国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2013 年 04 月 08 日-2013 年 04 月 14 日 **2013 年第 15 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 164 个，其中高危漏洞 81 个、中危漏洞 62 个、低危漏洞 21 个。上述漏洞中，可利用来实施远程攻击的漏洞有 136 个。本周收录的漏洞中，已有 103 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“WH MCS Group Pay Module 'hash' SQL 注入漏洞”、“PHP Address Book SQL 注入漏洞”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 家成员单位和多个合作伙伴及个人报送了本周收录的全部 164 个漏洞。各单位报送情况如表 1 所示。其中，绿盟科技、启明星辰等单位报送数量较多。此外，江苏分中心、奇虎公司、High-Tech Bridge Security Research Lab 以及个人报送者向 CNVD 提交了 28 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	181	0
绿盟科技	133	0
安天实验室	47	0
天融信	69	0
恒安嘉新	9	0
High-Tech Bridge Security Research Lab	1	1
奇虎 360	3	3
江苏分中心	1	1

个人	23	23
报送总计	467	28
录入总计	164（去重）	28

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Cisco、Microsoft、WordPress、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	Cisco	16	10%
2	Microsoft	14	9%
3	WordPress	12	7%
4	Adobe	9	5%
5	Linux	7	4%
6	IBM	7	4%
7	Apache	5	3%
8	Drupal	2	1%
9	D-Link	2	1%
10	Novell	1	1%
11	其它	89	55%

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 164 个漏洞。其中应用程序漏洞 91 个，WEB 应用漏洞 36 个，操作系统漏洞 17 个，网络设备漏洞 13 个，安全产品漏洞 7 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	91
WEB 应用漏洞	36
网络设备漏洞	13
操作系统漏洞	17
安全产品漏洞	7

表 3 漏洞按影响类型统计表

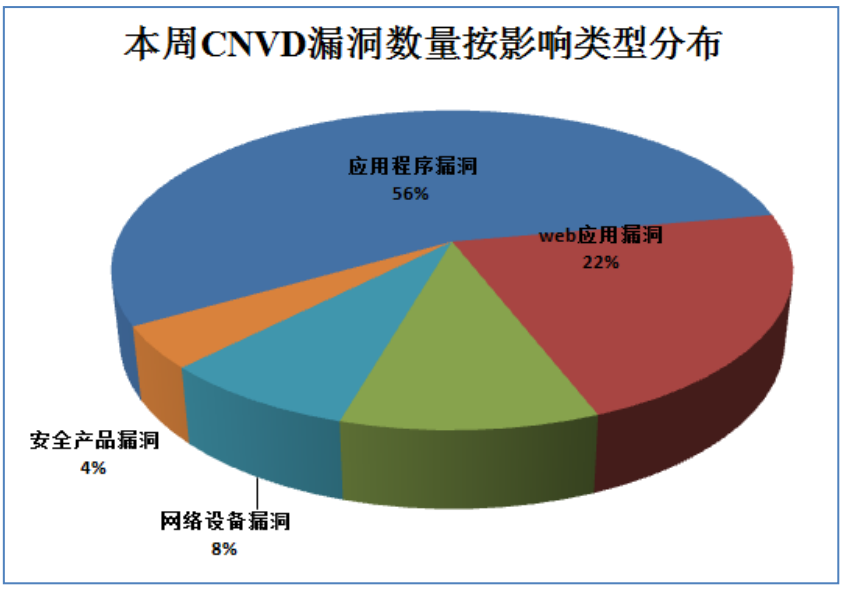

图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 13 个网络设备漏洞：Huawei Secospace VSM 默认用户组权限安全绕过漏洞、Aastra 6753i IP Telephone 内置密码安全绕过漏洞、D-Link 多个产品命令注入漏洞、D-Link 多个产品信息泄露漏洞、Huawei AR 系列路由器 DHCP 报文解析拒绝服务漏洞、TP-Link TD-8817 路由器跨站请求伪造漏洞、Foscam 跨站请求伪造漏洞、多个 Foscam IP Cameras 跨站请求伪造漏洞、Cisco IOS XE IPv6 组播通信处理拒绝服务漏洞、Cisco IOS XE L2TP 通信拒绝服务漏洞、Cisco IOS XE SIP 通信拒绝服务漏洞、Cisco IOS XE 'bridge-domain'接口通信拒绝服务漏洞、Cisco uBR 10000 Series IPv4 /IPv6 地址分配操作拒绝服务漏洞。其中，“Huawei Secospace VSM 默认用户组权限安全绕过漏洞、Aastra 6753i IP Telephone 内置密码安全绕过漏洞、D-Link 多个产品命令注入漏洞、Cisco IOS XE IPv6 组播通信处理拒绝服务漏洞、Cisco IOS XE L2TP 通信拒绝服务漏洞、Cisco IOS XE SIP 通信拒绝服务漏洞、Cisco IOS XE 'bridge-domain'接口通信拒绝服务漏洞”的综合评级均为“高危”，相关厂商已经发布了漏洞修补程序。

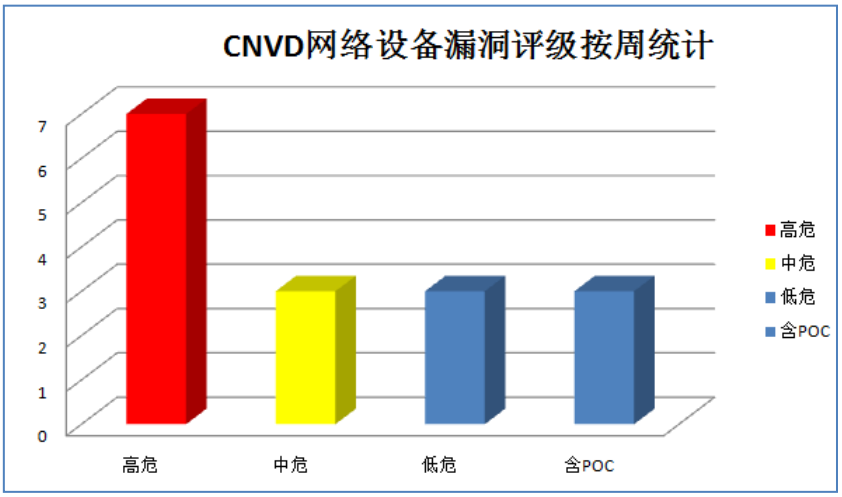

图 2 网络设备漏洞统计

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

4 月 10 日，微软发布了 2013 年 4 月份的月度例行安全公告，共含 9 项更新，修复了涉及 Microsoft Windows 操作系统、Internet Explorer 浏览器、 Office 套件、Microsoft Server 软件（SharePoint Server、Groove Server、SharePoint Foundation）、Office Web Apps、安全软件（Windows Defender）多款产品中存在的多个安全漏洞。其中， MS13-028 和 MS13-029 项更新的综合评级为最高级“严重”级别（微软定义的最高危害级别），其余 7 项更新综合评级均为“重要”级别。利用上述漏洞，攻击者可以执行任意代码，提升权限，进行拒绝服务攻击，获取敏感信息。

CNVD 收录的相关漏洞包括：Microsoft Windows OpenType 字体解析远程拒绝服务漏洞、Microsoft Internet Explorer 内存错误引用远程代码执行漏洞（CNVD-2013-21903、CNVD-2013-21904）、Microsoft Remote Desktop ActiveX Control 远程代码执行漏洞、Microsoft 产品 HTML 过滤 HTML 注入漏洞、Microsoft SharePoint 信息泄露漏洞、Microsoft Windows Active Directory 拒绝服务漏洞、Microsoft Windows CSRSS 本地权限提升漏洞（CNVD-2013-21909）等。CNVD 提醒广大 Microsoft 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/flaw/show/CNVD-2013-21850

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21903

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21904

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21905

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21906

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21907

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21908

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21909

2、Adobe 产品安全漏洞

Adobe Shockwave Player 是一款用于播放使用 Director Shockwave Studio 制作的网页的插件；Adobe Flash Player 是一款 Flash 文件处理程序；Adobe Air 是一款跨操作系统的运行时库；Adobe ColdFusion 是一个动态 Web 服务器。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可获得敏感信息，导致应用程序崩溃，远程执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Shockwave Player 内存破坏漏洞（CNVD-2013-21949、CNVD-2013-21947）、Adobe Shockwave Player 内存信息泄露漏洞、Adobe Shockwave Player 存在未明溢出漏洞、Adobe Flash Player/AIR 内存破坏漏洞（CNVD-2013-21944、CNVD-2013-21942、CNVD-2013-21941）、Adobe ColdFusion 访问绕过漏洞等。上述漏洞的综合评级均为“高危”。厂商已发布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/flaw/show/CNVD-2013-21949

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21948

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21947

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21946

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21944

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21942

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21941

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21940

3、IBM 产品安全漏洞

IBM Cognos Disclosure Management 是一款企业协作和流程自动化解决方案；IBM TRIRIGA Application Platform 是一款用于部署 IBM TRIRIGA 应用程序的可扩充式技术平台；IBM Scale Out Network Attached Storage 是一款集群 NAS 存储系统；IBM IMS Enterprise Suite 是一款信息管理系统企业套件。本周，上述 IBM 产品被披露存在多个安全漏洞，攻击者利用漏洞获得敏感信息，上传任意文件，发起钓鱼攻击，执行任意代码。

CNVD 收录的相关漏洞包括：IBM Cognos Disclosure Management EdrawSoft ActiveX 控件不安全方法漏洞、IBM TRIRIGA Application Platform 存在多个跨站请求伪造漏洞、IBM TRIRIGA Application Platform 存在多个链接注入漏洞、IBM TRIRIGA Application Platform 跨站脚本漏洞、IBM Scale Out Network Attached Storage 信息泄露漏洞、IBM IMS Enterprise Suite SOAP Gateway 不安全验证弱点漏洞。上述漏洞中“IBM Cognos Disclosure Management EdrawSoft ActiveX 控件不安全方法漏洞”的综合评级为“高危”。厂商已发布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/flaw/show/CNVD-2013-21878

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21938

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21937

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21917

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21827

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21810

4、Cisco 产品安全漏洞

Cisco Adaptive Security Appliance 是提供安全和 VPN 服务的模块。Cisco Prime 是一款以服务为中心从终端、网络设备和应用整合管理有线与无线 LAN、WAN 与数据中心，并筛选信息的解决方案。 Cisco AnyConnect VPN Client 是一款 VPN 客户端。本周，上述思科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，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括： Cisco Adaptive Security Appliance 拒绝服务漏洞（CNVD-2013-21971、CNVD-2013-21972、CNVD-2013-21973）、Cisco Adaptive Security Appliance DNS 消息处理拒绝服务漏洞、Cisco Prime Central for HCS Assurance TBSM 组件拒绝服务漏洞、Cisco AnyConnect VPN 客户端存在多个未明本地权限提升漏洞、Cisco AnyConnect VPN 客户端 ciscod.exe 本地堆溢出漏洞。其中，“Cisco Adaptive Security Appliance 拒绝服务漏洞（CNVD-2013-21971、CNVD-2013-21972、CNVD-2013-21973）、Cisco Adaptive Security Appliance DNS 消息处理拒绝服务漏洞”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/flaw/show/CNVD-2013-21971

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21972

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21973

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21974

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21840

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21975

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21976

5、PHP Address Book SQL 注入漏洞

PHP Address Book 是一款基于 PHP 的 Web 应用程序。本周，该产品被披露存在一个综合评级为“高危”的 SQL 注入漏洞。由于 PHP Address Book 多个脚本未能正确过滤用户提交的输入，远程攻击者利用漏洞可进行 SQL 注入攻击，获得敏感数据库信息或控制应用系统。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-2013-21811

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-2013-21970	BigAnt IM Server 缓冲区溢出漏洞	高	暂无
CNVD-2013-21969	ZAPms 'pid'参数 SQL 注入漏洞	高	暂无
CNVD-2013-21950	Canary Labs Trend Link ActiveX Control 'SaveToFile()'不安全方法漏洞	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.canarylabs.com/software/canary-trend-link
CNVD-2013-21894	Sysax Multi Server SSH 密钥交换拒绝服务漏洞	高	Sysax Multi Server 6.1 已经修复此漏洞，建议用户下载更新：http://www.sysax.com/server/
CNVD-2013-21954	MiniWeb 任意文件上传漏洞	高	暂无
CNVD-2013-21952	EasyPHP 'index.php'远程 php 代码注入漏洞	高	暂无
CNVD-2013-21892	Google Chrome OS 存在未明漏洞	高	Google Chrome OS 26.0.1410.57 已经修复此漏洞，建议用户下载更新：http://googlechromereleases.blogspot.com/
CNVD-2013-21887	RubyGems karteek-docsplit 'text_extractor.rb'远程命令执行漏洞	高	暂无
CNVD-2013-21886	Vanilla Forums SQL 注入漏洞	高	Vanilla Forums 2.0.18.8 已经修复此漏洞，建议用户下载更新：http://vanillaforums.org
CNVD-2013-21880	Nitro PDF 'bcgcbproresen.dll' DLL 加载任意代码执行漏洞	高	Nitro Pro 8.5.2.10 已经修复此漏洞，建议用户下载更新：http://www.nitropdf.com/about

表 3 部分高危漏洞列表

小结：本周，微软发布了 2013 年 4 月份的月度例行安全公告，共含 9 项更新，修复了涉及 Microsoft Windows 操作系统、Internet Explorer 浏览器、Office 套件、Microsoft Server 软件（SharePoint Server、Groove Server、SharePoint Foundation）、Office Web Apps、安全软件（Windows Defender）多款产品中存在的多个安全漏洞，建议企业和个人用户及时更新。Adobe、IBM、Cisco 多款产品也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，发起钓鱼攻击或拒绝服务攻击，导致应用程序崩溃，远程执行任意代码。此外，PHP Address Book 被披露存在零日漏洞，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、D-Link 发布升级程序，修补多个产品安全漏洞

D-Link 多款路由器设备存在漏洞。本周，HP 发布升级程序，修补了 System Management Homepage 存在的漏洞。远程攻击者可利用漏洞获得敏感信息，注入和执行任意 shell 命令。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/patchInfo/show/33192

http://www.cnvd.org.cn/patchInfo/show/33191

本周要闻速递

1. Android 手机曝新漏洞

德国研究人员发现了破解 Android 手机加密信息的新方法：将手机冷冻到零下 15 度，迅速重启，就可读取内存数据，包括短信、相册及电子邮件。研究人员表示，目前还未在其他手机上测试这种方法，不过相信对 iOS 来说，可能会很困难。

参考链接：http://world.kankanews.com/device/2013-04-13/1110499.shtml

2. IOS 安全漏洞在非越狱手机中也存在

此前被认为因相对封闭，而安全系数较高的 IOS 平台中，也开始出现一系列安全问题，其中包括非越狱手机。今年 8 月，法国黑客发现 IOS 短信漏洞，可将诈骗短信伪装成合法身份，诱骗用户接收、点击其中的短信链接等，这一漏洞同样存在于非越狱手机中。随着大量用户购买和同时使用多台 IOS 设备，如 IPHONE、IPAD 等，在信息同步过程中也开始出现一系列安全问题，如一旦黑客成功破译 APPLE ID 账号，可导致用户的 IMESSAGE 信息、安装的应用列表以及 ICLOUD 数据被轻易同步到另外的 IOS 设备上，直接盗取隐私信息。

参考链接：http://www.zj.xinhuanet.com/newscenter/science/2013-04/12/c_115371298.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