

信息安全漏洞周报

2010年9月13日-2010年9月19日

2010年第36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 102 个，其中高危漏洞 10 个、中危漏洞 47 个、低危漏洞 45 个。上述漏洞中，可利用来实施远程攻击的漏洞有 78 个。经跟踪发现，网上已经出现针对“MediaHuman Music Converter 缓冲区溢出漏洞”和“A-PDF All to MP3 Converter '.wav'文件处理缓冲区溢出漏洞”的零日攻击代码，请相关用户注意做好相关防护措施。本周收录的安全漏洞中，已有 78 个漏洞由相关厂商提供了修补方案，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、Microsoft 多款产品存在安全漏洞

微软Windows操作系统、Outlook及IIS等产品存在多个安全漏洞，攻击者可利用漏洞提升特权、获得敏感信息、实施拒绝服务攻击或以应用程序权限执行任意代码。具体漏洞包括：Microsoft IIS请求头缓冲区溢出漏洞、Microsoft Windows后台打印服务远程代码执行漏洞、Microsoft Windows多个系统win32k.sys文件缓冲区溢出漏洞、Microsoft MPEG-4 Codec媒体文件远程代码执行漏洞、Microsoft Windows CSRSS内存分配本地特权提升漏洞、Microsoft Exchange Server Outlook Web Access跨站请求伪造漏洞、Microsoft IIS 5.1基础验证安全绕过漏洞、Microsoft Windows和Office unicode脚本处理器内存破坏漏洞、Microsoft Windows RPC内存分配远程代码执行漏洞、Microsoft LSASS ADAM/ADLDS特权提升漏洞、Microsoft IIS重复参数请求拒绝服务漏洞、Microsoft Outlook 'Online Mode'远程堆缓冲区溢出漏洞、Microsoft WordPad文本转换器Word 97文件解析内存破坏漏洞。目前微软已发布安全公告及补丁修复上述安全漏洞，建议相关用户尽快下载使用。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02057>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02058>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02068>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02031>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02035>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02036>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02037>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02038>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02039>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02041>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02042>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02051>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02043>

2、Microsoft .NET Framework ASP.NET 信息泄漏漏洞

Microsoft .NET Framework 是一款流行的软件开发工具包。微软近日发布 2416728 号安全公告，称正在调查一个新公开披露的 ASP.NET 漏洞，该漏洞可导致信息泄漏。攻击者利用该漏洞可能访问到包括目标服务器 web.config 在内的任何文件、获取目标服务器上的加密信息或通过回传错误数据获取错误返回代码，从而发动进一步攻击。漏洞几乎存在于 ASP.NET 所有已发布版本中，微软目前尚无补丁发布，希望广大 ASP.NET 用户加强防范并继续关注厂商官网，以便及时下载补丁更新。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02115>

3、IBM 多个产品存在安全漏洞

IBM 的 Lotus Domino 服务器、AIX 操作系统和 Records Manager 等产品存在多个安全漏洞。远程攻击者可利用漏洞获得敏感信息、绕过安全限制、以应用程序权限执行任意代码或实施跨站脚本攻击。具体漏洞包括：IBM Records Manager 跨站脚本攻击漏洞、IBM Records Manager 信任管理漏洞、IBM Records Manager 开放重定向漏洞、IBM Lotus Sametime Connect Web Container 存在未明安全漏洞、IBM AIX sa_snap 存在未明漏洞、IBM AIX sa_snap “/usr/esa/sbin/sa_snap”程序存在漏洞、IBM Lotus Domino iCalendar 远程栈缓冲区溢出漏洞、IBM DB2 撤除“PUBLIC”组数据对象触发错误的漏洞、IBM FileNet 应用程序引擎重定向和跨站脚本漏洞、IBM FileNet 应用程序引擎存在多个安全漏洞、IBM DB2 使用“update”语句编译组合 SQL 语句存在错误漏洞。目前 IBM 已发布更新程序修复上述漏洞，建议相关用户尽快下载使用。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02052>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02050>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02049>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02034>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02033>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02032>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02055>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02111>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02110>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02093>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02112>

4、OTRS核心系统存在多个安全漏洞

OTRS（Open Ticket Request System）是用于管理用户投诉和售后问题的系统，OTRS核心系统存在多个安全漏洞，远程攻击者可利用这些漏洞进行脚本注入和拒绝服务攻击。具体漏洞包括：OTRS核心系统存在跨站脚本漏洞、OTRS核心系统存在拒绝服务漏洞。目前OTRS 2.4.8和2.3.6已修复上述漏洞，建议相关用户尽快下载使用。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02095>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02094>

5、Adobe Flash Player 存在未明任意代码执行漏洞

Adobe Flash Player是一款多媒体程序播放器，Adobe Flash Player存在一个严重的安全漏洞，攻击者可利用漏洞获取系统控制权限或导致系统崩溃。目前此漏洞在网络上已被利用。Adobe厂商尚未发布升级补丁修复该安全漏洞，建议用户关注厂商主页以获得修补方案。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02025>

6、Cisco无线LAN控制器存在权限许可和访问控制漏洞

Cisco无线LAN控制器(WLC) 是使用轻量级接入点协议(LWAPP)管理Cisco Aironet接入点的应用设备。4.2至6.0版本的Cisco无线LAN控制器存在权限许可和访问控制漏洞，远程认证用户可借助未明向量绕过访问限制，修改配置并可能获得管理权限。Cisco已经发布安全公告（cisco-sa-20100908-wlc）及更新程序修复该安全漏洞，建议相关用户尽快下载使用。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02065>

小结：本周，Microsoft 发布 9 月安全公告修复了 Windows 操作系统、Outlook 及 IIS 等产品中存在的 13 个安全漏洞并发布 2416728 号公告称正在调查一个新公开披露的 ASP.NET 漏洞。此外，IBM 多个产品、OTRS、Adobe Flash Player、Cisco 无线 LAN 控制器均出现安全漏洞。这些漏洞对用户的信息安全和公共互联网网络安全构成威胁，请使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、Apple发布4个重要漏洞修补补丁

继上周 Apple 发布多个修补程序后，本周 Apple 又更新了几个重要漏洞的修补升级程序。Safari 是苹果家族机器操作系统中默认捆绑的 WEB 浏览器。此次 Apple 发布的补丁程

序修补了 Safari 存在的 4 个重要漏洞，其中 3 个的危害级别为“高危”，1 个为“中危”。CNVD 提醒广大 Safari 用户尽快下载安装补丁程序，避免引发漏洞相关的网络安全事件。

补丁下载链接：<http://www.cnvd.org.cn/patch/1029>
<http://www.cnvd.org.cn/patch/1030>
<http://www.cnvd.org.cn/patch/1031>
<http://www.cnvd.org.cn/patch/1079>



本周要闻速递

1、Adobe 高危漏洞现身国内网络

Adobe Reader 是 Adobe 公司出品的专业 PDF 阅读软件，在国内外均有众多用户。9 月 15 日，Adobe 公开承认“PDF 安全漏洞”的存在，并称这个安全漏洞影响 Reader 9.3.4 版以及用于 Windows、Mac OS X 和 Unix 操作系统的早期版本的 Reader 软件。Adobe 认为，上述安全漏洞很“严重”，因为它可以使黑客控制任何一台正在运行 PDF 的电脑。目前，Adobe 软件 0Day 漏洞已现身国内网络。Adobe 尚未发布针对“PDF 安全漏洞”的补丁。网络安全专家建议用户在官方未正式发布安全补丁之前，一定不要打开或接收陌生人传来的 PDF 文件。

参考链接：<http://tech.sina.com.cn/it/2010-09-20/16404678283.shtml>

2、黑客利用 Linux Web 服务器漏洞获取超级权限

64 位系统 Linux 在 32 位兼容模式下存在一处漏洞，可以用来增强用户权限，攻击者可以利用漏洞闯入系统并利用 Web 服务器的一处漏洞获取受害系统的超级权限或准入许可。目前已经有一个利用该漏洞的方法在流通。内核开发者已经在软件仓库纠正了这一瑕疵，Linux 的发行厂商们也很可能近期会推出新的内核来修复这一漏洞。

参考链接：http://tech.ccidnet.com/art/302/20100919/2191577_1.html

3、Intel 证实 HDCP 主密钥泄露 蓝光世界崩盘

Intel 近日证实，经过调查日前在互联网上泄露的所谓 HDCP 主密钥的确是真实有效的，这也就意味着数百万蓝光光盘、播放器等设备的保护盾已经在瞬间土崩瓦解，所有蓝光光盘都可以自由解锁、复制。最可能的利用方式是有黑客制作一颗计算机芯片，在其中嵌入泄露的这个主密钥，用来解码蓝光光盘，而软件解码器的可能性不大。

参考链接：<http://news.mydrivers.com/1/175/175251.htm>

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