

信息安全漏洞周报

2010 年 10 月 25 日-2010 年 10 月 31 日

2010 年第 42 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 109 个，其中高危漏洞 13 个、中危漏洞 65 个、低危漏洞 31 个。上述漏洞中，可利用来实施远程攻击的漏洞有 90 个。经跟踪发现，网上已经出现针对“Mozilla Firefox 3.5/3.6 document.write 和 DOM 插入堆缓冲区溢出漏洞”、“Winamp 5.5.8.2985 (in_mod plugin) 栈缓冲区溢出漏洞”以及“Microsoft Windows 'lpksetup.exe' 'oci.dll' DLL 装载任意代码执行漏洞”的零日攻击代码，请使用上述漏洞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 80 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、Mozilla Firefox 存在多个安全漏洞

Mozilla Firefox（火狐）是由 Mozilla 基金会与开源团体共同开发的网页浏览器。本周，Mozilla Firefox 出现了多个安全漏洞，CNVD 收录的火狐安全漏洞包括：Mozilla Firefox 3.5/3.6 document.write 和 DOM 插入堆缓冲区溢出漏洞、Mozilla Firefox 浏览器引擎拒绝服务漏洞、Mozilla Firefox 文本渲染功能栈缓冲区溢出漏洞、Mozilla Firefox 释放后使用漏洞、Mozilla Firefox LookupGetterOrSetter 函数缓冲区溢出漏洞等，其中“Mozilla Firefox 3.5/3.6 document.write 和 DOM 插入堆缓冲区溢出漏洞”为 0-day 漏洞，互联网上已经出现针对 Mozilla Firefox 的恶意代码攻击；后面 4 个漏洞的安全等级为“高危”。攻击者可以利用上述漏洞实施拒绝服务攻击、影响浏览器正常运行或执行任意代码等恶意活动。目前，Mozilla 已为上述所有漏洞发布了漏洞修补程序，CNVD 提醒广大用户及时下载更新，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-2010-02595>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02596>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02598>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02599>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02600>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02601>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02603>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02604>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02605>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02636>

2、Opera 多款产品存在安全漏洞

Opera 是一款支持多平台的开源 WEB 浏览器。本周，CNVD 收录了 Opera 产品的多个漏洞，具体包括：Opera 跨站脚本攻击和任意代码执行漏洞、Opera URL 欺骗输入验证漏洞、Opera CSS 解析权限许可和访问控制漏洞、Opera SVG 文档缓冲区溢出漏洞、Opera 跨站脚本攻击漏洞、Opera 信息泄露漏洞等。攻击者可利用这些漏洞获取敏感信息、执行任意代码、实施拒绝服务攻击等。目前 Opera 已经发布补丁或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-2010-02579>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02574>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02575>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02576>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02578>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02579>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02580>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02581>

3、Adobe存在多个安全漏洞

Adobe公司的Adobe Reader/Acrobat、Adobe Flash Player、Adobe RoboHelp均存在漏洞。Adobe Reader是一款的PDF文件阅读软件；Adobe RoboHelp是一款专业开发工具，可用于开发帮助系统、电子教学内容、知识库以及项目方案和流程。CNVD本周收录的Adobe漏洞包括：Adobe Acrobat/Reader/Flash远程代码执行漏洞、Adobe RoboHelp跨站脚本攻击漏洞（CVE-2010-2885、CVE-2010-2886）。攻击者成功利用漏洞后可导致受影响系统崩溃、获取系统控制权限、注入任意web脚本或HTML。其中，“Adobe Acrobat/Reader/Flash远程代码执行漏洞”的危险漏洞等级为“高危”，厂商计划在2010年11月发布升级程序，建议相关用户关注Adobe公司主页以便及时获取修补方案。Adobe RoboHelp已经修复了上述安全漏洞，建议相关用户尽快下载使用。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02634>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02631>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02630>

4、IBM多款产品存在安全漏洞

本周，CNVD收录了IBM公司多款产品的漏洞。包括：IBM Informix Dynamic Server 'oninit.exe'栈缓冲区溢出漏洞、IBM Informix Dynamic Server 'librpc.dll'整数溢出漏洞、IBM Informix Dynamic Server缓冲区溢出漏洞、IBM Rational Quality Manager信任管理漏洞、IBM Tivoli Access Manager for e-business跨站脚本漏洞、IBM solidDB 'solid.exe'拒绝服务攻击漏洞、IBM solidDB 'solid.exe'数字错误漏洞、IBM WebSphere MQ主题标识名(DN) X.509证书伪造漏洞、IBM solidDB 'solid.exe'栈消耗漏洞和IBM WebSphere MQ证书欺骗漏洞等。受漏洞影响的产品包括：Informix Dynamic Server数据库管理软件、solidDB数据库、Tivoli Access Manager for e-business、Rational Quality Manager软件和WebSphere MQ应用程序等。攻击者可以利用这些漏洞实施拒绝服务攻击、执行任意代码、欺骗证书认证、获取管理员访问权限、获取敏感信息以及劫持目标用户会话等。其中“IBM Informix Dynamic Server 'oninit.exe'栈缓冲区溢出漏洞”为高危漏洞，目前IBM已经发布安全公告及补丁修复部分安全漏洞，CNVD建议相关用户尽快下载使用。另外，IBM尚未发布solidDB相关漏洞的补丁，CNVD也提醒广大用户关注厂商主页及时获得修补方案。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02613>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02570>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02573>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02625>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02556>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02572>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02571>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02544>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02582>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02629>

5、SAP Business Objects产品存在多个安全漏洞

SAP Business Objects是SAP公司推出的全球领先的商务智能产品套件。本周，CNVD收录了该产品的多个安全漏洞，具体漏洞包括：SAP Business Objects 的"Central Configuration Manager"中存在漏洞、SAP Business Objects的"Crystal Reports/viewrpt.cwr"脚本漏洞、SAP Business Objects "modules"参数传递漏洞、SAP Business Objects在创建CUID时dswsbobje/services/biplatformHTTP中的"GenerateCuids" SOAP方法存在漏洞、SAP BusinessObjects Enterprise XI 3.2中的Dswsbobje在生成不同错误消息时存在漏洞。攻击者可以利用上述漏洞提升权限、限制网络端口、获取敏感信息和实施拒绝服务攻击等。目前网上已出现针对该漏洞的攻击行为，相关厂商尚未发布升级补丁修复这些安全漏洞，CNVD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-2010-02555>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02554>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02553>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02552>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02551>

6、HP多款产品存在安全漏洞

本周，CNVD收录了HP公司多款产品存在的多个漏洞。其中较为重要的漏洞包括：HP Operations Orchestration 跨站脚本攻击漏洞、HP Virtual Connect Enterprise Manager任意文件读取漏洞、HP Systems Insight Manager跨站请求伪造漏洞、HP Systems Insight Manager未明权限提升漏洞、HP Asset Center跨站脚本攻击漏洞、HP Virtual Server Environment任意文件下载漏洞、HP Insight Control虚拟机管理未明远程特权提升漏洞、windows平台下的HP Insight Control Server Migration未明未授权访问漏洞、HP Insight Control Server Migration未明未授权访问漏洞、Windows平台下的HP Insight Control Server Migration数据访问本地特权提升漏洞、HP Insight Control虚拟机管理跨站请求伪造漏洞（CVE-2010-3987）、HP Insight Control虚拟机管理跨站请求伪造漏洞（CVE-2010-3989）、HP Virtual Connect Enterprise Manager未明文件下载漏洞、HP Operations Orchestration (CVE-2010-3985)未明跨站脚本漏洞。受这些漏洞影响的相关产品包括：Operations Orchestration工作流自动化软件、Virtual Connect Enterprise Manager Cisco管理逻辑服务器、Systems Insight Manager服务器管理系统、Asset Center生命周期资产管理软件、Virtual Server Environment虚拟机服务器环境管理软件、Insight Control virtual machine management系统和Operations Orchestration软件。攻击者可以利用这些漏洞注入任意web脚本、读取任意文件、劫持未明受害者的认证、获得权限提升等；此外，攻击者还会在未授权的情况下获得敏感信息或劫持目标用户会话、下载系统上的任意文件、获得SYSTEM权限等。目前，HP已经发布安全公告及补丁程序修复这些安全漏洞，CNVD建议相关用户尽快下载使用。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02542>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02543>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02562>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02563>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02564>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02565>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02566>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02567>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02568>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02594>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02609>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02611>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02627>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02628>

小结：本周，Mozilla 公司出现了 Firefox 3.5/3.6 document.write 和 DOM 插入堆缓冲区溢出高危 0-day 漏洞，经跟踪发现已被攻击者利用。此外，HP、IBM、SAP Business Objects、Opera、Adobe 等应用广泛的产品均出现了安全漏洞，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、Adobe 发布漏洞修补了多个漏洞

Adobe 于 10 月 28 日在官方网站上更新了多个漏洞的补丁程序。这些漏洞包括 CNVD 收录的“Adobe Shockwave Player rcsL Chunk EAX 寄存器内存破坏漏洞”，详细信息请参考 Adobe 发布的安全公告 APSA10-04，攻击者成功利用该漏洞可以在受影响的系统上执行恶意代码。CNVD 提醒使用 Adobe Shockwave Player 11.5.8.612 及之前版本的用户及时更新到新发布的 Adobe Shockwave Player 11.5.9.615 版本，以避免引发漏洞相关的信息安全事件。

补丁下载链接：<http://www.cnvd.org.cn/patch/1540>

<http://www.cnvd.org.cn/patch/1538>

<http://www.cnvd.org.cn/patch/1537>

本周要闻速递

1、AVG 截获最新“0day 漏洞”病毒

AVG 病毒实验室 28 日截获到利用 Adobe Flash Player 的 0day 漏洞攻击用户计算机的病毒。日前该漏洞已被 Adobe 核实为 CVE-2010-3654，但是尚未给出修复漏洞的补丁。经分析，该漏洞存在于 authplay.dll 当中。该组件在以下各产品都存在，因此以下该程序都受到该漏洞的影响：Windows, Macintosh, Linux and Solaris 下的 Adobe Flash Player 10.1.85.3 及更早的版本；Android 移动平台下的 Adobe Flash Player 10.1.95.2 及更早的版本；Windows, Macintosh and UNIX 平台下的 Adobe Reader 9.4 和更早的 9.x 版本；Windows 和 Macintosh 下的 9.4 和更早的 9.x 版本。当用户访问利用该漏洞的恶意 pdf，或者访问包含利用该漏洞的 swf 的网页时，该 pdf/swf 会执行漏洞利用代码。除了通过访问恶意网页攻击用户之外，该病毒还会被当作邮件附件发送给用户。只要用户访问恶意 pdf，就会执行病毒代码。建议广大相关用户更新到最新的病毒码，以保护自身的计算机安全。

参考链接：<http://tech.sina.com.cn/b/2010-10-29/16021546867.shtml>

2、Adobe 将取代微软 成为黑客首要攻击目标

黑客入侵某个网络系统最常采用的攻击方式就是利用该网络中最普遍存在的某个软件的漏洞，而漏洞率较高，同时又不经常更新的软件就经常成为黑客的首选。在 2002 年，大部分黑客选择的这个软件很可能是微软的 Windows 系统。而如今，所选择的很可能是比 Windows 漏洞更多，更脆弱的 Adobe Reader 或 Flash Player。根据安全软件厂商 F-Secure 的统计，当前近半数的攻击所利用的都是 Acrobat Reader 这个网民们最常用的 PDF 阅读器。

而基于 web 的 PDF 文件攻击在去年前三个半月的统计数量为 128 例，今年同期则上升到了超过 2300 例。

参考链接: <http://tech.it168.com/a2010/1026/1118/000001118231.shtml>

3、 iPhone4 锁屏漏洞苹果做回应 11 月更新修复漏洞

报道称，iPhone 出现安全漏洞，其他人可以轻松绕过您 iPhone 的锁屏密码，从而获取联系人、语音信箱和通话历史等资料。即使在最新版本的系统 iOS 4.1 下的 iPhone 4 仍存在这一漏洞。特别是如果绕过密码的步骤已经在网络传开，iPhone 用户难免会担心自己的隐私遭窃取。苹果发言人联系 Wired.com 科技新闻网站，回应了 iPhone 的安全漏洞：“我们已经获知该问题。我们会在 11 月发布的 iOS 4.2 软件更新中为顾客修复这一漏洞。”其实曾在 2008 年 iPhone 也出现过类似的漏洞，可让其他人绕过锁屏密码访问 iPhone 的邮箱、联系人和书签。但苹果很快就提供软件更新进行修复。

参考链接: http://news.xinhuanet.com/eworld/2010-10/28/c_12709953.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