

信息安全漏洞周报

2010 年 5 月 24 日-2010 年 5 月 30 日

2010年第21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 40 个,其中高危漏洞 5 个、中危漏洞 9 个、低危漏洞 26 个。上述漏洞中,可利用来实施远程攻击的漏洞有 38 个。经检测发现,网上已经出现针对“Flock 浏览器 v2.5.6 远程内存破坏漏洞”、“Webby HTTP GET 请求缓冲区溢出漏洞”、“Cisco DPC2100 安全绕过和跨站请求伪造漏洞”、“Open&Compact FTP Server 远程拒绝服务漏洞”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 24 个漏洞提供了修补方案,建议用户及时下载补丁更新,以避免遭受网络攻击。

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、Adobe Photoshop CS4 存在一个严重的安全漏洞

Adobe Photoshop 是一款流行的图形处理软件。Windows 和 Mac 版的 Photoshop CS4 11.0.1 及更早版本中存在一个严重的安全漏洞, 远程攻击者通过诱使用户在 Photoshop CS4 软件中打开恶意的 .ASL、.ABR 或者 .GRD 文件, 可以获得系统的完全控制权。Adobe 已经提供了修补方案, 请 Photoshop CS4 用户尽快升级到 Photoshop CS4 11.0.2 版本。

参考链接: <http://www.adobe.com>

2、Cisco Network Building Mediator 存在多个安全漏洞

Cisco Network Building Mediator 是思科推出的基于 IP 网的“智能互联建筑”解决方案。Cisco Network Building Mediator 存在多个安全漏洞, 具体漏洞包括: 默认验证凭证漏洞、特权提升漏洞、未授权信息截获和访问漏洞。目前厂商已经发布了升级补丁以修复这个安全问题, 建议相关用户尽快下载更新。

参考链接: <http://www.cisco.com/warp/public/707/cisco-sa-20100526-mediator.shtml>

3、Google Chrome 5.0.375.55 之前版本存在多个安全漏洞

Google Chrome 是一款开源的 WEB 浏览器。Google Chrome 5.0.375.55 之前版本存在多个

安全漏洞，具体漏洞包括：通过卸载事件处理器可进行URL地址伪造、安全浏览交互（Safe Browsing interaction）存在内存错误漏洞、白名单列表模式插件拦截器存在漏洞、拖放操作存在内存错误漏洞、执行扩展内容存在JavaScript漏洞。目前Google Chrome 5.0.375.55已经修复了以上漏洞，建议使用该产品的用户尽快下载更新。

参考链接：<http://www.google.com/chrome>

4、Ziproxy 存在整数溢出漏洞

Ziproxy是一款具备转发、压缩功能的HTTP代理服务器软件，它可以将网页图像转换成低质量的JPEG文件或JPEG 2000，也可以压缩HTML和其他文字样的数据。Ziproxy的src/image.c文件中的"jpg2bitmap()"函数和"png2bitmap()"函数存在整数溢出漏洞，远程攻击者可以通过构建恶意图像，诱使用户解析以触发基于堆的缓冲区溢出。目前Ziproxy 3.0.1已经修复此漏洞，建议相关用户尽快下载更新。

参考链接：http://secunia.com/secunia_research/2010-75/

5、EMC Avamar 'gsan'服务存在拒绝服务漏洞

EMC Avamar是一款企业级的数据备份和恢复解决应用。EMC Avamar "gsan"服务在处理网络报文时存在漏洞，攻击者可通过提交特殊构建的TCP报文，导致服务挂起，造成拒绝服务攻击。目前厂商已经发布了升级补丁以修复该安全问题，EMC Avamar 4.1用户可联系EMC客户服务获得patch #18975补丁更新，或请求升级到5.0 SP1及之后版本。建议相关用户尽快进行更新。

参考链接：<http://www.packetstormsecurity.org/1005-advisories/ESA-2010-007.txt>

小结：本周CNVD所整理的漏洞信息中，Adobe Photoshop、Cisco Network Building Mediator、Google Chrome等流行软件均出现了严重漏洞，它们可被攻击者利用来执行任意代码，对广大网民的上网安全造成严重影响。请使用上述软件的用户注意采取针对性的安全防范措施，避免受到漏洞的影响。

本周重要漏洞修补信息

本周，CNVD整理和发布以下重要漏洞修补信息。

1、HP Business Availability Center 多个安全补丁

HP 于 5 月 26 日发布编号为“emr_na-c01800059”的安全公告及相关补丁信息，修复了 HP Business Availability Center 存在的多个安全漏洞。建议用户尽快下载补丁程序修复漏洞，避免远程攻击者可以利用该漏洞窃取敏感信息或进行拒绝服务攻击。

补丁下载链接：https://www11.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c01800059



本周要闻速递

1、南非世界杯主题的恶意 PDF 开始大量传播

近日，赛门铁克公司研究人员发表报告称，黑客企图利用 2010 南非世界杯的资讯来发送恶意软件，诱使终端用户执行恶意的 PDF 文件，而这个文件中利用了 Adobe Reader 的最新漏洞（CVE-2010-0188）。预计 2010 年，借助南非世界杯主题实施的网路攻击将会增多。研究报告显示，“利用恶意 PDF”在 2009 年所有垃圾信息中的比例已经超过 80%，成为了黑客有针对性攻击的首选媒介，PDF 也是有史以来第一次超过 Microsoft Office 成为网络犯罪第一载体。对于用户而言，应该及时更新手中的 Adobe Reader 软件，如果有更高的安全需求，应该采用其他的 PDF 阅读软件。

参考链接：<http://sec.chinabyte.com/212/11348212.shtml>

2、iPhone 新漏洞 可致数据泄漏

黑客刚刚发现一个新的漏洞，它可以让入侵者自由读取 iPhone 手机内记载的信息，并且最新固件 3.1.3 也受影响，用 PIN 来锁定电话也没有用。这种漏洞很有可能导致 iPhone iRickRoll'd 蠕虫等病毒再度爆发，特别是后台运行 SSH，却没有修改默认密码的用户尤其容易受到影响。

参考链接：<http://safe.zol.com.cn/180/1802541.html>

3、微软 5 月病毒威胁报告：Win7 基本不受蓝屏影响

Win32/Alureon 病毒是导致 Windows 蓝屏的一大原因，微软近期一直在不遗余力地清除该病毒。日前微软公布了 5 月份的 Win32/Alureon 病毒清理报告，根据报告，Alureon 病毒又出现新的变体 Alureon.H，占据所检测并清理病毒的 42.9%。受此病毒影响最严重的操作系统为 Windows XP，Windows 7 用户几乎不受此影响。

参考链接：<http://www.chinaz.com/News/IT/05251163N2010.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