

信息安全漏洞周报

2010年7月12日-2010年7月18日

2010年第27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高。

国家信息安全漏洞共享平台(以下简称CNVD)本周共收集、整理信息安全漏洞65个,其中高危漏洞16个、中危漏洞27个、低危漏洞22个。上述漏洞中,可利用来实施远程攻击的漏洞有62个。经检测发现,网上已经出现针对“PHP-Nuke 'Web_Links'模块SQL注入漏洞”、“Siemens SIMATIC WinCC 默认密码安全绕过漏洞”和“Microsoft Windows LNK文件自动执行文件漏洞”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54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、Microsoft Windows LNK 文件存在自动执行漏洞

Windows支持使用快捷方式或LNK文件。LNK文件是指向本地文件的引用,点击LNK文件与点击快捷方式具有相同的效果。LNK文件存在安全漏洞,攻击者可通过构建特殊的LNK文件,致使Windows自动执行该文件所指定的代码。这些代码可能位于USB驱动、本地和远程文件系统、光驱等其他位置,使用资源管理器查看LNK文件所在位置就可触发此漏洞。此漏洞已经被黑客大量利用。目前,微软已发布了一个FixIt小工具修复该漏洞,建议尽快下载使用,避免因此漏洞而遭受网络攻击。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2010-01407>

2、Apache Struts XWork 存在安全绕过漏洞

Apache Struts是用于构建Java web应用的开源平台。Apache Struts中的XWork "ParameterInterceptor"类在限制服务端对象访问时存在漏洞,攻击者通过特殊构建OGNL (Object-Graph Navigation Language)表达式可修改服务端对象或执行任意命令。目前厂商已发布了安全公告及相应的补丁信息,建议相关用户尽快下载使用。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2010-01359>

3、Microsoft Access ActiveX控件存在远程代码执行漏洞

Microsoft Access是微软Office套件中的关系数据库管理系统。Microsoft Access实例化

ImexGrid和FieldList等ActiveX控件在未初始化变量时存在内存破坏漏洞，攻击者可利用此漏洞获取当前用户的权限，执行特定代码。目前Microsoft已经发布安全公告（MS10-044）及相应的补丁信息，建议相关用户尽快下载使用。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01356>

4、Microsoft Outlook 存在远程代码执行漏洞

Microsoft Outlook是微软Office套件捆绑的邮件客户端软件。Microsoft Outlook在校验Email消息中PR_ATTACH_METHOD属性的ATTACH_BY_REFERENCE值的附件时存在错误，如果目标用户打开经攻击者特殊构建的Email附件，可在没有任何警示的情况下执行远程UNC路径中的代码。目前Microsoft已经发布安全公告（MS10-045）及相应补丁信息，建议相关用户尽快下载使用。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01355>

5、Winamp VP6存在内容解析栈溢出漏洞

Winamp是一款流行的媒体播放程序。Winamp中的"vp6.w5s"组件在解析畸形的Flash视频数据时存在整数和缓冲区溢出漏洞，攻击者诱使用户打开经构建特殊的FLV文件后可以以应用程序权限执行任意指令。目前Winamp 5.58已经修复了此漏洞，建议相关用户尽快下载使用。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01365>

小结：本周，微软发布了7月份的安全更新，修复了来自Windows和Office的一系列漏洞，其中包括之前披露并已被黑客利用的Windows帮助中心漏洞；Oracle发布安全公告（cpujul2010）以及相应补丁修复了多个安全漏洞，请广大用户尽快下载使用。同期，在国内应用广泛的Windows操作系统、MS office套件、Winamp播放器、Apache Struts 建站平台均曝出高危漏洞，并可被攻击者利用于实施网络攻击，对国内用户的信息安全和互联网网络安全环境均构成严重威胁，请使用以上软件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、发布以下重要安全修补信息。

1、Oracle 2010年7月份更新修复多个漏洞

Oracle在7月15日发布了一个安全公告（cpujul2010）以及相应补丁，修复了包括Oracle Secure Backup、Oracle Business Process Management、Sun Access Manager、Sun Java Communications Suite、Sun Solaris和Oracle WebLogic等在内的多个安全漏洞。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漏洞获得敏感信息或以应用程序权限执行任意命令。

补丁下载链接：<http://www.cnvd.org.cn/patch/627>

<http://www.cnvd.org.cn/patch/628>

<http://www.cnvd.org.cn/patch/629>
<http://www.cnvd.org.cn/patch/630>
<http://www.cnvd.org.cn/patch/631>
<http://www.cnvd.org.cn/patch/632>
<http://www.cnvd.org.cn/patch/633>
<http://www.cnvd.org.cn/patch/638>
<http://www.cnvd.org.cn/patch/639>
<http://www.cnvd.org.cn/patch/640>
<http://www.cnvd.org.cn/patch/641>
<http://www.cnvd.org.cn/patch/642>
<http://www.cnvd.org.cn/patch/643>
<http://www.cnvd.org.cn/patch/644>
<http://www.cnvd.org.cn/patch/645>
<http://www.cnvd.org.cn/patch/646>
<http://www.cnvd.org.cn/patch/647>
<http://www.cnvd.org.cn/patch/648>
<http://www.cnvd.org.cn/patch/649>
<http://www.cnvd.org.cn/patch/650>
<http://www.cnvd.org.cn/patch/651>
<http://www.cnvd.org.cn/patch/652>
<http://www.cnvd.org.cn/patch/653>
<http://www.cnvd.org.cn/patch/654>
<http://www.cnvd.org.cn/patch/655>
<http://www.cnvd.org.cn/patch/656>
<http://www.cnvd.org.cn/patch/657>

2、FreeType 2.4.0 更新修复多个安全漏洞

FreeType 是一个流行的字体函数库。FreeType 及其 truetype 字节码在处理某些字体文件和字体轮廓时存在堆溢出、整数溢出和无效内存释放漏洞，当用户受骗打开了特制字体就可能导致拒绝服务或执行任意代码。本周，厂家发布的 FreeType 2.4 已经修复了漏洞，建议用户尽快下载使用，避免远程攻击者可以利用漏洞以链接此库的应用程序权限执行任意指令。

补丁下载链接：<http://www.cnvd.org.cn/patch/621>

<http://www.cnvd.org.cn/patch/622>
<http://www.cnvd.org.cn/patch/623>
<http://www.cnvd.org.cn/patch/613>
<http://www.cnvd.org.cn/patch/624>
<http://www.cnvd.org.cn/patch/625>



本周要闻速递

1、警惕具有数字签名的恶意软件

程序的数字签名是用来识别软件身份的凭证，一般的正规软件都具有数字签名。所以，普通网友一旦发现某程序具有数字签名，都会认为此软件是正规的良性软件。但事实却并非如此。卡巴斯基实验室近期就截获到一种带有数字签名的恶意软件样本。此恶意软件为一种名为“桌面推广助手”（Trojan-Downloader.Win32.Small.knz）的下载器木马。此软件采用 VB 编写，并且带有数字签名，但其本质却是一种恶意软件。一旦运行，它会自动下载两个木马程序到受感染计算机并运行，同时，在没有用户的许可下，下载安装某种浏览器以及某款网络游戏大厅客户端。不仅如此，此恶意软件还会自动创建服务，实现开机自动启动。并且在桌面和快速启动栏，创建多个快捷方式，还会修改系统的 DNS 设置，严重危害用户的计算机安全。

参考链接：http://tech.china.com/zh_cn/news/safe/895/20100713/16023940.html

2、苹果漏洞最多，第三方软件漏洞最危险

安全厂家 Secunia 本周公布 2010 年上半年安全报告，发现苹果在五年来首度超越甲骨文，成为安全漏洞最多软件供应商，但第三方应用程序因缺少容易使用的定期更新机制而风险最高。产品漏洞多寡的排序，苹果位居第一，其他依序是甲骨文、微软、HP、Adobe、IBM、VMware、思科、Google 及 Mozilla 等。近年来研究人员及骇客，逐渐锁定第三方应用程序漏洞，Secunia 说，这是因为微软开始强化安全功能并启用自动更新机制修补漏洞，而使得骇客攻陷视窗作业系统的机会变少，但修补第三方应用软件的问题可能要几年的时间才有办法解决。

参考链接：<http://www.hackbase.com/news/2010-07-14/36470.html>

3、CNNIC 报告称我国网民达 4.2 亿 六成曾遭木马攻击

近日，中国互联网络信息中心（CNNIC）在京发布了《第 26 次中国互联网络发展状况统计报告》。报告显示，截至 2010 年 6 月底，我国网民规模达 4.2 亿人，较 2009 年底增加 3600 万人；互联网普及率持续上升至 31.8%，与 2009 年底相比提高了 2.9 个百分点。值得关注的是，今年上半年 59.2% 的网民在使用互联网过程中遇到过病毒或木马攻击，有 30.9% 的网民账号或密码被盗过，网络安全问题仍然制约着中国深层次的网络应用发展。

参考链接：<http://www.nsfocus.net/news/7304>

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