

信息安全漏洞周报

2012 年 2 月 6 日-2012 年 2 月 12 日

2012 年 第 6 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 137 个，其中高危漏洞 60 个、中危漏洞 76 个、低危漏洞 1 个。上述漏洞中，可利用来实施远程攻击的漏洞有 133 个。本周收录的漏洞中，已有 96 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“TORCS '.xml' 文件缓冲区溢出漏洞”、“OfficeSIP Server 远程拒绝服务漏洞”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 1 家合作伙伴单位报送了本周收录的全部 137 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、安天实验室报送数量较多。

报送单位或个人	漏洞报送数量	原创漏洞数量
启明星辰	89	0
绿盟科技	72	0
安天实验室	30	0
安氏领信	4	0
天融信	2	2
总计	137（去重）	2

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Google、Apple、Siemens 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	Google	20	14.6%

2	Apple	14	10.2%
3	Siemens	10	7.3%
4	Real Networks	7	5.1%
5	Open Handset Alliance	7	5.1%
6	PHP	5	3.6%
7	Red Hat	3	2.2%
8	Computer Associates	3	2.2%
9	Novell	3	2.2%
10	zenphoto	3	2.2%
11	其它	62	45.3%

表 2 漏洞产品涉及厂商分布统计表

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、Google Chrome 安全漏洞

Google Chrome 是一款开源的 WEB 浏览器。本周，Google Chrome 被披露存在多个安全漏洞，远程攻击者可以利用漏洞绕过部分安全限制，操作数据或执行任意代码。CNVD 收录的相关漏洞包括：Google Chrome SVG 布局内存错误引用漏洞、Google Chrome CSS 处理存在未明漏洞、Google Chrome 表单错误处理内存错误引用漏洞、Google Chrome 实用程序存在未明漏洞、Google Chrome 语言环境处理缓冲区溢出漏洞、Google Chrome IndexedDB 事务存在未明漏洞、Google Chrome 剪贴板监控存在未明漏洞、Google Chrome 音频解码存在漏洞。其中，除“Google Chrome 音频解码存在漏洞”外，其余漏洞的综合评级均为“高危”。目前，Google 已经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/sites/main/preview/ldgg_preview.htm?tid=38908
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38901
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38897
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38841
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38837
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38831
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38829
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38839

2、Apple Mac OS X 安全漏洞

Apple Mac OS X 是苹果公司发布的一款操作系统。本周，Apple Mac OS X 存在多个安全漏洞，远程攻击者可以利用漏洞使应用程序崩溃、执行任意代码或窃取敏感信息。CNVD 收录的相关漏洞包括：Apple Mac OS X 远程代码执行漏洞（CNVD-2012-09731、CNVD-2012-09729）、Apple Mac OS X 地址簿组件信息泄露漏洞、Apple Mac OS X CFNetwork 组件信息泄露漏洞、Apple Mac OS X 存在多个内存破坏漏洞（CNVD-2012-09734）、Apple Mac OS X 整数溢出漏洞（CNVD-2012-09732）、Apple Mac OS X CoreUI 远程代码执行漏洞（CNVD-2012-09726）、Apple Mac OS X CoreText 释放后重用代码执行漏洞。其中，“Apple Mac OS X 存在多个内存破坏漏洞（CNVD-2012-09734）”、“Apple Mac OS X 整数溢出漏洞（CNVD-2012-09732）”的漏洞综合评级为“高危”。目前，Apple 已经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/sites/main/preview/ldgg_preview.htm?tid=38341
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38340
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38339
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38338
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38350
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38348
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38336
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38708

3、Siemens SIMATIC 安全漏洞

Siemens SIMATIC 是一款工业控制自动化管理软件。本周，上述 Siemens 产品被披露存在多个安全漏洞。攻击者可以利用漏洞获得敏感信息，提升特权，执行任意代码或进行拒绝服务攻击。CNVD 收录的相关漏洞包括：Siemens SIMATIC WinCC HMI Telnet 存在漏洞（CNVD-2012-09748、CNVD-2012-09747）、Siemens SIMATIC WinCC HMI 目录遍历漏洞（CNVD-2012-09752、CNVD-2012-09750）、Siemens SIMATIC WinCC HMI 跨站脚本漏洞（CNVD-2012-09745）、Siemens SIMATIC WinCC HMI 字符串栈溢出漏洞（CNVD-2012-09749）、Siemens SIMATIC WinCC HMI 拒绝服务攻击漏洞（CNVD-2012-09751）、Siemens SIMATIC WinCC HMI 存在漏洞（CNVD-2012-09753）。上述漏洞的综合评级均为“高危”。目前，Siemens 已经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/sites/main/preview/ldgg_preview.htm?tid=38375
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38428
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38372
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38374
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38388

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38408
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38409
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38448

4、Real Networks RealPlayer 产品安全漏洞

RealNetworks RealPlayer 是一款媒体播放程序。本周，RealNetworks RealPlayer 存在多个安全漏洞，远程攻击者可以利用漏洞构建恶意媒体文件，诱使用户解析，以应用程序上下文执行任意代码。CNVD 收录的相关漏洞包括：Real Networks RealPlayer 'rvrender' RMFF 标记远程代码执行漏洞、Real Networks RealPlayer RV20 帧大小远程代码执行漏洞、Real Networks RealPlayer 'VIDOBJ_START_CODE'远程代码执行漏洞、Real Networks RealPlayer 'coded_frame_size'远程代码执行漏洞、Real Networks RealPlayer Atrac 样本解码远程代码执行漏洞、Real Networks RealPlayer 远程代码执行漏洞（CNVD-2012-09776、CNVD-2012-09777）。上述漏洞的综合评级均为“高危”。目前，厂商已经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/sites/main/preview/ldgg_preview.htm?tid=38781
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38780
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38776
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38770
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38768
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38772
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=38773

5、TORCS '.xml'文件缓冲区溢出漏洞

TORCS 是一款开源的赛车模拟器，同时也作为人工智能研究平台。本周，TORCS 被披露存在一个缓冲区溢出漏洞。由于应用程序未能正确处理.xml文件，攻击者可以构建恶意文件，诱使用户打开，可以利用漏洞以应用程序上下文执行任意代码。该漏洞的综合评级为“高危”。目前，互联网上已经出现针对该漏洞的攻击代码，主要影响 TORCS 1.3.2 版本。厂商尚未发布上述漏洞的修补程序，CNVD 提醒相关研发或个人用户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=38814

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-2012-09835	Novell iPrint Client 远程代码执行漏洞（CNVD-2012-09835）	高	Novell iPrint Client 5.78 已经修复此漏洞，建议用户下载使用： http://www.novell.com/

CNVD-2012-09836	PhotoLine JPEG2000 远程堆缓冲区溢出漏洞	高	PhotoLine 17.02 已经修复此漏洞，建议用户下载使用： http://pl32.com/index.php
CNVD-2012-09833	MySQL 存在未明远程代码执行漏洞	高	暂无
CNVD-2012-09851	Sysax Multi Server 'uploadfile_name1.htm'缓冲区溢出漏洞	高	暂无
CNVD-2012-09843	OpenConf 存在未明漏洞（CNVD-2012-09843）	高	OpenConf 4.12 已经修复此漏洞，建议用户下载使用： http://www.zakongroup.com/technology/openconf.shtml
CNVD-2012-09828	CVS 'proxy_connect()'堆缓冲区溢出漏洞（CNVD-2012-09828）	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://bugzilla.redhat.com/show_bug.cgi?id=784141
CNVD-2012-09824	Advantech BroadWin WebAccess 远程代码执行漏洞	高	暂无
CNVD-2012-09844	PeerBlock 'pbfilter.sys'缓冲区溢出漏洞	高	暂无
CNVD-2012-09803	Zenphoto SQL 注入漏洞	高	zenphoto 1.4.2.1 已经修复此漏洞，建议用户下载使用： http://www.zenphoto.org/news/zenphoto-1.4.2.1
CNVD-2012-09811	Computer Associates Total Defense SQL 注入漏洞（CNVD-2012-09811）	高	Computer Associates Total Defense 12 SE3 已经修复此漏洞，建议用户下载使用： http://home3.ca.com/partnerportal/business/BusinessProducts/totaldefense.aspx

表 3 部分高危漏洞列表

小结：本周，Google 发布安全更新，修复了 Chrome 浏览器存在的多个安全漏洞，防范由此引发的挂马攻击或针对主机的远程攻击威胁。Apple 操作系统、Siemens 和 Real Networks 的应用产品被披露存在多个安全漏洞，影响涉及终端用户以及工业行业用户。此外，BroadWin 工业控制软件、MySQL 数据库、CA Total Defense 安全产品的高危漏洞也值得相关用户注意，加强防范。

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、IBM 发布升级程序，修补多款产品安全漏洞

本周，IBM 发布升级程序，修补了 Cognos TM1 Executive Viewer 和 AIX 存在的安全漏洞，避免远程攻击者可以利用漏洞进行跨站脚本和拒绝服务攻击。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=9191
http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=8852

本周要闻速递

1. Mozilla 紧急发布补丁修复火狐漏洞

据国外媒体报道，Mozilla 发布了一个紧急补丁，修复火狐浏览器中的一个严重的安全漏洞。Mozilla 把这个安全漏洞的等级列为“严重”。攻击者利用这个安全漏洞可以执行其代码和安装软件，除了用户正常浏览之外不需要用户任何互动。Mozilla 发布的最新版本火狐 10.0.1 版修复的这个安全漏洞能够引起浏览器崩溃。恶意黑客可以利用这个漏洞实施执行代码攻击。Mozilla 的安全公告称，Mozilla 开发者发现“ReadPrototype Bindings”函数将在哈希表中留下一个 XBL 绑定，即使在这个功能失效的时候也是如此。如果发生这种情况，当这个循环收集器读到这个哈希表并且要对这个绑定采取虚拟方法时，浏览器将崩溃。黑客可以利用这个浏览器崩溃实施攻击。Mozilla 把这个安全漏洞列为“严重”等级，因为这个安全漏洞能够用于运行攻击者的代码和安装软件，不需要用户干预。Mozilla 称，火狐 9 和早期版本的火狐浏览器不受这个安全漏洞的影响。

参考链接：http://news.ccidnet.com/art/1032/20120213/3581197_1.html

2. 谷歌钱包存在安全漏洞 用户识别码可被破解

谷歌钱包的漏洞被曝光后，谷歌上周六已经暂停了该服务与预付费卡的关联功能。利用这一漏洞，未授权用户也可以窃取用户账号资金。这一安全漏洞是上周四被揭露的。打开 Android 手机的设置界面，清空所有有关谷歌钱包的设置，未经授权的用户就可以访问此前与该服务关联的预付费卡账号。此前一天，安全公司刚刚发布了一种破解谷歌钱包 PIN 码的方法。该公司发现，谷歌钱包的 PIN 码并未存储在硬件“安全单元”中，而是存放于一个被 Android 系统保护的数据库中。通过对该数据库的强力攻击，黑客就可以获取 PIN 码。但这种攻击仅适用于获得了 Root 权限的账号。手机厂商都不鼓励用户获取 Root 权限，因为这样不仅会影响设备保修，而且可能会产生安全漏洞。如果用户设置了锁屏密码，便可不受这两项漏洞的影响。该功能会在手机被激活时要求用户输入 PIN 码，而如果未授权用户不知道 PIN 码，便无法发动攻击。但很多用户因为怕麻烦并未设置这一功能。值得注意的是，未经授权的用户都必须亲手接触到手机才能利用上述漏洞，而无法通过恶意软件远程操作。另外，这些漏洞都源于谷歌钱包，而非该服务

所使用的 NFC(近场通讯)技术。

参考链接: <http://tech.sina.com.cn/i/2012-02-13/08256714969.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