

信息安全漏洞周报

2010年8月23日-2010年8月29日

2010年第33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、整理信息安全漏洞94个,其中高危漏洞12个、中危漏洞12个、低危漏洞70个。上述漏洞中,可利用来实施远程攻击的漏洞有86个。目前,有关厂商已针对57个漏洞提出了修补方案,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、Adobe Shockwave Player 存在多个安全漏洞

Adobe Shockwave Player是一款用于播放使用Director Shockwave Studio制作的网页的外挂软件。Adobe Shockwave Player存在多个安全漏洞,攻击者可利用这些漏洞实施拒绝服务攻击或以应用程序权限执行特定代码。具体漏洞包括:Adobe Shockwave Director csww块解析远程代码执行漏洞、Adobe Shockwave Player tSAC块解析内存破坏漏洞、Adobe Shockwave Player Director文件FFFFFF45记录处理远程代码执行漏洞、Adobe Shockwave Director PAMI块解析远程代码执行漏洞、Adobe Shockwave Director tSAC块解析远程代码执行漏洞、Adobe Shockwave Player Director文件记录处理远程代码执行漏洞、Adobe Shockwave Player TextXtra分配器整数溢出远程代码执行漏洞、Adobe Shockwave Director mmap块解析远程代码执行漏洞、Adobe Shockwave Player tSAC块非法搜索内存破坏漏洞、Adobe Shockwave Director rcsL块解析远程代码执行漏洞、Adobe Shockwave Player解析.dir媒体文件内存破坏漏洞、Adobe Shockwave Player解析.dir DIRAPI.dll内存破坏漏洞、Adobe Shockwave Player解析.dir IML32.dll存在多个内存破坏漏洞、Adobe Shockwave Player Director rcsL块解析堆溢出漏洞。目前Adobe已经发布补丁程序修复上述安全漏洞,建议相关用户尽快下载更新。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2010-01776>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01742>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01744>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01748>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01749>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01757>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01758>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01710>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01716>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01717>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01718>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01719>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01726>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01727>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01728>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01729>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01730>

2、Apple iTunes和Mac OS X存在多个安全漏洞

Apple iTunes 是一款用于 Mac 和 PC，可播放所有数字音乐和视频的应用程序；Apple Mac OS X 是一款基于 UNIX 的操作系统。这两款产品存在多个安全漏洞，攻击者可利用漏洞实施拒绝服务攻击。具体漏洞包括：Apple iTunes 对日志文件的不安全操作致使本地特权提升漏洞、Apple iTunes DLL 装载任意代码执行漏洞、Apple Mac OS X CoreGraphics 处理 PDF 文件存在堆缓冲区溢出漏洞、Apple Mac OS X Type 服务处理嵌入式字体存在栈缓冲区溢出漏洞、Apple Mac OS X 2010-005 允许绕过扫描的漏洞、Apple Mac OS X 处理证书主机名存在漏洞、Apple Mac OS X PHP libpng 库漏洞、Apple Mac OS X Samba 缓冲区溢出漏洞、Apple Mac OS X CFNetwork 组件存在漏洞、Apple Mac OS X ClamAV 执行任意代码的漏洞。目前 Apple 已经发布升级包修复上述安全漏洞，建议相关用户尽快下载更新。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01775>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01760>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01756>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01755>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01754>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01753>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01763>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01762>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01766>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01765>

3、MySQL存在多个安全漏洞

MySQL是一款轻量级的关系数据库管理系统。MySQL存在多个安全漏洞，攻击者可利用漏洞实施拒绝服务攻击。具体漏洞包括：MySQL “TEMPORARY InnoDB” 表拒绝服务漏洞、MySQL使用唯一“SET”列加入(join)相关的表时存在漏洞、MySQL可空列特征的

TEMPORARY InnoDB表存在漏洞、MySQL处理部分畸形参数传递给“BINLOG”语句时存在漏洞、MySQL处理NULL参数传递给“IN()”或“CASE”存在漏洞、MySQL处理DDL语句存在漏洞、MySQL“LOAD DATA INFILE”语句存在漏洞、MySQL查询执行“EXPLAIN”语句时存在漏洞、MySQL使用“HANDLER”接口存在漏洞。目前MySQL 5.1.49版本已经修复上述安全漏洞，建议相关用户尽快下载使用。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01685>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01733>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01736>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01735>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01734>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01732>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01739>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01738>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01737>

4、IBM 多款产品存在安全漏洞

IBM 的Tivoli Storage Manager FastBack管理平台 and Autonomy KeyView软件包存在多个安全漏洞，攻击者可以利用漏洞以应用程序权限执行特定代码。具体漏洞包括：IBM Tivoli Storage Manager FastBack存在远程代码执行和拒绝服务漏洞、IBM Lotus Notes Autonomy KeyView WK3解析存在远程代码执行漏洞、IBM Lotus Notes Autonomy KeyView Office轮廓解析存在远程代码执行漏洞、IBM Lotus Notes Autonomy KeyView word解析存在远程代码执行漏洞。目前IBM已经发布安全公告以修复上述安全漏洞，建议相关用户尽快下载使用。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01682>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01723>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01722>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01721>

小结：本周，微软发布了新的安全建议 (MSA2269637)，提醒用户防范因应用程序采用不安全的 DLL 加载方式而导致的远程代码执行威胁，即“DLL 劫持攻击”。攻击者可以利用这个漏洞，通过打开特制的程序或者文档获得计算机控制权限。目前互联网上已经有人公布了大量存在问题的应用软件列表，建议用户继续关注微软官网，提高警惕并做好安全防范工作。

此外，公众常用的 Adobe Shockwave Player 播放器、Apple iTunes 播放器和 Mac OS X 操作系统、MySQL 数据库等软件产品均曝出安全漏洞，对相关用户的信息安全和公共互联网安全构成威胁，请实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、RealNetworks 发布安全公告

RealNetworks 厂商 8 月 26 日发布了有关其产品 RealPlayer 的安全公告，以修复 RealNetworks RealPlayer FLV 解析整数溢出漏洞、RealNetworks RealPlayer 畸形 IVR 对象索引代码执行漏洞等。攻击者可利用这些漏洞进行拒绝服务攻击或以应用程序权限执行特定代码，给相关用户带来严重的安全威胁。CNVD 提醒广大用户及时下载更新补丁以避免受到影响。

补丁下载链接：<http://www.cnvd.org.cn/patch/896>
<http://www.cnvd.org.cn/patch/897>

本周要闻速递

1、多款应用软件被曝 DLL 劫持漏洞

近日，DLL 劫持漏洞成为了用户关注的安全热点，包括微软 Windows 操作系统和多款第三方应用软件在内的程序均被检测存在此类漏洞。相关网站公布的漏洞波及报告中，包括用户最为常用的 Photoshop 等工具也赫然在列。安全专家表示，“DLL 劫持漏洞”使得用户打开图片、音乐、视频、BT 种子、网页等文件时都存在中毒的风险。攻击者利用 DLL 劫持漏洞构造一个特殊的 DLL 文件，并将这个 DLL 文件打包到一些 JPG、PPT、MP3、MPG、HTML 文件中分发，用户解压后双击打开这些文件时，病毒被立即触发。对于这个漏洞所引发的安全风险，从根本上解决需要众多软件开发商检查自己的软件代码，对存在缺陷的软件进行版本更新。

参考链接：http://tech.ccidnet.com/art/1099/20100830/2169445_1.html

2、IBM 安全团队:云计算最大威胁来自防护问题

8 月 27 日消息，据国外媒体报道，IBM X-Force 安全团队 26 日发布报告称，随着云计算和远程访问的不断增长，防护问题成为其不得不面对的硬伤。报告称，网络应用程序数量每年以 55% 的速度增长，但其具有大量的安全漏洞。脚本中和其它网络应用程序代码中包含大量的恶意代码，比一年前增加了 52%。但是，网络钓鱼比一年前下降 82%。同时，浏览器开发商也通过警告用户来阻止网络钓鱼犯罪。IBM X-Force 安全团队的报告称，截止 26 日，对于报告中列出的超过一半的安全漏洞，供应商在 2010 年上半年都没有及时提供补丁。

参考链接：http://security.zdnet.com.cn/security_zone/2010/0827/1864116.shtml

3、国内首份域名安全报告发布：超 50% 域名不安全

8 月 26 日消息，国内互联网基础服务提供商北龙中网在京发布了国内首份《中国域名服务及安全现状报告》。报告显示，目前我国域名服务器总量接近百万台，其中超过 50%

的域名服务器相对不安全，更有 57%的重要信息系统存在域名解析风险。北龙中网报告数据显示，从 2009 年 8 月到 2010 年 8 月，全球大型的域名攻击多达 20 起，但是由于域名攻击手段隐蔽、技术先进而导致防范较为困难，也给诸多企业造成困难。中国互联网网络信息中心的毛伟透露，目前我国完全拥有自主管理的域名只有“.cn”和“.中国”这两个后缀的域名。工信部通信保障局的闫宏强呼吁，国内网站应尽量采用“.cn”域名，因为“这是我国自主可控的，一旦发生意外情况，解决起来也快速简便”。

参考链接：<http://www.cert.org.cn/articles/news/common/2010082625111.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