

信息安全漏洞周报

2010 年 6 月 7 日-2010 年 6 月 20 日

2010年第23期

本期漏洞基本情况

2010 年 6 月 7 日至 2010 年 6 月 20 日, 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) 两周内共收集和整理信息安全漏洞 75 个, 其中高危漏洞 8 个、中危漏洞 17 个、低危漏洞 50 个。上述漏洞中, 可利用来实施远程攻击的漏洞有 70 个。经检测发现, 网上已经出现针对“Microsoft ‘帮助和支持中心’ 应用程序漏洞”、“Linksys WAP54Gv3 无线路由器安全绕过漏洞”、“Adobe Flash Player、Reader 和 Acrobat 远程代码执行漏洞 (CVE-2010-1297)” 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 43 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。

本期重要漏洞信息

本期, CNVD 整理和发布以下重要安全漏洞信息。

1、Microsoft ‘帮助和支持中心’ 应用程序存在漏洞可能允许远程代码执行

微软发布安全公告(2219475)称, Windows XP 和 Windows Server 2003 “帮助和支持中心” (helpctr.exe) 存在一个安全漏洞, 如果攻击者诱使用户打开经特殊构造的恶意页面, 便可能远程执行恶意代码。微软表示, 目前该漏洞的相关信息和PoC代码已经被公开, 并收到局部小范围的利用此漏洞进行攻击的报告。公开的PoC代码在Windows Server 2003并不能导致执行代码。目前用户可以采用微软提供的临时修补方案(Microsoft Fix it 50459)或删除注册表中HCP协议注册, 来避免受到漏洞威胁。

参考链接: <http://www.microsoft.com/technet/security/advisory/2219475.mspx>

2、Apple Webkit 存在多个安全漏洞

Apple Safari 是一款流行的 WEB 浏览器, WebKit 是 Safari 浏览器使用的内核。WebKit 存在多个安全漏洞, 允许恶意用户利用漏洞获得系统控制权限或未授权获取应用程序执行权限。具体漏洞信息为: WebKit 拖拽或粘贴跨站越脚本漏洞、WebKit 'Node.normalize'方法远程代码执行漏洞、Webkit HTML documentFragment 跨站脚本漏洞、Apple Webkit SVG RadialGradient Run-in 远程代码执行漏洞、Apple Webkit ConditionEventListener 远程代码执

行漏洞、Apple Webkit ProcessInstruction 远程代码执行漏洞、Apple Webkit First-Letter 远程代码执行漏洞等。目前苹果公司已经发布升级补丁修复了这些漏洞，建议相关用户尽快下载使用。

参考链接: <http://support.apple.com/kb/HT4196>

3、Wireshark 0.8.20至1.2.8版本存在多个安全漏洞

Wireshark（前称Ethereal）是一个网络封包分析软件。Wireshark存在多个安全漏洞，允许恶意用户对应用程序进行拒绝服务攻击。具体漏洞信息为：SMB解析器存在空指针应用错误、ASN.1 BER解析器存在栈溢出错误、SMB PIPE解析器存在空指针应用错误、SigComp通用解压缩虚拟机存在无限循环错误、SigComp通用解压缩虚拟机存在单字节溢出错误。目前Wireshark 1.2.9和Wireshark 1.0.14版本已经修复了上述漏洞，建议相关用户尽快下载使用。

参考链接: <http://www.wireshark.org/security/wnpa-sec-2010-05.html>

4、Adobe Flash Player 10.0.45.2/AIR 1.5.3.9130 存在多个安全漏洞

Adobe发布安全公告(APSB10-14)称，Adobe Flash Player 10.0.45.2及之前版本、Adobe AIR 1.5.3.9130及之前版本存在32个安全漏洞，其中包括远程代码执行“0 day”漏洞（CVE-2010-1297），远程攻击者利用这些漏洞可导致应用程序崩溃，并可能获得系统控制权限。目前厂商已经发布升级补丁修复了这些漏洞，建议相关用户尽快下载使用。

参考链接: <http://www.adobe.com/support/security/bulletins/apsb10-14.html>

5、Ziproxy PNG 图像处理漏洞

Ziproxy是一款具备转发、压缩功能的HTTP代理服务器。它可以将页面图像转换到低质量JPEG文件或JPEG 2000，也可以压缩HTML和其他文字样的数据。Ziproxy处理部分PNG图像时存在错误，攻击者诱使用户通过Ziproxy载入经特殊构建的PNG图像，可触发基于堆的缓冲区溢出。目前Ziproxy 3.1.1已经修复了该漏洞，建议相关用户尽快下载使用。

参考链接: <http://secunia.com/advisories/40156/>

小结：上述 CNVD 所整理的漏洞信息中，微软“帮助和支持中心”漏洞的“0 day”攻击代码已经被公开并且互联网上已经有攻击行为发生。Adobe Flash Player/Adobe AIR 存在的 32 个安全漏洞，包括远程代码执行“0 day”漏洞（CVE-2010-1297）对用户威胁程度较高。Wireshark、Apple Webkit、Ziproxy 等存在的漏洞，也对国内网民的上网安全构成一定影响。提醒广大用户尽快下载相关补丁或采取相关措施，避免遭受漏洞影响。

本期重要漏洞修补信息

本期，CNVD 整理和发布以下重要安全修补信息。

1、微软发布六月安全公告

微软六月安全更新发布了 10 个安全公告，用来修复 Windows 操作系统以及 IE、Office 等软件中的 34 个安全漏洞。此次发布的 10 个公告中，有 3 个公告的安全级别为“严重”

级别，其中 2 个用于修复包括 Windows7 在内的操作系统漏洞，另 1 个用于修复 IE 浏览器漏洞。其余 7 个安全公告的安全级别则为“重要”，仅次于“严重”级别，这些补丁主要用于修复包括 Mac 版 Excel2004、2008 在内的 Office 和 Sharepoint 等的安全漏洞。

补丁下载链接：<http://www.microsoft.com/china/technet/security/current.msp>



本期要闻速递

1、Windows7/Mac OS X 被曝新致命漏洞

据国外媒体报道，黑客们将在 7 月份的 Hack in the Box 黑客大会上展示 Windows7/Mac OS X 等操作系统的新致命漏洞。该漏洞是由安全专家 Christophe Devine 和 Damien Aumaitre 在操作系统的 DMA 模块部分发现的，漏洞可以让攻击者绕过操作系统的安全保护直接获得硬件的控制权，这个漏洞与主板功能有关，因此从软件上是很难修补的。有关漏洞的信息已经提交给微软和苹果公司，但目前为止他们还没有做出回应。

参考链接：<http://www.cnbeta.com/articles/113556.htm>

2、Windows XP 系统被曝最新 0day 漏洞

Windows XP 系统被曝最新 0day 漏洞(CVE-2010-1885)，黑客可借此入侵网站，在网站服务器的 ASX 文件中嵌入漏洞代码，当用户浏览这些网站时，其个人电脑就会被木马侵入继而自动下载多种盗号木马、恶性病毒等。在此挂马过程中，用户系统的“帮助和支持中心”会主动弹出，这是判断电脑遭到此漏洞攻击的一个明显特征。安全专家表示，该漏洞主要针对 Windows XP 和 2003 系统。由于 Windows XP 系统仍在国内广泛使用，市场占有率高达 63%，而且其中部分用户使用的为非正版操作系统，无法正常更新补丁，从而对我国用户造成巨大的威胁。

参考链接：<http://www.hackbase.com/news/2010-06-19/35962.html>

3、CNCERT 组织召开中美网络安全对话机制中方专家组第三次会议

2010 年 6 月 8 日下午，由国家互联网应急中心（CNCERT）主办的中美网络安全对话机制中方专家组第三次会议在北京召开。来自中国互联网协会网络与信息安全工作委员会、中国互联网协会反垃圾邮件中心、北京邮电大学、中国联通、网易、腾讯、263、万网志成等专家组成员单位的十余位专家参加了本次会议。本次会议的议题为研讨由中国互联网协会网络与信息安全工作委员会起草的中方反垃圾邮件报告。该报告重点阐述了当前垃圾邮件治理工作的特点，提出了治理过程中存在的若干重大问题，并对中美双方下一步在垃圾邮件治理工作上应重点关注的议题提出了建议。

参考链接：<http://www.cert.org.cn/articles/news/common/2010061225034.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