

信息安全漏洞周报

2011 年 6 月 13 日-2011 年 6 月 19 日

2011年第24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 108 个，其中高危漏洞 73 个、中危漏洞 31 个、低危漏洞 4 个。上述漏洞中，可利用来实施远程攻击的漏洞有 101 个。网上已经出现针对“Gogago YouTube Video Converter ActiveX 控件'Download()'方法缓冲区溢出漏洞”、“Opera Web Browser 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做好防护措施。本周收录的漏洞中，已有 88 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，共有 5 家成员单位报送了本周收录的全部 108 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。另外，知道创宇公司报送了广东移动网站列目录漏洞，该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	102	0
绿盟科技	49	0
恒安嘉新	28	0
东软	4	0
知道创宇	1	1
总计	108（去重）	1

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 Microsoft、Adobe、Sun、Siemens、Google 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	Microsoft	31	28.7%
2	Adobe	29	26.9%
3	RedHat	10	9.3%
4	Sun	9	8.3%
5	OProfile	3	2.8%
6	IBM	2	1.9%
7	Siemens	2	1.9%
8	ClearSCADA	2	1.9%
9	Joomla!	1	0.9%
10	Google	1	0.9%
11	其他	18	16.4%

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、Siemens SIMATIC S7-1200 安全漏洞

Siemens SIMATIC S7-1200 是西门子推出的一款模块化控制器。本周，CNVD 收录了该产品被披露两个漏洞。“Siemens SIMATIC S7-1200 控制器指令重放漏洞”是由于控制器引擎软件向可编程逻辑控制器发送未加密数据，通过发起中间人攻击重放引擎软件发送的指令；而“Siemens SIMATIC S7-1200 控制器拒绝服务漏洞”则是由于 WEB 服务器存在一个未明错误，可触发拒绝服务攻击。上述漏洞的综合评级均为“高危”。目前，厂商已经发布安全补丁，CNVD 提醒相关用户及时获取补丁程序进行修补。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05921>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05920>

2、TurboCMS 产品安全漏洞

TurboCMS 是一款企业级内容管理软件平台与整体解决方案。6 月 4 日，CNVD 接到中国电力科学研究院信息安全实验室报送的 TurboCMS 内容管理系统存在的 4 个安全漏洞。CNVD 对该漏洞进行了验证和测试，确定了漏洞的危害程度，并于本周正式发布。攻击者可以利用漏洞进行跨站脚本、SQL 注入攻击，或上传脚本木马获取服务器控制权。CNVD 收录的漏洞包括：TurboCMS Java 内容管理系统跨站脚本漏洞、TurboCMS Java 内容管理系统注入漏洞、TurboCMS Java 内容管理系统上传漏洞、TurboCMS Java

内容管理系统特权提升漏洞。除“TurboCMS Java 内容管理系统跨站脚本漏洞”综合评级为“中危”外，其余漏洞的综合评级均为“高危”。根据协调的情况，厂商将于六月底至七月中旬陆续开发完成这些漏洞的补丁程序，建议相关用户根据暂时通过限制通过互联网访问后台的方式进行安全控制，避免诱发攻击事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05702>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05701>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05700>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05699>

3、Microsoft 产品安全漏洞

6月14日，微软发布了2011年6月份的月度例行安全公告，共包含16项安全更新。其中，9项更新的综合评级为“严重”，另外7项更新的综合评级为“重要”。本次发布的安全更新修复了Windows、.NET Framework、Silverlight、Forefront Threat Management Gateway、Internet Explorer、Office、SQL Server 和 Visual Studio 多个产品中存在的34个安全漏洞，包括近日被披露的影响IE所有版本的IE cookie 劫持漏洞。攻击者可以利用这些漏洞远程执行任意代码、窃取敏感信息、提升特权或进行拒绝服务攻击。CNVD收录的相关漏洞包括：Microsoft .NET Framework JIT 对象校验漏洞、Microsoft Internet Explorer Time 元素未初始化内存远程代码执行漏洞、Microsoft Windows 'win32k.sys' OpenType 字体解析远程代码执行漏洞、Microsoft Windows SMB Server 远程拒绝服务漏洞、Microsoft Silverlight 非法数组偏移远程代码执行漏洞(CVE-2011-0664)、Microsoft Forefront Threat Management Gateway (TMG)防火墙客户端内存破坏漏洞等。上述漏洞的综合评级均为“高危”。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/vulnerability/CNVD-2011-05906>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05874>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05872>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05870>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05862>

4、Adobe 产品安全漏洞

本周，Adobe在官网发布安全公告，修复了Adobe Shockwave Player、LifeCycle Data Services、BlazeDS、Flash Player、ColdFusion等多个产品存在的安全漏洞。攻击者可以利用漏洞远程执行任意代码、进行拒绝服务攻击或以管理员权限执行恶意操作。CNVD收录的相关漏洞包括：Adobe Shockwave Player 内存破坏漏洞（CVE-2011-2128）、Adobe LiveCycle Data Services 和 BlazeDS 存在多个安全漏洞、Adobe Flash Player 远程内存破坏漏洞（CVE-2011-2110）、Adobe ColdFusion 远程拒绝服务漏洞（CVE-2011-2091）、Adobe Shockwave Player 缓冲区溢出漏洞（CVE-2011-2126）等。CNVD提醒广

大 Adobe 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-2011-05931>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05905>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05904>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05903>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05901>

5、Gogago YouTube Video Converter ActiveX 控件缓冲区溢出漏洞

Gogago YouTube Video Converter 是一款视频转换工具。本周，Gogago YouTube Video Converter 存在一个缓冲区溢出漏洞。该漏洞是由于用户提供给"bsURL"参数的数据在拷贝到 MDIEX.dll 文件中"Download()"方法缓冲区时缺少充分的边界检查，攻击者可以构建嵌入恶意代码的网站页面，诱使用户访问，进而以应用程序上下文执行任意代码。目前，互联网上已经出现针对该漏洞的攻击代码，主要影响 Gogago YouTube Video Converter 1.1.6 版本。厂商尚未发布该漏洞的补丁程序，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-2011-05929>

小结: 本周，CNVD 收录了 Siemens SIMATIC S7-1200 控制器存在的两个安全漏洞，攻击者可以利用漏洞重放控制指令或进行拒绝服务攻击，对使用 Siemens 该产品的用户构成较为严重的威胁。根据互联网上公开的信息，漏洞报告者对西门子公司发布的官方补丁有效性存疑。CNVD 还发布了本月初收录的中国电力科学研究院信息安全实验室报送的 TurboCMS 内容管理系统存在的 4 个安全漏洞。Microsoft 和 Adobe 均发布安全公告，修复多个产品安全漏洞。此外，Gogago YouTube Video Converter 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、Oracle 发布升级程序，修补多个产品安全漏洞

本周，Oracle 发布升级程序，修补 JRE、JDK 等多个产品的安全漏洞。远程攻击者可以利用漏洞执行任意代码。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/4089>
<http://www.cnvd.org.cn/patch/4098>
<http://www.cnvd.org.cn/patch/4097>
<http://www.cnvd.org.cn/patch/4096>



本周要闻速递

1. 微软发布 2011 年 6 月安全补丁公告

北京时间 6 月 15 日凌晨,微软向全球用户发布了 16 个安全补丁,用于修复 Windows、IE、Office、SQL Server 和其它产品中的多个安全漏洞,补丁规模之大仅次于 4 月安全更新。其中,今年刚刚亮相的 IE 9 浏览器也将首次接受漏洞修复。微软 6 月安全公告显示,本次 16 个补丁中有 9 个被定为“高危”级别,其他补丁则被定为“重要”。值得关注的是,IE 浏览器本月需要修复 2 个“高危”漏洞补丁,涉及今年 3 月中旬发布的 IE9,这也将成为 IE 9 自问世以来的首个补丁。安全专家认为:“网络安全是一个长期的攻防过程。尽管 IE9 在隐私保护方面非常出色,但如果用户不慎打开恶意网站,黑客仍有可能利用漏洞窃取 IE9 浏览器的 cookie,从而获取受害者的帐号登录信息,如邮箱、微博等。因此,电脑及时打补丁修复漏洞才能提升安全防护能力。据悉,本月微软安全更新除了 2 个影响 IE 的补丁外,还有 10 个 Windows 补丁、2 个 Office 补丁、1 个 Forefront 安全客户端补丁,以及 1 个 .Net 和 Silverlight 补丁,影响所有版本的 Windows 操作系统和相关软件,包括最新的 Windows 7 系统。

参考链接: <http://finance.sina.com.cn/20110615/10439994203.shtml>

2. Adobe Flash Player 又曝高危漏洞 用户需立即升级

Flash Player 近日频频曝出安全漏洞,本周,Adobe 再次对 Flash 版本进行了升级,主要修复了一个高危漏洞,这个内存损坏(memory corruption)漏洞会导致受感染系统被攻击者控制。幸运的是,这个问题不影响 Adobe Reader 和 Acrobat X 产品。受此漏洞影响的 Flash 包括:(1) Windows、Mac、Linux 和 Solaris 系统上的 Flash Player 10.3.181.23 及之前版本;(2) Android 系统上的 Flash Player 10.3.185.23 及之前版本。Adobe 建议 Windows、Mac、Linux 和 Solaris 用户升级至最新的 10.3.181.26。

参考链接: <http://news.newhua.com/news/2011/0615/124869.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