国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2012 年 10 月 8 日-2012 年 10 月 14 日 **2012 年第 40 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**高**。

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 249 个，其中高危漏洞 121 个、中危漏洞 114 个、低危漏洞 14 个。上述漏洞中，可利用来实施远程攻击的漏洞有 225 个。本周收录的漏洞中，已有 150 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“GOM Player 空指针引用拒绝服务漏洞”、“Pre Printing Press id 参数 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（含 10.1-10.7 日报送）

本周，共 6 家成员单位和多个合作伙伴报送了本周收录的全部 249 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、天融信等单位报送数量较多。此外，上海交通大学、网御星云公司以及 High-Tech Bridge Security Research 向 CNVD 提交了 15 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
绿盟科技	206	0
启明星辰	304	0
安天实验室	39	0
天融信	29	0
安氏领信	7	0
东软	4	0
上海交通大学	2	2
网御星云	2	2
High-Tech Bridge Security Research	11	11

报送总计	604	15
录入总计	249（去重）	15

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Mozilla、Adobe、Cisco、IBM 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	Mozilla	27	11%
2	Adobe	25	10%
3	Cisco	12	5%
4	IBM	8	3%
5	WordPress	8	3%
6	Microsoft	7	3%
7	Google	6	2%
8	Linux	5	2%
9	Drupal	5	2%
10	SAP	5	2%
11	其它	141	57%

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 249 个漏洞。其中操作系统漏洞 10 个，应用程序漏洞 168 个，WEB 应用漏洞 60 个，网络设备漏洞 6 个，数据库漏洞 2 个，安全产品漏洞 3 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	10
应用程序漏洞	168
WEB 应用漏洞	60
网络设备漏洞	6
安全产品漏洞	3
数据库漏洞	2

表 3 漏洞按影响类型统计表

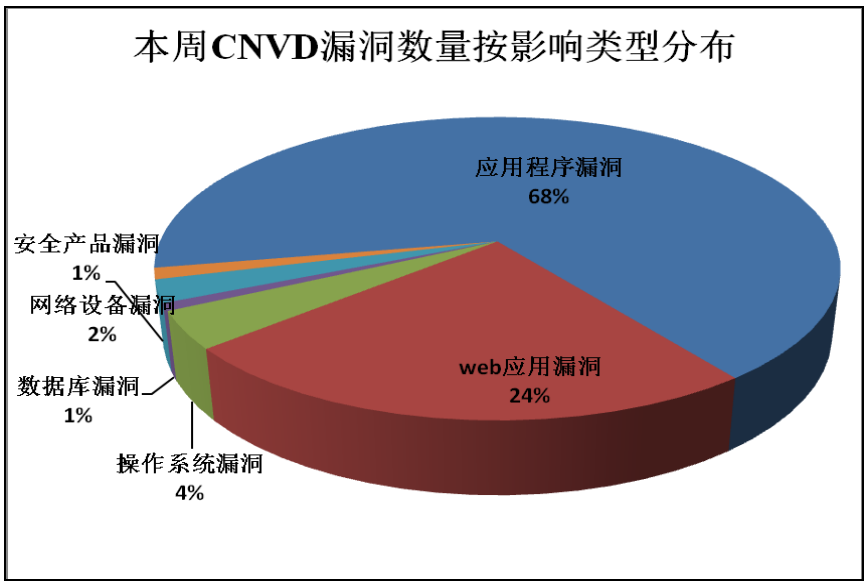

图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 6 个网络设备漏洞：Samsung Galaxy S III 内存破坏漏洞、Samsung Galaxy S III 沙盒绕过漏洞、Global Technology Associates GB-OS 存在多个 HTML 注入漏洞、Cisco ASA 5500 系列和 Cisco Catalyst 6500 系列 SSL VPN 拒绝服务漏洞、Cisco ASA 5500 系列和 Cisco Catalyst 6500 系列拒绝服务漏洞、Cisco ASA 5500/Cisco Catalyst 6500 DHCP 拒绝服务漏洞。其中，除“Global Technology Associates GB-OS 存在多个 HTML 注入漏洞”外，其余漏洞的综合评级均为“高危”。

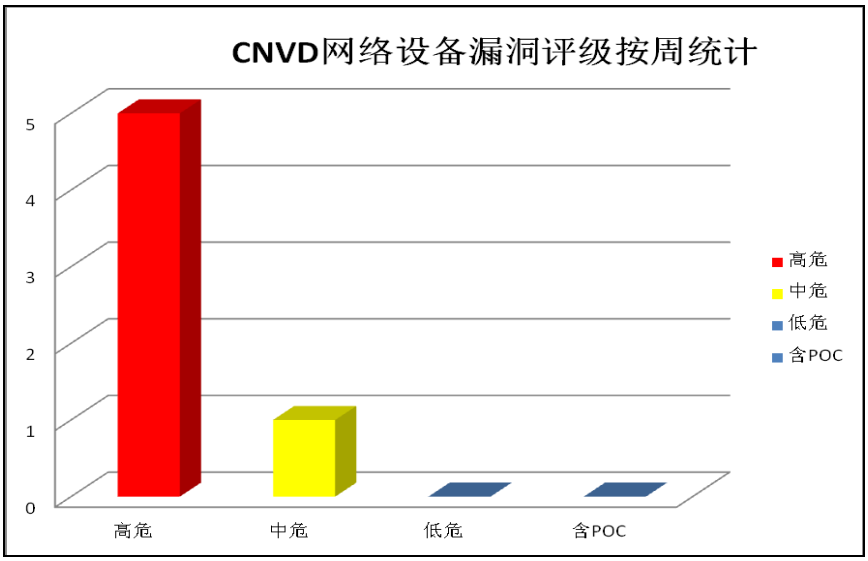

图 2 网络设备漏洞统计

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、Mozilla 产品安全漏洞

Mozilla Firefox/SeaMonkey/Thunderbird 是 Mozilla 所发布的 WEB 浏览器/新闻组客户端/邮件客户端。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可使应用程序崩溃，执行任意代码。

CNVD 收录的相关漏洞包括：Mozilla Firefox/Thunderbird/SeaMonkey instanceof 拒绝服务漏洞、Mozilla Firefox/Thunderbird/SeaMonkey 内存错误引用漏洞（CNVD-2012-15071、CNVD-2012-15076、CNVD-2012-15074、CNVD-2012-15072）、Mozilla Firefox/Thunderbird/SeaMonkey 缓冲区溢出漏洞（CNVD-2012-15080）、Mozilla Firefox/Thunderbird/SeaMonkey 堆缓冲区溢出漏洞（CNVD-2012-15082）、Mozilla Firefox/Thunderbird/SeaMonkey insPos 内存破坏漏洞等。上述漏洞的综合评级均为“高危”。厂商已经修复了上述漏洞，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=58980
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58998
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58985
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58983
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58981
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59001
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59000
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58957

2、 Adobe 产品安全漏洞

Adobe Flash Player 是一款 Flash 文件处理程序。本周，该产品被披露存在多个安全漏洞，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/AIR 内存破坏漏洞（CNVD-2012-14972、CNVD-2012-14943、CNVD-2012-14940）、Adobe Flash Player/AIR 缓冲区溢出漏洞（CNVD-2012-14941、CNVD-2012-14939、CNVD-2012-14928、CNVD-2012-14953、CNVD-2012-14951）等。上述漏洞的综合评级均为“高危”。目前，厂商已经修复了上述漏洞，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=58776
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58717
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58715
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58713

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58714

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58702

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58727

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58725

3、Cisco 产品安全漏洞

Cisco WebEx 是一款思科提供的网络会议解决方案，用于播放与会者在电脑上所记录的 WebEx 会议记录；Cisco Firewall Services Module 是一款防火墙服务模块；Cisco Adaptive Security Appliance 是一款自适应安全设备，可提供安全和 VPN 服务的模块；Cisco Catalyst 是思科公司开发的智能以太网交换机。本周，上述 Cisco 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，执行任意代码。

CNVD 收录的相关漏洞包括：Cisco WebEx Player 缓冲区溢出漏洞（CNVD-2012-15094、CNVD-2012-15097、CNVD-2012-15091、CNVD-2012-15095、CNVD-2012-15090、CNVD-2012-15093）、多个 Cisco 产品远程拒绝服务漏洞（CNVD-2012-15087）、Cisco ASA 5500/Cisco Catalyst 6500 DHCP 拒绝服务漏洞等。上述漏洞的综合评级均为“高危”。厂商已经修复了上述漏洞，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=59023

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59026

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59016

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59020

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59024

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58999

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59019

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59022

4、Google 产品安全漏洞

Google Chrome 是一款开源的 WEB 浏览器。本周，该产品被披露存在多个漏洞，远程攻击者利用漏洞可使应用程序崩溃或执行任意代码。

CNVD 收录的相关漏洞包括：Google Chrome 存在多个漏洞（CNVD-2012-15106）、Google Chrome ICU 处理漏洞、Google Chrome Compositor 越界读漏洞、Google Chrome 音频设备处理漏洞、Google Chrome 插件崩溃未处理漏洞、Google Chrome Skia 拒绝服务漏洞。其中，除“Google Chrome Skia 拒绝服务漏洞”外，其余漏洞的综合评级均为“高危”。厂商已经修复了上述漏洞，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=59036

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58890

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58892

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58889

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58893

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58887

5、GOM Player 空指针引用拒绝服务漏洞

Gom Player 是一款媒体播放软件。本周，Gom Player 被披露存在一个综合评级为“高危”的拒绝服务漏洞。攻击者利用漏洞可构建恶意文件，诱使用户解析，使应用程序崩溃。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=58856

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-2012-15110	WordPress WP Live.php 's'参数跨站脚本漏洞	高	暂无
CNVD-2012-15089	OpenX SQL 注入漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://svn.openx.org/openx/trunk/www/admin/campaign-zone-link.php
CNVD-2012-15050	Snitz Forums 2000 'TOPIC_ID' SQL 注入漏洞	高	暂无
CNVD-2012-15061	Pre Printing Press id 参数 SQL 注入漏洞	高	暂无
CNVD-2012-15021	Siemens SiPass Integrated 'SiPass server'组件缓冲区溢出漏洞	高	用户可联系厂商获得升级版本：http://www.siemens.com/
CNVD-2012-15092	SenseSites CommonSense CMS SQL 注入漏洞	高	暂无
CNVD-2012-15104	VLC Media Player 读访问冲突任意代码执行漏洞	高	暂无
CNVD-2012-14969	Drupal Drag 和 Drop Gallery 任意代码执行漏洞	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://drupal.org/node/1679444
CNVD-2012-15004	Arctic Torrent 远程内存破坏漏洞	高	暂无

CNVD-2012-14932	Linux 内核 udf_load_logicalvol 堆缓冲区溢出漏洞	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://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=adee11b2085bee90bd8f4f52123ffb07882d6256
CNVD-2012-15016	PLIB 'ssgParser.cxx'远程栈缓冲区溢出漏洞	高	暂无

表 3 部分高危漏洞列表

本周，Google Chrome 浏览器被披露存在多个安全漏洞，攻击者利用漏洞可执行任意代码，有可能发起大规模挂马攻击，请广大浏览器用户安装主机防护软件加强防范。Mozilla、Adobe、Cisco 的多款产品也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或执行任意代码。此外，Gom Player 播放器软件被披露存在零日漏洞，建议采用该软件的用户随时关注厂商主页，以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、微软发布 2012 年 10 月公告，修补多个产品安全漏洞

微软发布安全公告，修复 Microsoft Office，Windows，服务器软件，Lync 等多个产品存在的多个安全漏洞，其中 MS12-064 项公告的综合评级为“严重”，其余均为“重要”。攻击者可以利用漏洞远程执行任意代码，提升特权或进行拒绝服务攻击。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=23536

http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=23533

http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=23532

本周要闻速递

1. OS X 存在重大漏洞

据国外媒体报道，Mac OS X 存在一个漏洞，可让黑客 10 秒即可攻破并获取用户的苹果 ID。如果黑客与受影响用户同在一个 Wi-Fi 网络，黑客即可 10 秒获取该用户的苹果 ID。苹果 ID 绑定了用户的 iTunes 和 App Store 的信用卡，因此，泄露了苹果 ID 就等于泄露了信用卡信息。黑客获取苹果 ID 后，可轻易更改密码和邮箱地址。在这里提醒喜欢在公共网络使用 Mac 的用户，最好不要在公用的 Wi-Fi 网络登录自己的苹果账号。黑客解释道，这种攻击方法称之为“Session Fixation Attack”，Session 通常指从注册进

入系统到注销退出系统之间所经过的时间，具体到 Web 中的 Session 指的就是用户在浏览某个网站时，从进入网站到浏览器关闭所经过的这段时间，也就是用户浏览这个网站所花费的时间。可以想象，在用户登录浏览的时间内，黑客只需要瞬间的 10 秒钟就能获取你的苹果 ID，安全系数非常低。发现漏洞的安全人员已经就这个问题联系了苹果，目前苹果还未对此做出回应。

参考链接：http://security.ctocio.com.cn/323/12444823.shtml

2. Firefox 重大安全漏洞已修复

Firefox 16 正式版发布后就曝出了高危安全漏洞，昨日 Mozilla 在官方首页上删去了 Firefox 16 的下载。今天，Mozilla 在官方首页放上了 Firefox 16.0.1 的下载。Firefox 16.0.1 的 Windows、Mac、Linux 版本于当地时间 11 日晚 12 点正式上线，Android 版本也已经升级。Firefox 16 用户可获取自动更新。Firefox 16.0.1 主要修复了 Firefox 16 中的一个安全漏洞，该漏洞可能导致恶意网站获悉用户都访问了哪些网页或是 URL、URL 参数。该漏洞并不影响 Firefox 15 及之前版本。建议 Firefox 16 用户即刻升级至 16.0.1。

参考链接：http://tech.sina.com.cn/s/2012-10-12/09067696183.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