

信息安全漏洞周报

2011 年 8 月 1 日-2011 年 8 月 7 日

2011年第31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 120 个，其中高危漏洞 59 个、中危漏洞 55 个、低危漏洞 6 个。上述漏洞中，可利用来实施远程攻击的漏洞有 115 个。网上已经出现针对“Microsoft Windows CSRSS 'SrvGetConsoleTitle()'本地类型转换漏洞”、“WordPress Timthumb 插件'timthumb'目录任意文件上传漏洞”等的零日攻击代码，请使用相关产品的用户注意做好防护措施。本周收录的漏洞中，已有 73 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。

成员单位报送漏洞统计

本周，共 6 家成员单位报送了本周收录的全部 120 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、恒安嘉新报送的数量较多。此外，知道创宇报送了 1 个网站安全漏洞：腾讯 qq 空间跨站跳转漏洞。上述漏洞事件转由国家互联网应急中心（CNCERT）纳入安全事件处置流程，未分配 CNVD 漏洞编号。

报送单位或个人	漏洞报送数量	私有漏洞数量
启明星辰	99	0
绿盟科技	92	0
恒安嘉新	29	0
安氏领信	1	0
东软	11	0
知道创宇	1	0
总计	120（去重）	0

表 1 成员单位上报漏洞统计表

本周，CNVD 整理和发布的漏洞涉及 Google、Apple、IBM、Cisco、Microsoft 等多家厂商的产品，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	31	25.8%
2	Apple	8	6.7%
3	Libmodplug	5	4.2%
4	MiniUPnP Project	5	4.2%
5	ThreeDify	5	4.2%
6	IBM	4	3.3%
7	Joomla!	2	1.7%
8	WordPress	2	1.7%
9	Cisco	1	0.8%
10	Microsoft	1	0.8%
11	其它	56	46.6%

表 2 漏洞产品涉及厂商分类统计

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、Google Chrome 安全漏洞

Google Chrome 是一款 WEB 浏览器。本周，Google 发布安全更新，修复 Chrome 存在的多个安全漏洞。攻击者可以利用漏洞绕过安全限制，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：Google Chrome 旧指针引用漏洞(CVE-2011-2359)、Google Chrome 内存错误引用漏洞(CVE-2011-2792、CVE-2011-2790、CVE-2011-2801、CVE-2011-2818、CVE-2011-2793)、Google Chrome ICU 越界写漏洞(CVE-2011-2791)、Google Chrome URI 处理漏洞(CVE-2011-2819)等。上述漏洞的综合评级均为“高危”。CNVD 提醒广大 Google 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/vulnerability/CNVD-2011-06609>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06608>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06606>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06605>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06604>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06629>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06628>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06627>

2、Apple QuickTime 安全漏洞

Apple QuickTime 是一款多媒体播放器。本周，Apple QuickTime 被披露存在多个安全漏洞。攻击者可以利用漏洞构建恶意文件，诱使用户解析，导致应用程序崩溃或任意代码执行。CNVD 收录的漏洞包括：Apple QuickTime PICT 文件缓冲区溢出漏洞（CVE-2011-0245）、Apple QuickTime 'STSC atoms'堆缓冲区溢出漏洞（CVE-2011-0252、CVE-2011-0251、CVE-2011-0250、CVE-2011-0249）、Apple QuickTime ActiveX 控件栈缓冲区溢出漏洞（CVE-2011-0248）、Apple QuickTime 栈缓冲区溢出漏洞（CVE-2011-0247）、Apple QuickTime 堆缓冲区溢出漏洞（CVE-2011-0246）。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补丁程序，CNVD 提醒广大 Apple 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/vulnerability/CNVD-2011-06662>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06660>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06659>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06658>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06656>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06654>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06652>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06650>

3、WordPress 产品安全漏洞

WP e-Commerce 和 Timthumb 是 WordPress 的插件。本周，上述 WordPress 插件被披露存在安全漏洞。远程攻击者可以利用漏洞执行任意代码或窃取敏感信息。CNVD 收录的漏洞包括：WordPress WP e-Commerce Plug-in 'cart_messages[]'参数跨站脚本漏洞和 WordPress Timthumb 插件'timthumb'目录任意文件上传漏洞。上述漏洞的综合评级均为“高危”。目前，互联网上已经出现针对“WordPress WP e-Commerce Plug-in 'cart_messages[]'参数跨站脚本漏洞”的攻击代码，主要影响 WordPress WP e-Commerce 3.8.6 版本。厂商尚未修补该漏洞，只发布了“WordPress Timthumb 插件'timthumb'目录任意文件上传漏洞”的补丁程序，CNVD 提醒广大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/vulnerability/CNVD-2011-06668>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06580>

4、Joomla!产品安全漏洞

本周，Joomla!的 com_jdirectory 组件和 obSuggest 组件存在安全漏洞。远程攻击者可以利用漏洞控制应用程序，访问或修改数据以及执行任意脚本。CNVD 收录的漏洞包括：Joomla! com_jdirectory 组件'Itemid'参数 SQL 注入漏洞、Joomla! obSuggest 组件'controller'参数本地文件包含漏洞。目前，互联网上已经出现针对上述漏洞的攻击代码，且厂商尚

未发布这些漏洞的补丁程序，CNVD 提醒广大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/vulnerability/CNVD-2011-06667>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06578>

5、Microsoft Windows CSRSS 'SrvGetConsoleTitle()'本地类型转换漏洞

Microsoft Windows 是一款操作系统。Microsoft Windows CSRSS 存在安全漏洞。问题存在于执行某些大小检查时客户端/服务器运行子系统(CSRSS)中的"SrvGetConsoleTitle()"函数(winsrv.dll)存在一个类型转换错误，攻击者可以利用此漏洞获取某些 CSRSS 内存或引用非法内存导致内核崩溃。目前，厂商尚未发布该漏洞的修补程序，CNVD 提醒广大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/vulnerability/CNVD-2011-06649>

小结：本周，Google 发布安全更新，修补 Chrome 存在的多个安全漏洞。攻击者可以利用漏洞绕过安全限制，执行任意代码或进行拒绝服务攻击，对使用 Google 产品的用户构成较为严重的威胁。同时，Apple QuickTime、WordPress 和 Joomla!组件也被披露存在多个安全漏洞。此外，Microsoft Windows 零日漏洞也对使用该产品的用户构成较大威胁。请使用上述软件的相关机构和个人及时采取安全防范措施。

本周重要漏洞修补信息

本周，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 Lotus Symphony 安全漏洞

IBM Lotus Symphony 是 IBM 推出的一款办公软件。本周，IBM 发布升级程序，修补了 Lotus Symphon 存在的多个安全漏洞。攻击者可以利用漏洞引起应用程序崩溃或产生其他未明影响。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/patch/4591>

<http://www.cnvd.org.cn/patch/4590>

<http://www.cnvd.org.cn/patch/4589>

<http://www.cnvd.org.cn/patch/4588>

本周要闻速递

1. 快播发表有关 QvodInsert.dll 组件漏洞的声明

北京时间 8 月 5 日消息，针对近日有媒体报道称，有杀毒软件发现快播播放器的 QvodInsert.dll 组件存在安全漏洞。攻击者利用该漏洞可以攻击网页，安装快播的网民访问

这些网页时可能中毒。快播发表声明，称此安全漏洞仅存在于快播播放器较早的版本的，而且技术人员早已及时发现并进行了技术升级和优化，目前市面上的版本并不存在这一漏洞问题。

参考链接: <http://tech.cn.yahoo.com/ypen/20110805/511573.html>

2. 微软下周二将发布 2011 年 8 月安全更新

8 月 5 日消息，据国外媒体报道，微软周四称，在下周的补丁星期二将发布 13 个安全补丁，修复 IE、Windows、Visio 和 Visual Studio 等软件中的 22 个安全漏洞。在这 13 个安全补丁中，有 2 个“严重”等级的安全补丁，9 个是“重要”等级的安全补丁。剩下的 2 个是“中等”等级的安全补丁。

参考链接: http://news.ccidnet.com/art/11099/20110805/2463959_1.html

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