

信息安全漏洞周报

2011 年 6 月 20 日-2011 年 6 月 26 日

2011年第25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 110 个，其中高危漏洞 73 个、中危漏洞 31 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 98 个。网上已经出现针对“Microsoft Word 文件指针远程代码执行漏洞”、“Mozilla Firefox Firebug 扩展'chrome:'跨域脚本漏洞”、“FreeAmp '.fat'文件远程缓冲区溢出漏洞”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 85 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 110 个漏洞，各单位报送情况如表 1 所示。其中，启明星辰、绿盟科技报送的数量较多。

报送单位或个人	漏洞报送数量	私有漏洞数量
启明星辰	98	0
绿盟科技	90	0
恒安嘉新	11	0
东软	3	0
安天	1	0
总计	110（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 Microsoft、Adobe、Apple、Mozilla、Linux 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	Apple	19	17.3%
2	Mozilla	16	14.5%
3	Adobe	13	11.8%
4	Microsoft	9	8.2%
5	Easewe	4	3.6%
6	Cachelogic	3	2.7%
7	Linux	3	2.7%
8	IBM	2	1.8%
9	WordPress	2	1.8%
10	Apache	1	0.9%
11	其他	38	34.7%

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、Apple Mac OS X 安全漏洞

Apple Mac OS X 是一款苹果发布的操作系统。本周，Apple 官网发布安全公告，修复了 Mac OS X 10.6.8 之前版本存在的多个安全漏洞。远程攻击者可以利用漏洞获得敏感信息，劫持用户会话，执行任意代码或使应用程序崩溃。CNVD 收录的相关漏洞包括：Apple Mac OS X (Server) 10.6.8 之前版本空指针引用漏洞（CVE-2011-1132）、Apple Mac OS X (Server) 10.6.8 之前版本'QuickTime'缓冲区溢出漏洞（CVE-2011-0213、CVE-2011-0212）、Apple Mac OS X (Server) 10.6.8 之前版本'QuickLook'内存破坏漏洞（CVE-2011-0208）、Apple Mac OS X (Server) 10.6.8 之前版本'ICU'存在缓冲区溢出漏洞（CVE-2011-0206）等。上述漏洞的综合评级均为“高危”。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-2011-06041>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06040>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06039>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06035>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06033>

2、Mozilla 产品安全漏洞

本周，Mozilla 在官网发布安全公告，修复了 Firefox、Thunderbird、SeaMonkey 多个产品的安全漏洞。攻击者可以利用漏洞远程执行任意代码、窃取敏感信息或使目标浏览器崩溃。CNVD 收录的相关漏洞包括：Mozilla Firefox/Thunderbird/SeaMonkey SVG Polygon 解析远程代码执行漏洞、Mozilla Firefox/Thunderbird/SeaMonkey XUL 文档处理远程代码执行漏洞、Mozilla Firefox WebGL 越界读信息泄露漏洞、Mozilla Firefox 'nsTreeRange'悬摆指针远程代码执行漏洞、Mozilla Firefox Firebug 扩展'chrome:'跨域脚本漏洞。除“Mozilla Firefox Firebug 扩展'chrome:'跨域脚本漏洞”综合评级为“中危”外，其余漏洞的综合评级均为“高危”。目前，互联网上已经出现了“Mozilla Firefox 'nsTreeRange'悬摆指针远程代码执行漏洞和 Mozilla Firefox Firebug 扩展'chrome:'跨域脚本漏洞”的攻击代码，主要影响 Firefox 插件 Firebug 1.7.2 版本和 Mozilla Firefox 3.6.16 及之前版本。除上述两个漏洞外，其余漏洞均已修补，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-2011-05985>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05983>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05980>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05975>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05963>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05954>

3、Microsoft 产品安全漏洞

本周，CNVD 收录了 Microsoft 产品 Excel 存在的多个安全漏洞和 Word 存在的一个零日漏洞。Microsoft word 零日漏洞是由于文档中的某些值被用来作为一个指针使用，构建特制的文档可造成内存泄露，成功利用漏洞可以以应用程序上下文执行任意代码。目前互联网上已经出现了针对该漏洞的攻击代码，主要影响 Word 2002 版本。Excel 存在的多个安全漏洞可被远程攻击者利用特制的电子表格执行任意代码或者引起拒绝服务（内存破坏）。相关漏洞包括：Microsoft Word 文件指针远程代码执行漏洞、Excel 越界 WriteAV 漏洞、Excel 内存破坏漏洞、Excel 缓冲区溢出漏洞、Excel 内存堆重写漏洞等。除 Word 零日漏洞外，Microsoft 已修补其余漏洞，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-2011-05938>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05951>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05948>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05947>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05945>

4、Adobe 产品安全漏洞

Adobe Reader/Acrobat 是一款处理 PDF 文件的应用程序。本周，Adobe 在官网发布

安全公告，修复了 Adobe Reader/Acrobat 存在的多个安全漏洞。攻击者可以利用漏洞获得敏感信息，绕过安全限制或执行任意代码。CNVD 收录的相关漏洞包括：Adobe Reader / Acrobat 存在漏洞(CVE-2011-2106、CVE-2011-2105、CVE-2011-2104、CVE-2011-2103)等。除“Adobe Reader / Acrobat 存在漏洞(CVE-2011-2104)”外，其余漏洞的综合评级均为“高危”。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-2011-05960>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05959>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05958>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05957>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05956>

5、FreeAmp '.fat'文件远程缓冲区溢出漏洞

FreeAmp 是一款 MP3 播放程序。FreeAmp 处理'.fat'文件时存在缓冲区溢出漏洞，攻击者可以构建恶意文件，诱使用户解析，以应用程序上下文执行任意代码。目前，互联网上已经出现了针对该漏洞的攻击代码，主要影响 Freeamp 2.0.7 版本。厂商尚未发布该漏洞的修补程序，CNVD 提醒相关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-2011-06017>

小结：本周，Apple、Mozilla、Adobe 多个厂商发布安全公告，修复 Apple Mac OS X、Mozilla Firefox/Thunderbird/SeaMonkey 和 Adobe Reader/Acrobat 多个产品的安全漏洞，对使用上述产品的用户构成较为严重的威胁。Microsoft Word 被披露存在一个远程代码执行零日漏洞，攻击者可以利用漏洞以应用程序上下文执行任意代码。此外，FreeAmp 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、SAP 发布升级程序，修补 NetWeaver 安全漏洞

本周，SAP 发布升级程序，修补 NetWeaver 产品的多个安全漏洞。远程攻击者可以利用漏洞发起跨站脚本和拒绝服务等攻击，造成敏感信息泄露或应用程序崩溃。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/4227>
<http://www.cnvd.org.cn/patch/4228>
<http://www.cnvd.org.cn/patch/4225>



本周要闻速递

1. Chrome 官方扩展可自动识别漏洞

Google 发布了一个名为 DOM Snitch 的 Chrome 官方扩展，它可以让开发者和安全人士在浏览网站时自动识别出不安全的代码，这种扩展的灵感其实是来自于 5 周之前一家安全公司在 Firefox 上的作品 DOMinator，使用这种工具用户可以轻易发现例如 XSS、数据泄漏等问题，并指出问题所在的代码段，帮助用户规避以及厂商发现后修补。

参考链接: <http://www.2cto.com/News/201106/94227.html>

2. 三维力控修复多个产品漏洞

据报道：“美国国土安全部工业控制系统网络应急响应小组的报告称，三维力控的产品在中国被广泛使用，在美国等国也有一定市场。同时发布警告，北京三维力控科技有限公司制造的软件应用程序存在漏洞，黑客可能利用这些漏洞。”针对此，三维力控科技相关负责人称，早在 5 月 7 日该信息发布之前，三维力控科技即收到国家信息安全漏洞共享平台（CNVD）的通知，随即成立了应急响应小组，在两天后做出问题响应和处理方法，并于 5 月 20 日在公司网站及其它行业网站的媒体发布补丁下载公告。除了对 CNVD 提到的两款产品（ForceControl6.1 和 PNETPower6.0）进行漏洞修复，三维力控对其余几款产品（实时数据库 6.0，eForceCon2.0 等）也进行了漏洞检测。随着以太网技术在工业控制系统中的大规模应用，安全问题受到广泛关注。三维力控科技非常重视产品的稳定性和安全性，在补丁制作完毕之后，利用电话、邮件等方式，主动通知用户及时下载补丁，修复漏洞。在问题处理过程中，三维力控科技积极保持与国家信息安全漏洞共享平台（CNVD）、美国国土安全部工业控制系统网络应急响应小组（ICS-CERT）和网络安全公司 NSS Labs 的研究员 DillonBeresford 之间的联系，并计划通过合作的方式，全面研发针对防护工业网络安全的产品，避免公共基础设施受到袭击和威胁。

参考链接: <http://www.cbinews.com/solution/news/5332.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