

信息安全漏洞周报

2010 年 12 月 20 日-2010 年 12 月 26 日

2010 年第 50 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 104 个，其中高危漏洞 37 个、中危漏洞 39 个、低危漏洞 28 个。上述漏洞中，可利用来实施远程攻击的漏洞有 93 个。经跟踪发现，网上已经出现针对“Microsoft Internet Explorer CSS 内存损坏漏洞”、“Apple Mobile Safari 'decodeURIComponent' 远程拒绝服务漏洞”、“Google Urchin 'urchin.cgi' 本地文件包含漏洞”等的零日攻击代码，请使用相关产品的用户注意做好防护措施。本周收录的安全漏洞中，已有 76 个漏洞由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、微软发布了关于 IE 浏览器的 0day 预警

本周，微软发布了关于 IE 浏览器存在高危 0day 漏洞的预警公告，Microsoft Internet Explorer 存在 CSS 内存损坏漏洞，受此漏洞影响的 IE 浏览器产品包括 IE6、7、8 三个版本。攻击者可利用该漏洞进行网页挂马等攻击。由于 HTML 解释器模块的动态链接库文件 mshtml.dll 在处理包含各种“@import”规则的参考 CSS(层叠样式表)文件的网页时，会导致一个名为“use-after-free”的页面文件处理错误。利用这个漏洞，攻击者可通过构造特定网页使得 IE 浏览器执行其中嵌入的恶意代码。目前，针对此漏洞的攻击代码已经被披露。更为严重的是，这些攻击代码能够使 ASLR (Address Space Layout Randomization, 即：地址空间布局随机化) 和 DEP (Data Execution Prevention, 即：数据执行保护) 等微软 Windows 操作系统的保护机制失效。由于微软尚未对此漏洞发布补丁程序，CNVD 建议用户提高警惕，关注微软官方的最新动态。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03476>

2、IBM Lotus Notes Traveler 存在多个安全漏洞

本周，IBM 的产品 Lotus Notes Traveler 出现了多个安全漏洞。IBM Lotus Notes Traveler 软件是一款电子邮件产品，能够快速访问电子邮件、日历、地址簿、杂志和待办事项。CNVD 本周收录的漏洞包括：IBM Lotus Notes Traveler servlet 跨站脚本攻击漏洞、IBM Lotus Notes Traveler 资源管理错误漏洞、IBM Lotus Notes Traveler 预设访问限制绕过漏洞(CVE-2010-4546)、IBM Lotus Notes Traveler 预设访问限制绕过漏洞(CVE-2010-4547)、IBM Lotus Notes Traveler 拒绝服务漏洞、IBM Lotus Notes Traveler 权限许可和访问控制漏洞、IBM Lotus Notes Traveler 输入验证漏洞、IBM Lotus Notes Traveler 空指针引用漏洞、IBM Lotus Notes Traveler 内存泄露漏洞、IBM Lotus Notes Traveler Domino API 拒绝服务漏洞。攻击者可以利用这些漏洞实施执行任意代码和注入 WEB 脚本等攻击，造成用户应用程序崩溃或权限被获取。目前 IBM 已经发布了补丁程序修复这些漏洞，CNVD 建议广大用户及时下载更新，避免引发漏洞的相关安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03459>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03458>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03457>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03456>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03427>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03425>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03423>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03420>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03418>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03417>

3、Apple 存在多个安全漏洞

本周，Apple 的产品 Time Capsule、AirPort Extreme 和 Mobile Safari 均出现了安全漏洞。Time Capsule 是 Apple 的无线网络存储设备，AirPort Extreme 是针对家庭、学校和小微企业的无线解决方案，Mobile Safari 是一款 WEB 浏览器。CNVD 本周收录的具体漏洞包括：Apple Time Capsule 和 AirPort Base Station 多个远程安全漏洞、Apple Mobile Safari 'decodeURIComponent' 远程拒绝服务漏洞、Apple Mobile Safari 'decodeURIComponent' 远程拒绝服务漏洞。其中，“Apple Mobile Safari 'decodeURIComponent' 远程拒绝服务漏洞”和“Apple Mobile Safari 'decodeURI()' 远程拒绝服务漏洞”为 0day 漏洞，互联网上已经出现针对该漏洞的攻击程序。攻击者可以利用这些漏洞绕过安全限制，造成拒绝服务或应用程序崩溃。除“Apple Time Capsule 和 AirPort Base Station 多个远程安全漏洞”外，Apple 尚未发布其余漏洞补丁程序，CNVD 建议广大用户继续关注厂商主页，以获取最新版本。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03455>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03434>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03409>

4、RealNetworks Realplayer 出现多个安全漏洞

RealNetworks RealPlayer 是一款流行的媒体播放程序。本周，RealNetworks Realplayer 出现了多个安全等级为“高”的漏洞。CNVD 收录的 RealPlayer 漏洞包括：RealNetworks RealPlayer 堆缓冲区溢出漏洞（CVE-2010-4377、CVE-2010-4379）、RealNetworks RealPlayer 数组索引漏洞、RealNetworks RealPlayer 整数溢出漏洞、RealNetworks RealPlayer 任意代码执行漏洞、RealNetworks RealPlayer 远程代码执行漏洞、RealNetworks RealPlayer 整数缓冲区溢出漏洞、RealNetworks Realplayer 初始化函数内存破坏漏洞等。攻击者可以利用这些漏洞执行任意代码。目前，厂商已经发布了漏洞的补丁程序，CNVD 建议用户及时下载使用，避免引发此漏洞相关的安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03512>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03511>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03507>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03506>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03505>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03504>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03497>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03416>

5、Opera 存在多个安全漏洞

Opera 是一款支持多种平台的 WEB 浏览器。Opera 本周出现了多个安全漏洞。CNVD 收录的 Opera 漏洞包括：Opera 设计错误漏洞、Opera 信息泄漏漏洞、Opera 权限许可和访问控制漏洞、Opera Turbo 无安全指示漏洞、Opera X.509 证书加密问题漏洞、Opera 拒绝服务漏洞及多个未明漏洞（CVE-2010-4581、CVE-2010-4586、CVE-2010-4586、CVE-2010-4587）。攻击者可以利用这些漏洞获得敏感信息或绕过访问控制。其中，“Opera 未明漏洞（CVE-2010-4581、CVE-2010-4586、CVE-2010-4587）”和“Opera 拒绝服务漏洞”的危险等级为“高危”。目前，厂商已经发布了漏洞的补丁程序，CNVD 建议用户及时下载使用，避免引发此漏洞的相关安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03484>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03483>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03482>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03481>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03479>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03478>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03472>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03471>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03470>

小结：本周，Microsoft 发布了关于 IE 浏览器存在高危 0day 漏洞的预警公告，目前，针对此漏洞的攻击代码已经被披露，微软尚未对此漏洞发布补丁程序。Apple 的 Time Capsule、AirPort Extreme 和 Mobile Safari 均出现了安全漏洞。此外，使用范围也越来越广泛的 RealNetworks Realplayer 媒体播放器和 Opera 浏览器也出现多个高危漏洞，对国内用户的信息安全和互联网网络安全构成较为严重的威胁，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、IrfanView 发布升级程序修补了多个安全漏洞

IrfanView 是一款在 Windows 操作系统上运行的免费图像查看程序。本周，IrfanView 发布了多个升级程序用于修复多个安全漏洞，以避免攻击者利用漏洞获得敏感信息或绕过访问控制。CNVD 已收录相关补丁，请广大用户及时下载更新，避免引发漏洞相关的安全事件。

补丁下载链接：<http://www.cnvd.org.cn/patch/2159>
<http://www.cnvd.org.cn/patch/2161>
<http://www.cnvd.org.cn/patch/2162>
<http://www.cnvd.org.cn/patch/2163>
<http://www.cnvd.org.cn/patch/2442>

本周要闻速递

1. 微软 IE 浏览器存在严重漏洞 攻击者可诱导用户访问恶意网站

据国外媒体报道，微软公司于 12 月 22 日承认所有版本的 IE 浏览器都存在一个严重漏洞，攻击者可以利用这个漏洞诱导用户访问恶意网站。微软安全响应中心表示这个漏洞的影响是有限的，并没有任何被攻击的用户。微软表示将尽快修补这个漏洞，但并不打算仓促发布一个紧急补丁，如果情况有变，将及时发布紧急补丁。在微软发布补丁之前，用户可以使用增强减灾体验工具加强防御。

参考链接：http://news.ccidnet.com/art/946/20101224/2279151_1.html

2. 纽约旅游公司发生黑客恶意盗取 11 万张信用卡信息事件

12 月 21 日消息，黑客闯进了一家纽约旅游公司的网站，并盗取了 11 万张银行卡号码。该公司发言人表示，黑客使用 SQL 注入方式袭击网站服务器，获取了姓名、地址、电子邮件地址、信用卡账号、到期信息和信用卡验证码等信息。这些信息足以用于使用信用卡网上购物。该公司于两周前通知客户该黑客袭击事件，并表示已经使用了几项重要的措施来

提高数据的安全性，目前已经封锁了该服务器的访问权并安装了防火墙，提高系统的反黑能力。

参考消息：http://news.ccidnet.com/art/11099/20101221/2275911_1.html

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