

信息安全漏洞周报

2010年6月21日-2010年6月27日

2010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中。

国家信息安全漏洞共享平台(以下简称 CNVD)本周共收集和整理信息安全漏洞 54 个,其中高危漏洞 2 个、中危漏洞 7 个、低危漏洞 45 个。上述漏洞全部可利用来实施远程攻击。经检测发现,网上已经出现针对“Spring Framework "classLoader"代码执行漏洞”和“Open&Compact Ftp Server 验证绕过漏洞”的零日攻击代码,请广大用户注意做好防护措施。目前,相关厂商已经为 29 个漏洞提供了修补方案,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 Firefox/Thunderbird/SeaMonkey 存在多个远程安全漏洞

Mozilla Firefox/Thunderbird/SeaMonkey是Mozilla所发布的WEB浏览器和邮件新闻组客户端产品。本周Mozilla发布多个安全公告公开了上述产品的多个安全漏洞,攻击者可以利用这些漏洞进行拒绝服务、跨站脚本、任意代码执行等攻击。具体漏洞包括: Firefox nsCycleCollector::MarkRoots函数释放后使用漏洞、Firefox插件对象引用释放后使用漏洞、Firefox JavaScript和浏览器引擎多个内存破坏漏洞、Firefox nsGenericDOMDataNode::SetTextInternal函数整数溢出漏洞、Firefox focus()函数跨域信息泄露漏洞、Firefox忽略Content-Disposition: attachment HTTP头跨站脚本漏洞。Mozilla已提供了漏洞修补方案,建议用户尽快进行修补工作。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2010-01196>

2、Enemy Territory: Quake Wars 存在多个安全漏洞

Enemy Territory: Quake Wars (《雷神之战》)是一款多玩家第一人称射击游戏。Enemy Territory: Quake Wars 存在多个安全漏洞,攻击者可利用漏洞实施拒绝服务攻击或以应用程序权限执行任意指令。具体漏洞信息为: "idGameLocal::GetGameStateObject()"函数存在设计错误,可导致任意代码执行;打印错误消息时存在边界错误漏洞,发送特殊构建的

"pureServer"和"downloadInfo"命令给客户端便可触发此漏洞。目前厂商尚未发布补丁或更新程序，建议用户继续关注厂商主页以获得解决方案。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01174>

3、IBM WebSphere Application Server存在多个安全漏洞

IBM WebSphere Application Server是一款商业性质的WEB应用服务程序。IBM WebSphere Application Server存在多个安全漏洞，攻击者可能利用漏洞泄露信息、进行拒绝服务攻击。具体漏洞包括：IBM WebSphere Application Server链接注入安全漏洞、IBM WebSphere Application Server 'default_create.log'信息泄漏漏洞、IBM WebSphere Application Server HTTP Channel拒绝服务漏洞等。目前IBM已经发布升级补丁修复了上述漏洞，建议用户尽快下载更新。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01178>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01207>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01176>

4、Apple iPhone\iPod touch 存在多个安全漏洞

iPod touch是一款苹果公司发布的媒体播放器，iPhone是其发布的智能手机。Apple iPhone\iPod touch存在多个安全漏洞，允许恶意用户获得敏感信息或执行恶意代码。具体漏洞包括：WebKit处理history.replaceState时存在信息泄露漏洞、WebKit处理表格中的越界内存访问可能导致应用意外终止或执行任意代码、PEG图形处理中存在内存破坏漏洞、CFNetwork在处理URL时存在栈溢出漏洞、“设置”选项中存在设计错误，在连接到隐藏的无线网络时“设置”可能错误的显示其他无线网络等。目前厂商已经发布升级补丁修复了上述漏洞，建议用户尽快下载使用。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01190>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01191>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01205>

小结：本周，Mozilla Firefox/Thunderbird/SeaMonkey 存在的多个严重漏洞和 Enemy Territory: Quake Wars 射击游戏等拥有大量用户的应用软件被披露存在曝出的多个高危漏洞，可允许攻击者进行拒绝服务攻击或以应用程序权限执行任意指令对用户信息安全以及用户主机安全构成严重威胁。此外，IBM WebSphere Application Server 和 Apple iPhone\iPod touch 等被披露存在多个安全漏洞，也对国内网民的上网安全构成一定影响。请广大用户注意防范，特别是一些采用 IBM WebSphere 应用服务程序的网站，需尽快采取防范或修补更新措施，避免遭受漏洞影响。

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、RedHat 安全公告（RHSA-2010:0500-01）

RedHat 于 6 月 22 日发布安全公告（RHSA-2010:0500-01），修复影响 Red Hat Enterprise Linux 4 的多个 Firefox 漏洞。具体漏洞包括：Firefox focus()函数跨域信息泄露漏洞、Firefox nsGenericDOMDataNode::SetTextInternal 函数整数溢出漏洞、Firefox JavaScript 和浏览器引擎多个内存破坏漏洞、Firefox 插件对象引用释放后使用漏洞等。

补丁下载链接：<http://www.cnvd.org.cn/patch/532>

本周要闻速递

1、Firefox 爆出安全漏洞

据国外媒体报道，Google 安全工程师近日发现，Firefox 浏览器新建窗口或标签页存在一处安全漏洞，攻击者可以向其中注入任意代码。丹尼斯-费舍尔在卡巴斯基实验室的博客中表示，该漏洞可以在用户访问正规网站时跟踪用户，攻击者伺机向用户浏览器发送控制代码。目前 Firefox 3.6.4 已经修复了这个安全漏洞，Firefox 3.6.4 采用了全新的 Lorentz 功能，Lorentz 中包括备受关注的“OOPP（Out-of-Process Plug-in）进程外插件技术。当某个插件崩溃时，整个浏览器将不会受到影响。

参考链接：<http://www.hackbase.com/news/2010-06-24/36070.html>

2、高危木马感染 420 万电脑

近日，名为“呜呜祖拉”的木马下载器在网络上广泛传播，从 6 月 22 日的监测数据来看，“呜呜祖拉”木马已侵袭了大约 420 万台电脑，不但危害特别严重，而且成为目前最活跃的高危木马。据安全专家介绍，“呜呜祖拉”的典型特征就是屏蔽杀毒软件，再把数十个盗号木马和广告程序下载到中招电脑里，伺机盗取受害网民有价值的网上帐号。当彩民通过网银支付来购买世界杯彩票时，一旦中了‘呜呜祖拉’，网银密码就可能被木马通过记录键盘操作等方式窃取，直接对彩民造成经济损失。

参考链接：http://tech.ccidnet.com/art/1099/20100624/2096041_1.html

3、CNCERT 组织召开中美网络安全对话机制第四次会议

2010 年 6 月 22 日上午，由国家互联网应急中心（CNCERT）主办的中美网络安全对话机制第四次会议，暨中美专家组成员第一次电话会议在北京召开，中美双方专家组成员共 20 余人参加了本次会议。本次电话会议双方主要就垃圾邮件定义、垃圾邮件危害以及垃圾邮件治理难点等三方面共同关注的问题深入交换了意见。本次会议还商议了下一步的工作计划，拟定两周后召开中美专家组成员第二次电话会议，主要就垃圾邮件治理具体措施进行深入探讨。电话会议后，中方专家组就垃圾邮件定义内容和下一步工作计划等问题进行了内部讨论。CNCERT 将融汇专家组意见，提出中方关于垃圾邮件治理的具体措施和建议，以尽快促成中美双方反垃圾邮件的统一建议。

参考链接：<http://www.cert.org.cn/articles/news/common/2010062825045.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