

信息安全漏洞周报

2010年7月26日-2010年8月1日

会员版

2010年第29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、整理信息安全漏洞59个,其中高危漏洞1个、中危漏洞4个、低危漏洞54个。上述漏洞中,可利用来实施远程攻击的漏洞有51个。经检测发现,网上已经出现针对“WM Downloader '.m3u'文件缓冲区溢出漏洞”、“sSMTP 'standardize()'缓冲区溢出漏洞”的零日攻击代码,请广大用户注意做好相关防护措施。目前,相关厂商已经为34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、WebKit 存在多个远程安全漏洞

WebKit是一款由苹果公司开发的开源HTML渲染引擎,是Apple Safari、Google Chrome等网页浏览工具的内核。近日曝出WebKit存在多个安全漏洞,攻击者利用漏洞可进行拒绝服务攻击,并以应用程序权限执行特定代码。具体漏洞包括:WebKit 'foreignObject'元素释放后使用远程代码执行漏洞、WebKit 'Focus'元素释放后使用远程代码执行漏洞、WebKit 'inline'元素处理内存破坏漏洞、WebKit CSS计数器内存破坏漏洞、WebKit Jit编译的JavaScript stubs远程代码执行漏洞、WebKit JavaScript字符串对象远程堆缓冲区溢出漏洞、WebKit 'use'元素处理内存破坏漏洞、WebKit 'floating'元素处理内存破坏漏洞、WebKit ':first-letter'和':first-line'伪元素处理内存破坏漏洞、WebKit动态文本节点修改远程内存破坏漏洞、WebKit规则表达式处理远程内存破坏漏洞、WebKit JavaScript数组带符号错误远程代码执行漏洞、WebKit 'font-face'和'use'元素释放后使用远程代码执行漏洞。目前苹果公司已经发布更新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-2010-01494>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01495>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01496>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01477>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01478>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01479>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01480>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01482>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01511>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01497>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01498>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01509>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01510>

2、Autonomy KeyView 存在多个安全漏洞

Autonomy KeyView 是一款用于导出、转换和查看各种格式文件的软件包。Autonomy KeyView 存在多个安全漏洞，可触发缓冲区溢出。具体漏洞包括：Autonomy Keyview 的 WordPerfect 5 reader (wosr.dll)存在边界错误漏洞、Autonomy Keyview 的 RTF reader (rtfsr.dll)存在符号错误漏洞、Autonomy Keyview 解析存在整数下溢错误的漏洞、Autonomy Keyview 解析某些记录过程中存在分配指针数组的漏洞、Autonomy Keyview 解析部分存在记录错误的漏洞、Autonomy Keyview 转换浮点值 SpreadSheet Lotus 123 reader (wkssr.dll)存在边界错误漏洞、Autonomy Keyview 解析文档存在边界错误漏洞。目前 Autonomy 已经发布补丁程序以修复上述安全漏洞，建议相关用户尽快下载更新。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01514>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01515>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01516>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01517>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01518>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01519>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01513>

3、Google Chrome 5.0.375.125之前版本存在多个安全漏洞

Google Chrome是谷歌公司开发的一款开源WEB浏览器。Google Chrome存在多个安全漏洞，攻击者利用漏洞可进行拒绝服务、跨域脚本、绕过安全限制或执行任意代码攻击。具体漏洞包括：布局代码存在未明错误，会导致泄漏内存内容；相关超大canvas标签处理存在未明错误；渲染代码存在未明错误可破坏内存；SVG处理存在错误可破坏内存；相关主机名截断和不正确省略存在未明错误。目前Google Chrome 5.0.375.125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-2010-01489>

4、Apple Mac OS X WebDAV 内核扩展存在拒绝服务漏洞

Mac OS X苹果公司开发的一款基于UNIX的操作系统。Mac OS X支持使用WebDAV共享，由内核扩展实现。WebDAV内核扩展中存在拒绝服务漏洞，如果用户发布了包含超长字段值的mount请求，就可能导致内核忙碌。目前苹果公司尚未发布相应的升级补丁，建议

相关用户继续关注厂商主页以获取修补方案。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2010-01502>

5、Microsoft IE 处理帧边界属性时存在拒绝服务漏洞

Microsoft IE浏览器在处理包含超长整数值或字符串的frame.frameBorder属性时存在漏洞,攻击者可通过诱使用户访问经特殊构建的WEB页面,导致应用程序崩溃。目前微软尚未发布补丁或更新程序修复上述漏洞,建议相关用户继续关注厂商主页以获取修补方案。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2010-01485>

小结: 本周 CNVD 收集的漏洞信息中,三大 WEB 浏览器 Microsoft IE、Apple Safari 和 Google Chrome 均曝出多个安全漏洞,对网民的上网安全构成较大影响; Apple Mac OS X 操作系统、Autonomy KeyView 软件包也曝出安全漏洞,可被攻击者利用实施远程或本地攻击,对国内相关用户的信息安全和公共互联网网络安全均构成威胁,请使用以上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、MediaWiki 发布升级程序

MediaWiki 是一套以 GPL 授权发行的 Wiki 引擎。MediaWiki 于 7 月 28 日发布两个升级程序 1.16.0 和 1.15.5 版本,这两个版本已修复 MediaWiki 存在的两个安全漏洞: MediaWiki 'profileinfo.php'跨站脚本漏洞和 MediaWiki 'api.php'信息泄漏漏洞。建议用户尽快下载使用升级程序。

补丁下载链接: <http://www.cnvd.org.cn/patch/718>
<http://www.cnvd.org.cn/patch/719>

本周要闻速递

1、微软发布 EMET 安全工具包

7 月 29 日消息,微软在黑帽计算机安全会议上展示了一个新的工具,这个新工具的名字为“Enhanced Mitigation Experience Toolkit”(EMET,增强的减灾体验工具包)。它拥有自己的用户界面,显示所有当前的进程和可用于这些进程的安全补丁。用户能够使用新的安全漏洞补丁修复老程序的安全漏洞。

参考链接: <http://www.hackbase.com/news/2010-07-30/36878.html>

2、HTTPS 和 SSL 协议存在安全漏洞

HTTPS(安全 HTTP)和 SSL/TLS(安全套接层/传输层安全)协议是 Web 安全和可信电子商务的核心,但 Web 应用安全专家 Robert "RSnake" Hansen 和 Josh Sokol 在近日举办

的黑帽大会上宣布，Web 浏览器的基础架构中存在 24 个不同危险程度的安全漏洞。这些漏洞基本上使 HTTPS 和 SSL 所提供的浏览器保护荡然无存。Hansen 和 Sokol 指出，攻击者要利用这些漏洞，首先需要发起中间人攻击。攻击者一旦劫持了浏览器会话，就可以利用这些漏洞中的大多数对会话进行重定向，从而窃取用户凭据或者从远程秘密执行代码。对于电子商务应用来说，这些攻击简直是毁灭性的灾难。

参考链接：<http://www.hackbase.com/news/2010-08-02/36933.html>

3、谷歌 Android 操作系统存在漏洞

Spider Labs 主管 Nicholas Percoco 与其同事在拉斯维加斯举行的 Defcon 黑客大会上发布一款可以攻击谷歌 Android 智能手机的工具——Rootkit，以促使设备生产商修复可以让黑客获取用户电子邮件和文本信息的漏洞。

参考链接：<http://www.cnbeta.com/articles/118009.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