

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**高**。

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 101 个，其中高危漏洞 59 个、中危漏洞 31 个、低危漏洞 11 个。上述漏洞中，可利用来实施远程攻击的漏洞有 89 个。网上已经出现针对“Microsoft Host Integration Server 存在多个拒绝服务漏洞”、“MIT Kerberos kadmind 版本字符串处理远程拒绝服务漏洞”、“Winamp 'm3u8'文件远程缓冲区溢出漏洞”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。本周收录的漏洞中，已有 78 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。

成员单位上报漏洞统计

本周，共有 6 家成员单位报送了本周收录的全部 101 个漏洞，各单位报送情况如表 1 所示。其中，启明星辰报送数量较多。

成员单位	漏洞上报总数	私有漏洞数量
启明星辰	100	0
绿盟科技	5	0
东软	5	0
安氏领信	1	0
安天	1	0
恒安嘉新	1	0
总计	101（去重）	0

表 1 成员单位上报漏洞统计表

本周，CNVD 整理和发布的漏洞涉及 Microsoft、Computer Associates、HP、Linux、SAP、Google 等多家厂商的产品，漏洞数量按厂商统计如表 2 所示。

序号	厂商（产品）	漏洞数量	所占比例
1	Microsoft	37	36.63%
2	Computer Associates	8	7.92%
3	HP	4	3.96%
4	Linux	4	3.96%
5	SAP	4	3.96%
6	Google	3	2.97%
7	NullSoft	2	1.98%
8	Fiberhome	2	1.98%
9	Novell	1	0.99%
10	其他	36	35.65%

表 2 漏洞产品涉及厂商分类统计

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、Microsoft 发布安全公告，修复多个产品安全漏洞

本周，微软发布了 2011 年 4 月份的月度例行安全公告，共包含 17 项安全更新，其中 9 项更新的综合评级为“严重”，其余 8 项更新的综合评级为“重要”。本次发布的安全更新修复了包含 Windows 操作系统、Office 软件、IE 浏览器、服务器软件、开发工具等产品的多个安全漏洞。攻击者可以利用这些漏洞发起攻击，攻击一旦成功则可在受害主机上执行任意代码，窃取敏感信息或提升特权。CNVD 收录的相关漏洞包括：Microsoft Excel 整数下溢漏洞、Microsoft Excel 缓冲区溢出漏洞（CVE-2011-0098、CVE-2011-0104、CVE-2011-0105）、Microsoft Excel 任意代码执行漏洞（CVE-2011-0101、CVE-2011-0978、CVE-2011-0979）、Microsoft Excel 内存破坏漏洞（CVE-2011-0103）、Microsoft Windows/Office GD I+整数溢出漏洞、Microsoft HTML Help '.chm'文件栈缓冲区溢出漏洞、Microsoft Internet Explorer 绕过域限制漏洞、Microsoft Internet Explorer 处理帧标签对象存在安全漏洞等。CNVD 提醒广大 Microsoft 用户及时下载补丁程序进行修补。除上述公告提到的漏洞外，Microsoft Host Integration Server 被披露存在多个拒绝服务漏洞。Microsoft Host Integration Server 是一款主机平台互连互通解决方案。攻击者可以利用漏洞发起拒绝服务攻击，导致服务异常终止，该漏洞的综合评级为“高危”。目前，互联网上已经出现该漏洞的攻击代码，且微软尚未发布其补丁程序，CNVD 建议用户及时关注厂商主页，以获取补丁程序或最新

版本。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2011-05003>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05004>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05005>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05006>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05007>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05008>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05009>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05010>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05012>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05013>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05014>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05015>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04979>

2、Computer Associates Total Defense 安全漏洞

Computer Associates Total Defense 是由 CA 公司提供用于防范常见网络攻击的安全软件。本周, Computer Associates Total Defense 出现了一个远程代码执行漏洞和多个 SQL 注入漏洞。远程攻击者可以利用漏洞操作数据库或以数据库上下文执行任意代码。CNVD 收录的相关漏洞包括: Computer Associates Total Defense \UNCSW\服务远程代码执行漏洞、Computer Associates Total Defense 中 UnAssignFunctionalUsers 存储过程安全漏洞、Computer Associates Total Defense 中 RegenerateReport 存储过程安全漏洞、Computer Associates Total Defense 中 UnassignAdminRoles 存储过程安全漏洞、Computer Associates Total Defense 中 DeleteFilter 存储过程安全漏洞、Computer Associates Total Defense 中 NonAssignedUserList 存储过程安全漏洞、Computer Associates Total Defense 中 DeleteReportLayout 存储过程安全漏洞、Computer Associates Total Defense 中 DeleteReports 存储过程安全漏洞。上述漏洞的综合评级均为“高危”。厂商已经发布这些漏洞的补丁程序, CNVD 提醒相关用户及时获取补丁程序进行修补。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2011-05037>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05038>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05039>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05040>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05041>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05043>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05044>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05045>

3、Adobe Flash Player 'SWF'文件远程内存破坏漏洞

本周，HP 的产品 Photosmart 打印机和 HP-UX 操作系统存在多个安全漏洞。CNVD 收录的相关漏洞包括：HP Photosmart 打印机敏感信息泄露漏洞（CVE-2011-1531）、HP Photosmart 打印机 webscan 组件信息泄露漏洞（CVE-2011-1532）、HP Photosmart 打印机 SNMP 组件信息泄露漏洞（CVE-2011-1533）、HP-UX 未明远程拒绝服务漏洞。攻击者可以利用漏洞发起跨站脚本或拒绝服务攻击，获得敏感信息或劫持目标用户会话。目前，HP 已经发布了补丁程序，CNVD 提醒广大用户及时下载修复。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04993>

4、HP 产品安全漏洞

本周，HP 的产品 Photosmart 打印机和 HP-UX 操作系统存在多个安全漏洞。CNVD 收录的相关漏洞包括：HP Photosmart 打印机敏感信息泄露漏洞（CVE-2011-1531）、HP Photosmart 打印机 webscan 组件信息泄露漏洞（CVE-2011-1532）、HP Photosmart 打印机 SNMP 组件信息泄露漏洞（CVE-2011-1533）、HP-UX 未明远程拒绝服务漏洞。攻击者可以利用漏洞发起跨站脚本或拒绝服务攻击，获得敏感信息或劫持目标用户会话。目前，HP 已经发布了补丁程序，CNVD 提醒广大用户及时下载修复。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04995>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04996>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04997>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04998>

5、NullSoft Winamp 缓冲区溢出漏洞

Winamp 是一款流行的媒体播放器程序。本周，Winamp 出现了两个综合评级为“高危”的缓冲区溢出漏洞，远程攻击者可以利用漏洞在受影响的程序中执行任意代码。CNVD 收录的漏洞包括：Winamp '.wlz'文件远程缓冲区溢出漏洞、Winamp '.m3u8'文件远程缓冲区溢出漏洞。目前，互联网上已经出现针对这两个漏洞的攻击代码，主要影响 NullSoft Winamp 5.6.1 版本。厂商尚未发布这两个漏洞的补丁，CNVD 建议用户及时关注厂商主页，以获取补丁程序或最新版本。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05035>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05036>

小结：本周，Microsoft 发布安全公告，修复了包含 Windows 操作系统，Office 软件，IE 浏览器，服务器软件，开发工具等产品存在的多个安全漏洞。攻击者可以利用这些漏洞发起攻击，攻击一旦成功则可在受害主机上执行任意代码，窃取敏感信息或提升特权，对广大微软用户构成较严重威胁。Computer Associates Total Defense 出现多个高危安全漏洞，允许攻击者利用漏洞操作数据库或以数据库上下文执行任意代码。此外，Adobe 应用产品、HP 应用产品和 Winamp 播放器也出现了多个安全漏洞，一些漏洞的攻击代码也随即在互联网上公开，对使用上述产品

的用户构成较大威胁。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、Linux 发布升级程序，修补 Kernel 多个安全漏洞

本周，Linux 发布升级程序，修补了 Linux Kernel（内核）存在的多个安全漏洞。攻击者利用漏洞可以发起拒绝服务攻击，使内核崩溃。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/3496>

<http://www.cnvd.org.cn/patch/3481>

<http://www.cnvd.org.cn/patch/3482>

本周要闻速递

1. 甲骨文 19 日推出重要安全补丁

4 月 17 日消息，据国外媒体报道，甲骨文提前宣布将于下周二（19 日）推出 4 月重要安全补丁更新，解决 25 种产品的 73 个安全问题。涉及的产品有甲骨文数据库 11g，Fusion 中间件，应用程序服务器和 People Enterprise 平台等。甲骨文数据库服务器这次会进行 6 个漏洞的更新，其中 2 个可能导致黑客无需使用用户名登录，就可以对数据进行远程控制。Fusion 中间件更新包含了 9 个补丁，其中 6 个也可以被黑客用于远程控制。Sun 产品此次共计更新 18 个漏洞，甲骨文表示其中 7 个都是涉及远程控制的。甲骨文此次更新的推出可谓是迎合了最近安全更新的大趋势，微软日前刚刚推出了多个漏洞的补丁。苹果 iOS、Safari 和 MacOS X 也推出了更新包，Adobe 即将推出针对 Flash Player 的漏洞更新。

参考链接：http://news.ccidnet.com/art/1032/20110417/2365155_1.html

2. 苹果公司推出 iOS 系统最新版

苹果公司于北京时间 2011 年 4 月 15 日，正式推出 iOS 系统的最新版 iOS 4.3.2，用户可以将自己的 iOS 设备通过 iTunes 进行升级。iOS 4.3.2 修复了 3G 连接、Facetime 等功能中的问题。iOS 4.3.2 适用于 iPhone 3GS、iPhone 4、iPod Touch 3 和 4、iPad 以及 iPad 2。苹果公司放出 iOS 4.3.2 升级仅几个小时，即有黑客放出了 iOS 4.3.2 的越狱方法。黑客针对 iPhone 采用的越狱工具是 Redsn0w 0.9.6，针对 iPod Touch 和 iPad 则是使用的 PwnageTool，适用于 Windows 和 Mac 平台。

参考链接：<http://www.hackbase.com/news/2011-04-15/54742.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