

信息安全漏洞周报

2011年3月28日-2011年4月3日

会员版

2011年第13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 67 个，其中高危漏洞 13 个、中危漏洞 24 个、低危漏洞 30 个。上述漏洞中，可利用来实施远程攻击的漏洞有 58 个。网上已经出现针对“RealPlayer '.rmp'文件远程缓冲区溢出漏洞”和“Microsoft Windows Media Player '.ape'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 33 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 7 家成员单位报送了本周收录的全部 67 个漏洞，各单位报送情况如表 1 所示。其中，启明星辰、恒安嘉新报送数量较多；安氏领信公司自主发现并及时报送了一款国产网络设备的“无线控制器绕过验证下载配置文件漏洞”（CNVD-2011-04873），目前该漏洞正按 CNVD 漏洞处理流程进行处置，漏洞详情拟于 4 月 10 日正式公布。

成员单位	漏洞上报总数	私有漏洞数量
启明星辰	44	0
绿盟科技	6	0
安氏领信	1	1
东软	4	0
安天科技	1	0
恒安嘉新	20	0
知道创宇	1	0
总计	67（去重）	1

表 1 成员单位上报漏洞统计表

本周，CNVD 整理和发布了 IBM、HP、Real Networks、Cisco 等多家厂商的产品漏洞，按厂商统计如表 2 所示。

序号	厂商	漏洞数量	所占比例
1	IBM	8	12%
2	HP	4	6%
3	Real Networks	4	6%
4	Cisco	2	3%
5	Feng Office	2	3%
6	Mahara	2	3%
7	Google	1	1.5%
8	Microsoft	1	1.5%
9	其他	43	64%

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、域名系统软件 BIND 9 存在递归服务器对 .com 域名解析异常的漏洞

Bind 9 是一款应用广泛的域名解析服务器软件,本周 BIND 9.6-ESV-R3 及之前版本被曝存在漏洞。该漏洞在根分区发布.com 的 DS 记录后，将对递归服务器.com 域名的普通查询（非 DNSSEC，即查询的 CD 位=0）产生影响，查询结果可能返回 SERVFAIL 应答，相关测试结果显示，出现错误的比率约为 50%，但该漏洞对.com 域名的 DNSSEC 查询（即查询的 CD 位=1）没有影响。由于大多数 DNS 查询为非 DNSSEC 查询，因此该漏洞可能对国内使用 BIND 软件提供的递归解析服务造成较严重影响。CNVD 建议受漏洞影响的 BIND 用户采取以下防范措施：(1)升级 BIND 软件至不受漏洞影响的版本；(2)如果软件没有升级且服务已受到漏洞影响，建议执行命令“rndc flushname com”或者重启服务器解决。

参考链接：<http://www.cnvd.org.cn/notifications/146>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04890>

2、Microsoft Windows Media Player '.ape'文件远程缓冲区溢出漏洞

Microsoft Windows Media Player 是一款微软开发的媒体播放程序。本周，Microsoft Windows Media Player 被披露存在一个综合评级为“高危”的缓冲区溢出漏洞。Windows Media Player 未能正确解析'.ape'文件，远程攻击者可以构建相同后缀名的内嵌恶意代码的文

件，诱使用户解析，触发缓冲区溢出。成功利用漏洞后可以受影响程序的权限执行任意代码。目前，互联网上已经出现了针对该漏洞的攻击代码，影响 Windows Media Player11 版本。微软尚未发布该漏洞的补丁程序，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-2011-04846>

3、IBM 多个产品存在安全漏洞

本周，IBM 的 WEBi 软件、SolidDB 数据库、AIX 操作系统等多款产品被曝出多个安全漏洞。IBM WEBi 是一款用于内容管理的软件；IBM SolidDB 是一款内存型数据库系统；IBM AIX 是一款商用操作系统。CNVD 收录的相关漏洞包括：IBM WebSphere Application Server for z/OS 本地未授权访问漏洞、IBM WEBi 未明漏洞、IBM WEBi 跨站脚本攻击漏洞、IBM solidDB solid.exe 验证绕过远程代码执行漏洞、IBM AIX LDAP 登录未授权访问漏洞、IBM Tivoli Directory Server TDS 代理服务器安全漏洞、IBM Tivoli Directory 远程代码执行漏洞、IBM Rational Licensing 本地特权提升漏洞。攻击者可以利用这些漏洞获得敏感信息、劫持目标用户会话、提升特权或进行未授权操作。其中，“IBM solidDB solid.exe 验证绕过远程代码执行漏洞”的综合评级为“高危”。目前，厂商已经发布了上述漏洞的补丁程序，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-2011-04900>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04899>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04898>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04897>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04896>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04895>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04894>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04868>

4、Google Picasa 存在装载文件库漏洞

Picasa 是一款 Google 推出的免费图片管理工具。本周，Google Picasa 出现了一个装载文件库漏洞。Picasa 在装载文件库时未进行安全检查，攻击者可以通过远程 WebDAV 或 SMB 共享构建内嵌恶意代码的库文件，诱使用户通过"Locate on Disk"功能访问，进而执行恶意代码。此漏洞的综合评级为“高危”。目前，Google 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修复。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2011-04840>

5、RealNetworks 产品安全漏洞

本周，RealNetworks 的产品 RealPlayer 和 Helix Server 均曝出安全漏洞。RealPlayer 是一款流行的媒体播放程序；Helix Server 是一款支持多格式、跨平台的流媒体服务器软件。CNVD 收录的相关漏洞包括：RealPlayer '.avi'文件远程缓冲区溢出漏洞、Helix 和 Helix Mobile Server 'RTSP'栈缓冲区溢出漏洞、Helix Server 'x-wap-profile'文件头远程代码执行漏洞、

RealPlayer '.rmp'文件远程缓冲区溢出漏洞。攻击者可以利用这些漏洞在受影响的程序中执行任意代码。目前，互联网上已经出现针对 RealPlayer 缓冲区溢出漏洞的攻击代码，主要影响 Real Networks RealPlayer 11 和 14.0.2 633 版本。厂商尚未发布这两个漏洞的补丁，但已经发布了 Helix Server 产品漏洞的升级程序，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-2011-04906>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04880>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04879>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04847>

小结：本周漏洞中，BIND 9 漏洞影响递归服务器对.com 域名的普通查询，对相关基础电信运营企业和域名服务机构的递归解析服务器构成较大威胁。Microsoft Windows Media Player 缓冲区溢出漏洞、Google Picasa 库装载漏洞会导致在受影响的程序中执行任意代码。此外，IBM 产品和 RealNetworks 产品均出现了多个安全漏洞。上述漏洞若未能及时修补，会对互联网网络安全及用户个人信息安全构成威胁，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、HP 发布升级程序，修补多个产品安全漏洞

本周，HP 发布升级程序，修补了 HP Operations 软件和 HP-UX 操作系统等多个产品的安全漏洞，避免攻击者利用漏洞获得敏感信息、发起拒绝服务攻击或进行未授权操作。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/3406>
<http://www.cnvd.org.cn/patch/3425>
<http://www.cnvd.org.cn/patch/3426>
<http://www.cnvd.org.cn/patch/3427>

本周要闻速递

1. 微软高危长老漏洞补丁被攻破，影响 Windows 主流操作系统

2011 年 3 月 24 日消息，国内知名安全厂商发出互联网高危预警，微软一个存在 18 年长老漏洞的补丁程序(MS11-011)宣告失效，即便打了微软官方补丁，黑客也可利用该漏洞可轻松获得系统控制权。该漏洞几乎影响目前主流 Windows 操作系统，如果用户不及时防

范将有可能引发互联网上大规模的攻击潮。安全专家警告说，该漏洞影响目前主流的 Windows2000、WindowsXP、Windows Vista 以及 Windows 7 等在内的操作系统，超过九成电脑用户都受到影响。尽管上个月微软刚刚发布的 MS11-011 补丁程序对此漏洞进行修补，但这次修复并不彻底，短短一个月后就有安全软件爱好者攻破补丁程序，利用这些代码可以巧妙绕过安全漏洞补丁程序的限制，攻击程序可以轻松获得对系统的完全控制权，更甚的是攻击程序还可以绕过多数杀毒软件的主动防御系统。据专家介绍，如果黑客获得了系统的完全控制权，将使得系统本身的一切防护都将失效，“用户的家里已经门户大开，安装再多的防盗门黑客也能来去自如。”安全专家说，利用这个漏洞，黑客可以在用户的电脑中为所欲为。

参考链接：http://security.zdnet.com.cn/security_zone/2011/0402/2027951.shtml

2. 黑客组织发现 McAfee 网页存安全漏洞，McAfee 表示不影响客户安全性

北京时间 3 月 30 日消息，据国外媒体报道，安全厂商 McAfee 已经证实其网站网页上存在一些安全漏洞，但保证那些问题不会影响到客户的安全性。“正义黑客组织”YGN 表示，它在 McAfee 的网页上发现了许多问题，其中包括一些可能导致跨网站脚本攻击和信息泄露的安全漏洞。然而，McAfee 对于有关报道的反应比较低调，只是表示公司正在解决那些问题，同时承诺那些问题不会对客户安全构成威胁。

参考链接：http://www.chinadaily.com.cn/micro-reading/tech/2011-03-30/content_2168258.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