

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低。

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 5 个、中危漏洞 7 个、低危漏洞 42 个。上述漏洞中,可利用来实施远程攻击的漏洞有 44 个。经检测发现,网上已经出现针对“X.Org X Server RENDER 扩展'mod()'内存破坏漏洞”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 25 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、IBM WebSphere Application Server for z/OS 存在多个安全漏洞

IBM WebSphere Application Server是一款商业性的WEB应用服务基础程序。Z/OS平台下的IBM WebSphere Application Server存在多个安全漏洞,允许本地用户未经授权获得敏感信息,操作某些数据或进行拒绝服务攻击。具体漏洞包括:当完全SIP跟踪启用时,用户使用BASIC校验连接,应用程序会以明文写跟踪日志文件,用户可通过日志文件获得敏感信息;多线程多进程模块(MPM)存在错误,可泄漏敏感信息;处理会话重协商过程中,TLS协议存在错误,可被恶意利用操作部分数据;mod_proxy_ajp模块存在安全漏洞可导致拒绝服务攻击;mod_isapi模块存在错误可导致系统被破坏,可能以应用程序权限执行任意指令。目前,IBM WebSphere Application Server APAR PM12247或Fix Pack 6.1.0.31已经修复以上漏洞,建议用户下载使用。

参考链接: <http://www-01.ibm.com/support/docview.wss?uid=swg1PM12247>

2、JBoss Enterprise Application Platform 存在多个安全漏洞

JBoss Enterprise Application Platform是一款企业级应用程序平台,用于基于JBoss的应用开发。JBoss Enterprise Application Platform存在多个安全漏洞,允许恶意用户绕过部分安全限制、获得敏感信息。具体漏洞包括:访问JMX控制台缺少合理限制,攻击者提交没有指定GET或POST的HTTP请求可绕过验证;访问JBoss应用服务WEB控制台(/web-console)缺少合理限制,攻击者提交没有指定GET或POST的HTTP请求可获得敏感信息;状态Servlet

无需验证即可访问，攻击者可访问此servlet获得所部署WEB内容的详细细节。目前，Redhat Linux用户可参考如下安全公告获得补丁信息。

参考链接：<https://rhn.redhat.com/errata/RHSA-2010-0376.html>

3、Internet Download Manager FTP缓冲区溢出漏洞

Internet Download Manager是一款功能强大的下载工具，提供断点续传等多种功能。Internet Download Manager存在缓冲区溢出漏洞，远程攻击者可以利用该漏洞以应用程序权限执行任意指令。当发送部分测试序列给FTP服务器时存在边界错误，攻击者构建一个特殊的FTP URI，诱使用户使用IDM下载可触发基于栈的缓冲区溢出。目前，Internet Download Manager 5.19已经修复此漏洞，建议用户下载使用。

参考链接：<http://www.tonec.com/products/idm/index.html>

4、Adobe 的 Photoshop 和 Download Manager 存在高危漏洞

Adobe Photoshop是一款功能强大的图像处理软件。Adobe Photoshop CS4处理TIFF文件存在错误，通过诱使用户处理特殊构建的TIFF文件，可获得任意代码执行权限。恶意用户通过利用该漏洞可以应用程序权限执行任意指令。Adobe Download Manager是一款用于改进文件下载过程的工具软件，与Adobe服务器配合工作，可帮助控制Adobe Reader、Adobe Acrobat等Adobe产品的下载过程。gp.ocx ActiveX控件存在缺陷，此控件的CLSID为{E2883E8F-472F-4fb0-9522-AC9BF37916A7}且ProgID为Atlcom.get_atlcom。在初始化过程中此控件会拷贝两个参数的值到固定长度的缓冲区，如果提供足够大的值可触发缓冲区溢出。目前，Adobe Photoshop CS4 11.0.1已经修复此漏洞，建议用户下载使用。使用Adobe Download Manager 的用户可参考供应商提供的安全公告获得补丁程序。

参考链接：

<http://www.adobe.com/support/security/bulletins/apsb10-10.html>

<http://www.adobe.com/support/security/bulletins/apsb10-02.html>

5、Wing FTP Server 存在多个信息泄漏漏洞

Wing FTP Server是一款专业的跨平台FTP服务器端。Wing FTP Server存在多个安全漏洞，允许攻击者获得敏感信息。具体漏洞包括：传递给web客户端的输入在使用前缺少正确过滤，通过目录遍历攻击可访问用户HOME目录之外的文件；当使用HTTP协议时存在一个未明错误，可泄漏敏感信息。目前，Wing FTP Server 3.4.1已经修复以上漏洞，建议用户下载使用。

参考链接：<http://www.wftpserver.com/>

小结：本周 CNVD 所整理的漏洞信息中，WEB 应用服务、企业级应用程序平台、Photoshop 图像处理软件、FTP 服务器端等均出现了严重漏洞。这些漏洞严重影响了我国网民的信息安全，请广大用户注意采取安全防范措施，尽快下载相关补丁程序进行修补。

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 Linux 安全公告

Redhat Linux 于 4 月 26 日发布了一个安全公告以及相应补丁，修复了 JBoss Enterprise Application Platform 多个安全漏洞。建议用户尽快下载使用，以避免远程攻击者利用漏洞绕过部分安全限制或获得敏感信息。

补丁下载链接：<https://rhn.redhat.com/errata/RHSA-2010-0376.html>

本周要闻速递

1、微软 SharePoint 发现高危 XSS 漏洞

近日，微软安全应急小组确认了微软 SharePoint Server 2007 产品中存在严重跨站脚本本漏洞 (XSS)。黑客可以通过浏览器利用该漏洞，执行任意的 JavaScript 代码。该漏洞的具体细节已经被公布，微软表示将提供补丁修复这一漏洞。

参考链接：<http://www.hackbase.com/news/2010-05-01/34990.html>

2、Google 修复 Chrome 三个重要安全漏洞

Google 周三发布了最新稳定版的 Chrome 软件，修复了此前版本中的 Javascript 和 Java 插件漏洞，google 还同时修复了软件中的其他三个安全漏洞。三个安全漏洞修复的分别是：解决利用 google 网站来进行的路过式威胁、HTML5 的内存泄露威胁、字体渲染中的内存错误。

参考链接：<http://www.hackbase.com/news/2010-04-30/34984.html>

3、“狗皮膏”木马肆虐互联网

近日，网上大量用户反映“IE 首页被改成了 123.***.com”，通过某杀毒公司分析，这类问题是由一个恶性木马点击器病毒导致的，某杀毒公司将其命名为“狗皮膏”木马。安全专家介绍，用户访问某些恶意网站后会感染该木马，中毒电脑的浏览器首页被强制锁定为某网址。电脑一旦中毒，则其安装的杀毒软件无法升级，如果用户手工删除病毒文件 netsflt.sys，则会无法上网，目前至少有近万网民受害。

参考链接：<http://www.hackbase.com/news/2010-04-26/34912.html>

4、全世界 13%垃圾邮件来自美国，中国占 1.5%列第 15

根据 net-security 的报道，美国继续成为垃圾邮件的头号发源地，全世界超过 13%的垃圾邮件来源于美国，每天有数百万封垃圾邮件从美国发出。另外，需要指出的是，来源于中国的垃圾邮件数量已经大大缩减，已经跌出前十名，仅排位 15，占全部垃圾邮件的 1.5%。前十名分别是：美国 13.1%；印度 7.3%；巴西 6.8%；韩国 4.8%；越南 3.4%；德国 3.2%；英国 3.1%；俄国 3.1%；意大利 3.1%；法国 3.0%。

参考链接：<http://it.sohu.com/20100430/n271851731.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