

信息安全漏洞周报

2010 年 7 月 19 日-2010 年 7 月 25 日

2010 年第 28 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 46 个，其中高危漏洞 14 个、中危漏洞 10 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 42 个。经检测发现，网上已经出现针对“海海软件 PDFReaderOCX ActiveX 控件‘URL’属性缓冲区溢出漏洞”、“CoolSoft PowerFTP ‘RETR’命令缓冲区溢出漏洞”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 36 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、Mozilla Firefox/Thunderbird/SeaMonkey 存在多个远程安全漏洞

Mozilla Firefox/Thunderbird/SeaMonkey 是 Mozilla 开发的 WEB 浏览器/邮件客户端/新闻组客户端软件，该三款产品存在多个安全漏洞，可被攻击者利用于拒绝服务攻击、执行特定代码、提升权限、获取敏感信息等恶意活动。具体漏洞信息为：Mozilla Firefox/Thunderbird/SeaMonkey 存在多个存储安全漏洞；Firefox DOM 属性克隆远程代码执行漏洞；Mozilla Firefox/Thunderbird/SeaMonkey 用于遍历文档对象模型的 NodeIterator 接口实现存在漏洞；Mozilla Firefox/Thunderbird/SeaMonkey 用于存储插件参数元素的名字和值的代码存在漏洞；Mozilla Firefox/Thunderbird/SeaMonkey 执行任意 JavaScript 漏洞；Mozilla Firefox/Thunderbird/SeaMonkey 处理外部字体资源的引用存在漏洞；Mozilla Firefox/Thunderbird/SeaMonkey Web Worker 方法错误读取或解析资源漏洞；Mozilla Firefox/Thunderbird/SeaMonkey canvas 元素违反了同源策略漏洞；Mozilla Firefox/Thunderbird/SeaMonkey 恶意 WEB 页绕过某些字符过滤方法的漏洞；Mozilla Firefox/Thunderbird/SeaMonkey 伪造地址栏内容漏洞；Mozilla Firefox/Thunderbird/SeaMonkey 可跨域读取数据漏洞；Mozilla Firefox/Thunderbird/SeaMonkey 敏感 URL 参数可被跨域泄漏漏洞。目前厂商已经发布更新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-2010-01422>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01423>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01424>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01425>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01426>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01427>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01428>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01429>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01430>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01431>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01432>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01433>

2、海海软件 PDFReaderOCX ActiveX 控件存在"URL"属性缓冲区溢出漏洞

海海软件 PDF 阅读器是一款免费的阅读器软件。海海软件 PDF 阅读器所安装的 PDFReaderOCX ActiveX 控件未正确验证 URL 属性参数, 当用户受骗访问了恶意网页并在文件名中提供了超过 2048 字节的超长字符串, 便可能触发栈溢出, 导致执行特定代码。目前厂商尚未发布补丁或更新程序, 建议相关用户临时将 clsid: 28CB49D6-E530-442B-A182-79F047C3AA1B 设置为 kill bit, 以避免受到漏洞影响。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2010-01420>

3、Cisco CDS Internet Streamer存在目录遍历漏洞

Cisco Content Delivery System是思科公司开发的内容分发系统解决方案。Cisco CDS 所捆绑的Cisco Internet Streamer存在目录遍历漏洞, 攻击者可以通过特制的URL来利用这个漏洞, 从Web Server文档目录外读取设备上包括用于保护管理员账号详细信息和系统日志的口令文件在内的任意文件。目前Cisco Content Delivery System 2.5.7已经修复了该安全漏洞, 建议相关用户尽快下载使用。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2010-01452>

4、HP OpenView 网络节点管理器存在多个安全漏洞

HP OpenView 网络节点管理器是一款惠普公司开发和维护的网络管理系统软件, 具有强大的网络节点管理功能。HP OpenView 网络节点管理器存在多个安全漏洞, 允许攻击者进行缓冲区溢出攻击, 以应用程序权限执行特定代码。具体漏洞包括: HP OpenView网络节点管理器ov.dll库的execvp_nc函数远程栈溢出漏洞; HP OpenView "nnmrptconfig.exe" CGI 存在缓冲区溢出漏洞。目前惠普已经发布相应的升级补丁, 建议相关用户尽快下载使用。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2010-01444>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01443>

5、Microsoft DirectX DirectPlay 拒绝服务漏洞

DirectPlay8 (DP8)是Microsoft DirectX中的网络协议实现, 用于多个游戏和小型服务程序。Microsoft DirectX存在多个安全漏洞, 允许攻击者执行拒绝服务攻击。具体漏洞信息

为：通过报文0xc2中断服务器，可导致服务器不能处理入站报文并没有任何错误提示；通过0xc8类型报文可使服务停止响应；通过0xcc类型报文可在InterlockedDecrement中引起访问冲突；当调用回调时某些游戏没有验证DP8层返回的数据，会由于空指针引用而使应用程序崩溃。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-2010-01434>

小结：本周，Mozilla 发布了多个有关 WEB 浏览器和邮件/新闻组客户端的漏洞并提供了更新程序，海海软件尚未为其产品 PDF 阅读器提供修补方案，建议用户采取临时解决方案。同期，Cisco 的内容分发系统解决方案、HP 的 OpenView 网络节点管理器均曝出高危漏洞，并可被攻击者利用来实施远程或本地网络攻击，对国内用户的信息安全和互联网网络安全环境带来威胁，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、VMware 安全公告（VMSA-2010-0012）

VMware vCenter Update Manager 是用于 VMware ESX 主机和选定的 Microsoft 及 Linux 虚拟机的自动化补丁程序管理解决方案。VMware 于 7 月 19 日发布安全公告（VMSA-2010-0012），修复 VMware vCenter Update Manager 存在的两个安全漏洞：VMware vCenter 升级管理程序跨站脚本漏洞和 VMware vCenter 升级管理程序信息泄漏漏洞。建议用户尽快下载使用相应补丁。

补丁下载链接：<http://www.cnvd.org.cn/patch/666>

<http://www.cnvd.org.cn/patch/665>

本周要闻速递

1、WPA2 协议爆 0day 漏洞

无线安全研究者称发现了迄今最强的加密验证标准——WPA2 安全协议的漏洞，该漏洞可能会被网络内部的恶意用户利用。来自 AirTight Network 无线网络安全公司的研究人员将其命名为“漏洞 196”。这个绰号的来源则是 IEEE 802.11 标准（2007 版）埋下漏洞的页码。漏洞 196 会导致一个类似于中间人的攻击方式：凭借内部授权用户和开源软件，攻击者可以在半空中解密其他用户私密数据、注入恶意流量至网络、危害其它授权设备。

参考链接：<http://www.hackbase.com/news/2010-07-26/36720.html>

2、Windows Shell 零日漏洞攻击上升

据国外媒体报道，上周 Windows Shell 爆出的零日漏洞，已遭到两项攻击，和 Stuxnet 蠕虫病毒一样，该攻击使用一个特制的快捷方式自动激活恶意程序。此次恶意攻击的第一个恶意软件被称为 Dulkis-A，是一种 Windows 蠕虫病毒，另外一个 Chymine，是木马程序，用来窃取被感染的电脑的数据。目前，微软尚未修复 Windows Shell 漏洞，不过于周二发布了一个工具，可阻止该漏洞被利用。不幸的是，该工具未能阻止该漏洞被攻击。

参考链接：<http://www.hackbase.com/news/2010-07-26/36722.html>

3、Safari 被曝新漏洞，可导致个人数据被窃

Safari 浏览器的自动填充功能存在安全漏洞，此次出现的漏洞可允许攻击者获取到用户所有联系人的工作、居住地址甚至是电子邮件地址。安全人员还发布了一个验证该漏洞的概念代码网站，将用户的联系人姓名，公司，城市，州，国家和电子邮件全部列在一个页面上。目前，该漏洞影响 Safari 4 和 5，主要影响 Mac 系统，Windows 用户在攻击代码修改后也有可能受到影响，建议用户通过禁用自动填充功能来暂时修补该漏洞。

参考链接：<http://www.cnbeta.com/articles/117211.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