

信息安全漏洞周报

2011 年 2 月 14 日-2011 年 2 月 20 日

会员版

2011 年第 7 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 112 个，其中高危漏洞 59 个、中危漏洞 22 个、低危漏洞 31 个。上述漏洞中，可被利用于实施远程攻击的漏洞有 104 个；网上已经出现零日攻击代码的有 2 个，分别是“Microsoft Active Directory 'BROWSER ELECTION'缓冲区溢出漏洞”和“PHP 'grapheme_extract()'空指针引用拒绝服务漏洞”。请使用相关产品的用户注意做好防护措施。本周收录的漏洞中，已有 96 个漏洞具备官方修补方案，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、Oracle 产品安全漏洞

Oracle Database 是一款大型数据库系统软件；Java Runtime Environment 则是为 JAVA 应用程序提供运行环境。本周，Oracle 公司的 Database 和 Java Runtime Environment 被披露存在多个安全漏洞。CNVD 收录的漏洞包括：Oracle 数据库导出工具缓冲区溢出漏洞、Oracle Java Webstart 可信 JNLP 扩展远程代码执行漏洞、Oracle Java 运行时 NTLM 验证信息泄漏漏洞、Oracle Java Applet 剪贴板注入远程代码执行漏洞、Oracle Java 无符号 Applet Applet2ClassLoader 远程代码执行漏洞、Oracle Java XGetSamplePtrFromSnd 远程代码执行漏洞。攻击者可以利用这些漏洞执行任意代码。除“Oracle 数据库导出工具缓冲区溢出漏洞”外，厂商已经提供了漏洞的补丁信息，CNVD 提醒广大用户及时下载更新，避免引发漏洞相关的安全事件。

参考链接：
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04266>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04216>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04214>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04213>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04212>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04211>

2、Adobe 产品安全漏洞

Adobe 的产品 Flash Player 是一款处理 Flash 文件的应用程序；Reader/Acrobat 是一款处理 PDF 文件的应用程序；Shockwave Player 是一款用于播放使用 Director Shockwave Studio 制作的网页外挂软件。本周，Adobe 的 Flash Player、Reader/Acrobat 和 Shockwave Player 均出现了多个综合评级为“高危”的安全漏洞。CNVD 收录的 Adobe 漏洞包括：Adobe Shockwave Player 任意代码执行漏洞（CVE-2010-2587、CVE-2010-2588）、Adobe Flash Player 任意代码执行漏洞、Adobe Flash Player 库装载漏洞、Adobe Reader / Acrobat 中的 rt3d.dll 组件缓冲区溢出漏洞、Adobe Reader / Acrobat 跨站脚本漏洞等。攻击者可以利用漏洞在受影响的程序中执行任意代码或使应用程序崩溃。目前，Adobe 已经发布了这些漏洞的修补程序，CNVD 提醒广大用户尽快下载安装补丁程序，避免引发漏洞相关的网络安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04234>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04233>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04187>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04185>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04180>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04178>

3、PHP 产品安全漏洞

PHP 是一款流行的编程语言。本周，PHP 产品出现了多个安全漏洞。CNVD 收录的漏洞包括：PHP 'grapheme_extract()'空指针引用拒绝服务漏洞、PHP 输入验证漏洞、PHP 整数溢出漏洞、PHP 后置链接漏洞、PHP Exif 扩展'exif_read_data()'函数远程拒绝服务漏洞、PHP '_zip_name_locate()'空指针引用拒绝服务漏洞。攻击者可以利用漏洞使应用程序崩溃。上述漏洞中，“PHP 'grapheme_extract()'空指针引用拒绝服务漏洞”的综合评级为“高危”，互联网上已出现针对该漏洞的攻击代码，主要影响的是 PHP 5.3.5 版本。CNVD 提醒广大用户加强防范措施。除“PHP 整数溢出漏洞、PHP 后置链接漏洞”外，厂商已经发布了其余漏洞的补丁信息，CNVD 提醒广大用户及时下载更新，避免引发漏洞相关的安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04267>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04249>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04248>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04247>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04196>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04195>

4、Microsoft Active Directory 'BROWSER ELECTION'缓冲区溢出漏洞

Microsoft Windows Server 是一款微软发行的服务器操作系统。由于 Microsoft Windows Server 的 Mrxsmb.sys 驱动在处理用户提交的'BROWSER ELECTION'请求时相关参数处理存在错误，攻击者提交特定构造的恶意请求可触发缓冲区溢出。目前，互联网上已经出现了针对该漏洞的攻击代码，主要影响 Windows Server 2003 多个版本。厂商尚未发布该漏洞的补丁程序，CNVD 提醒广大用户随时关注厂商主页，并加强防范措施。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04189>

5、Smarty 存在未明漏洞

Smarty 是一个使用 PHP 编写的模板引擎。本周，Smarty 出现了综合评级为“高危”的未明漏洞，远程攻击者可以利用漏洞进行恶意攻击。CNVD 收录的具体漏洞包括：Smarty 存在未明漏洞（CVE-2010-4722、CVE-2010-4723、CVE-2010-4725）、Smarty math 插件存在未明漏洞，Smarty 输入验证漏洞。目前，厂商已经发布了这些漏洞的补丁程序，CNVD 提醒广大用户及时下载更新，避免引发此类漏洞相关的安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04226>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04225>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04222>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04220>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04210>

小结：本周，微软 Windows Server 操作系统被披露存在一个 Windows BROWSER 协议零日漏洞，攻击者可以通过提交恶意请求利用该漏洞，触发缓冲区溢出。目前，微软尚未发布这个漏洞的解决方案。Oracle Database 和 Java Runtime Environment 出现了多个安全漏洞，攻击者可以利用这些漏洞执行任意代码。此外，Adobe 的 Flash Player、Reader/Acrobat 和 Shockwave Player 以及 PHP 产品、Smarty 产品均出现了安全漏洞，对互联网用户的信息安全和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、IBM 发布升级程序,修补了多个产品的安全漏洞

本周，IBM 发布多个升级程序用于修补了 IBM FileNet P8、Lotus Connections 等产品的多个安全漏洞，避免远程攻击者可以利用漏洞绕过安全限制，修改对象属性或提升特权。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/2999>
<http://www.cnvd.org.cn/patch/2956>



本周要闻速递

1. 微软披露 Windows BROWSER 协议零日漏洞 恐影响 Windows 所有版本

据国外媒体报道，近日，一名安全研究人员对外发布了一个未修复的 Windows 安全漏洞的概念型验证代码，并表示这个漏洞可能会对所有版本的 Windows 操作系统产生影响。微软表示，从理论上讲，用户通过这个漏洞执行远程代码攻击是可能的。微软的发言人 Mark Wodrich 表示，这个漏洞存在于 BROWSER 协议中，尽管所有的 Windows 版本都会受到这个漏洞的影响，但是它对于作为主域控制器（PDC）运行的服务器操作系统的影响会更大一些。目前最佳的解决方案就是将 BROWSER 协议局限于边缘防火墙，尽管当地网络中也存在一些攻击。这个已知的 Windows 漏洞是一个缓冲器溢出漏洞，一个畸形的 BROWSER 信息将会导致主浏览器击中一部分的漏洞代码去触发这个漏洞。目前，微软还没有针对这个漏洞发布正式的解决方案。

参考链接：http://xiazai.zol.com.cn/article_topic/217/2171748.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