在多个漏洞，可被利用发起挂马、钓鱼等攻击，针对 IE 漏洞的挂马攻击已经被监测到。此外，WordPress 内容管理系统也被披露存在零日漏洞，相关网站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、 Cisco 发布升级程序，修补 Unified IP Phone 设备漏洞

Cisco Unified IP Phone 是思科的统一 IP 电话解决方案。本周，Cisco 修补了 Unified IP Phone 存在的任意代码执行漏洞。攻击者利用漏洞可通过特制的程序执行任意代码或发起由于内存覆盖引起的拒绝服务攻击。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=27075

本周要闻速递

1. 思科 VoIP 电话曝安全漏洞

北京时间 1 月 7 日早间消息，思科的 VoIP 电话中存在严重安全漏洞。通过在思科 VoIP 电话技术中插入恶意代码的方法，从而窃听私人通话。这样的窃听可以在远离通话者的全球任何地点进行。思科已经发布了多个补丁尝试修复这些漏洞，但效果不明显。崔昂表示：“这些补丁没有解决我们向思科指出的基本问题。除了采用软件共生技术，或重新编写固件之外，我们不知道是否还有其他解决这一系统性问题的方案。我们计划在未来一次会议上演示由软件共生技术保护的思科 VoIP 电话。”

参考链接：http://tech.xinmin.cn/2013/01/07/18014774.html

2. 三星修复 Galaxy S III 安全漏洞

1 月 6 日消息，据国外媒体报道，对于上周发现的一个 Galaxy S III 安全漏洞，三星已经发布安全升级，并消除了无故死机的现象。漏洞发现后，三星就为已经 ROOT 的用户提供了一个临时的补丁，但根本解决措施还需要迅速制定出来。今天，三星针对所有 Galaxy S III 推出了正式的安全升级。据了解，这个漏洞不仅会给用户带来安全隐患，还会影响所有使用 Exynos 4 四核处理器的智能手机。据悉，新升级不仅修补了安全漏洞，还对 Galaxy S III 出现的无故死机情况进行了修复。

参考链接：http://tx.southcn.com/shumachanpin/content/2013-01/07/content_61461555.htm

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