

信息安全漏洞周报

2011 年 1 月 17 日-2011 年 1 月 23 日

2011 年第 3 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低。

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 25 个、中危漏洞 35 个、低危漏洞 52 个。上述漏洞中，可利用来实施远程攻击的漏洞有 87 个。经跟踪发现，网上已经出现针对“Kingsoft Antivirus 'KisKrn1.sys' 驱动拒绝服务漏洞”、“PHP-fusion Team Structure Infusion SQL 注入漏洞”、“Linux 内核'execve()'内存扩展"OOM-killer"本地拒绝服务漏洞”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 103 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、KingSoft 'KisKrn1.sys'驱动存在拒绝服务漏洞

金山毒霸是国内流行的反病毒应用软件。金山毒霸的 KisKrn1.sys 使用钩子函数(hook)调用了 KiFastCallEntry 入口，但是在处理用户数据堆栈时跳过了系统的 MmUserProbeAddress 地址判断函数直接去复制堆栈。本地攻击者可以利用漏洞使系统崩溃。经 CNVD 跟踪发现，互联网上已经出现针对这个漏洞的攻击代码。目前，金山公司已经发布了补丁程序修复这个漏洞，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-2011-03766>

2、Oracle 发布公告修复多个安全漏洞

本周，Oracle 发布 2011 年第一个安全更新公告，修复了包括 Oracle 数据库、Fusion Middleware、Enterprise Manager Suite、E-Business Suite、PeopleSoft、Oracle Sun Products Suite 等多个产品存在的 66 个安全漏洞。CNVD 收录的漏洞主要包括：Oracle Database "Database Vault"组件存在未明漏洞（CVE-2010-4423）、Oracle Database "Scheduler Agent"组件存在未明漏洞、Oracle Database "Oracle Spatial"组件存在未明漏洞、Oracle Database "Database Vault"

组件存在未明漏洞（CVE-2010-4413）、Oracle Database "Cluster Verify Utility"组件存在未明漏洞、Oracle Database 企业管理网格控件存在输入验证漏洞、Oracle Beehive JSP 代码执行漏洞、Oracle WebLogic server "Servlet Container"组件存在漏洞、Oracle WebLogic server "Node Manager"组件存在漏洞、Oracle PeopleSoft Enterprise "Portal"组件存在漏洞等。攻击者在拥有一定的操作系统或数据库软件权限或在可以访问特定的数据库软件程序的情况下，能发起远程攻击，可导致拒绝服务，严重的甚至能获得数据库的管理控制权限。CNVD 提醒广大用户尽快下载安装补丁，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-2011-03852>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03851>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03850>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03849>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03848>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03847>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03846>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03835>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03833>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03818>

3、MySQL 存在多个安全漏洞

MySQL 是一个小型关系型数据库管理系统。本周，MySQL 出现了多个拒绝服务漏洞，攻击者可以利用漏洞实施拒绝服务攻击。CNVD 收录的漏洞包括：MySQL 拒绝服务漏洞（CVE-2010-3840、CVE-2010-3839、CVE-2010-3838、CVE-2010-3837、CVE-2010-3836、CVE-2010-3834、CVE-2010-3840、CVE-2010-3833）。目前，厂商已经发布了补丁程序修复这些漏洞，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-2011-03786>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03785>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03784>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03783>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03782>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03781>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03780>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03779>

4、IBM 多款产品出现安全漏洞

本周，IBM 的产品 AIX、WebSphere MQ、IBM Tivoli Access Manager for e-business、WebSphere Application Server 均出现了安全漏洞。攻击者可以利用漏洞在受影响的应用程序中运行任意代码或进行拒绝服务攻击。CNVD 收录的 IBM 漏洞包括：IBM AIX 'FC SCSI'协议驱动拒绝服务漏洞、IBM WebSphere MQ 头字段远程缓冲区溢出漏洞、IBM Ti

voli Access Manager for e-business 未明目录遍历漏洞、IBM WebSphere Application Server 管理控制台 servlets 访问控制漏洞、IBM WebSphere Application Server 跨站脚本漏洞。目前，IBM 已经发布了补丁修复了这些漏洞，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-2011-03862>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03798>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03773>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03765>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03764>

5、Sybase EAServer 存在多个安全漏洞

Sybase EAServer 是一款应用服务器，适用于多层架构的电子门户和互联商务解决方案。本周，Sybase EAServer 出现两个安全等级为“高”的漏洞。CNVD 收录的漏洞包括：Sybase EAServer 体系设计漏洞、Sybase EAServer 条件过滤漏洞。攻击者可以利用漏洞实施执行任意代码攻击或读取本地系统中的任意文件。目前，厂商已发布了补丁修复了这两个漏洞，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-2011-03760>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03759>

小结：本周，金山毒霸 "KisKrn1.sys" 驱动出现拒绝服务漏洞，本地攻击者可以利用这个漏洞发起恶意攻击，使用户系统崩溃。Oracle 发布 2011 年最新安全公告修复的 Oracle 数据库、Fusion Middleware、Enterprise Manager Suite、E-Business Suite、People Soft、Oracle Sun Products Suite 等多个产品存在的安全漏洞，以及 MySQL、Sybase EAServer 和 IBM 产品出现的安全漏洞，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、Oracle 发布升级程序,修补了 Sun 产品套件等的多个安全漏洞

本周，Oracle 发布了 2011 年的安全更新，修复 Oracle 产品的多个漏洞，其中包含了 Sun 产品套件的多个漏洞，避免攻击者利用这些漏洞提升特权、进行拒绝服务攻击或者获取敏感信息。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/2668>
<http://www.cnvd.org.cn/patch/2671>
<http://www.cnvd.org.cn/patch/2676>

<http://www.cnvd.org.cn/patch/2678>

<http://www.cnvd.org.cn/patch/2685>



本周要闻速递

1. 苹果在线应用商店存在安全漏洞

2011 年 1 月 21 日消息，据国外媒体报道，不久之前苹果应用商店(Mac App Shop)开张仅一天，就已经步入了网络黑客的视线。很多用户纷纷反映发现了 Mac App Shop 的安全漏洞，其中一个漏洞就会影响到包括目前最流行的游戏《愤怒的小鸟(Angry Birds)》在内的多个应用程序。利用该漏洞可以对程序进行简单复制，并将付费程序的购买代码发布使得其可以被免费使用。另一个黑客组织表示已经开发了一款名为“Kickback”的程序，该程序可轻松击破 App Store 出售的任意一款软件的保护。也就是说，一旦这款程序被传播开来，App Store 内超过 1000 余款程序都有被非法复制或免费共享的可能。苹果系统的应用十分丰富，但其安全隐患也逐渐增多，安全专家提示广大用户务必提高安全意识，养成良好的上网习惯，在下载、接收、存储陌生文件时最好安装一款适合 Mac 系统的专业安全软件，以确保系统足够安全。

参考链接：<http://tech.hexun.com/2011-01-21/126944064.html>

2. 黑客公布 Windows 新补丁攻击代码

2011 年 1 月 20 日消息，据国外媒体报道，在去年 Pwn2Own 黑客大赛上发现的漏微软件操作系统漏洞，在 9 个月后终于得到了修补。但是短短一天过后，就有研究者公布了新的 Windows 补丁的攻击代码。这个被微软定义为最高危险等级“危急”的漏洞早在 9 个月前的黑客大赛上就发现了，当时它被其发现者用于强强联手攻击 Internet Explorer 8，并为其赢得了 10000 美元的奖金。Vreugdenhil 在去年的 Pwn2Own 上只用了 2 分钟就攻击了 IE 8，被称为“技术上令人印象深刻的”。Vreugdenhil 指出，这个攻击代码并不适用于实施犯罪的人，单单运行该开发程序不会起作用，不过会使得 IE 瘫痪。

参考链接：http://news.ccidnet.com/art/11099/20110120/2298945_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