

信息安全漏洞周报

2011 年 5 月 9 日-2011 年 5 月 15 日

2011 年第 19 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**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 58 个、中危漏洞 35 个、低危漏洞 8 个。上述漏洞中，可利用来实施远程攻击的漏洞有 84 个。网上已经出现针对“Symantec Backup Exec System Recovery 'GEARAspiWDM.sys'拒绝服务漏洞、Nagios XI 'reset_configs-perms.c'本地特权提升漏洞、ChasysChasys Media Player 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 68 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。

成员单位报送漏洞统计

本周，共有 6 家成员单位和 1 位个人上报者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、恒安嘉新、东软、绿盟科技报送的数量较多。

报送单位或个人	漏洞报送数量	私有漏洞数量
启明星辰	77	0
绿盟科技	7	0
恒安嘉新	23	0
东软	11	0
安氏领信	1	0
安天	1	0
个人报告者	1	1
总计	101（去重）	1

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 Adobe、HP、Linux、Microsoft、Oracle 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	Adobe	15	14.7%
2	HP	10	9.8%
3	Linux	9	8.8%
4	Inventive Technology	6	5.9%
5	Microsoft	3	2.9%
6	Joomla	2	1.9%
7	Citrix	2	1.9%
8	Apache	2	1.9%
9	Oracle	1	1.0%
10	其他	52	51.2%

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 5 月份的月度例行安全公告，共包含 2 项安全更新。其中，1 项更新的综合评级为“严重”，此项更新修复了 Windows Internet Name Service (WINS) 存在的一个安全漏洞，受影响的操作系统平台包括：Windows Sever 2008 和 2003。另外 1 项更新的综合评级为“重要”，修复了 Office 软件 PowerPoint 中存在的两个安全漏洞，受影响的软件包括 Office XP、2003、2007 以及 Mac 平台下 Office 2004 和 2008。本次修复的 3 个漏洞均为秘密报告的漏洞，攻击者可以利用这些漏洞远程执行任意代码。CNVD 收录的漏洞包括：Microsoft PowerPoint 远程代码执行漏洞(CVE-2011-1269、CVE-2011-1270)、Microsoft Windows Internet Name Service (WINS)失败响应远程代码执行漏洞。CNVD 提醒广大 Microsoft 用户尽快下载补丁更新，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-2011-05403>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05401>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05397>

2、HP 产品安全漏洞

HP Intelligent Management Center 是一款惠普公司发行的智能管理应用程序；HP web

OS 是用于平板电脑的操作系统。本周，上述产品出现了多个安全漏洞。攻击者可以利用漏洞以 SYSTEM 用户上下文远程执行任意代码或窃取敏感信息。CNVD 收录的相关漏洞包括：HP Intelligent Management Center 远程代码执行漏洞(CVE-2011-1851、CVE-2011-1848、CVE-2011-1849、CVE-2011-1850、CVE-2011-1852、CVE-2011-1853、CVE-2011-1854)、HP WebOS Email 应用程序 HTML 注入漏洞、HP WebOS 插件开发工具(PDK)远程脚本代码注入漏洞。CNVD 对上述漏洞的综合评级为“高危”，且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-2011-05392>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05391>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05390>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05388>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05387>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05387>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05393>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05386>

3、Adobe 产品安全漏洞

本周，Adobe 在其官网发布 4 项安全公告，修复了 Flash Player、Flash Media Server、Audition 和 RoboHelp/ RoboHelp Server 存在多个安全漏洞。攻击者可以利用漏洞发起拒绝服务攻击、远程执行任意代码或窃取敏感信息。CNVD 收录的漏洞包括：Adobe Flash Player 内存破坏漏洞(CVE-2011-0627、CVE-2011-0622、CVE-2011-0621)、Adobe Flash Player 任意代码执行漏洞(CVE-2011-0626、CVE-2011-0625、CVE-2011-0624、CVE-2011-0623)、Adobe Flash Player 整数溢出漏洞(CVE-2011-0618)、Adobe Flash Player 信息泄露漏洞(CVE-2011-0579)、Adobe RoboHelp Server 和 RoboHelp 跨站脚本漏洞、Adobe Audition '.ses' 缓冲区溢出漏洞(CVE-2011-0615)、Adobe Flash Media Server XML 数据远程拒绝服务漏洞等。除“Adobe RoboHelp Server 和 RoboHelp 跨站脚本漏洞”的综合评级为“中危”外，其余漏洞的综合评级均为“高危”。CNVD 提醒广大 Adobe 用户尽快下载补丁更新，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-2011-05455>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05449>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05447>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05446>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05445>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05454>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05452>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05451>

4、Linux Kernel 安全漏洞

Linux 是一款开源的操作系统。本周，Linux 内核出现多个安全漏洞，攻击者通可以利用漏洞发起拒绝服务攻击、获得敏感信息或绕过安全限制执行未授权操作。CNVD 收录的相关漏洞包括：Linux Kernel 'net/can/raw.c'本地拒绝服务漏洞、Linux Kernel 'AGPIOC_SERVE'和'AGPIOC_ALLOCATE' IOCTL'本地拒绝服务漏洞、Linux Kernel EFI 分区缓冲区溢出漏洞、Linux Kernel 蓝牙"rfcomm_sock_getsockopt_old()"函数信息泄露漏洞、Linux Kernel DCCP 选项长度远程拒绝服务漏洞、Linux Kernel CIFS 'O_DIRECT'空指针引用本地拒绝服务漏洞、Linux Kernel 蓝牙"l2cap_sock_getsockopt_old()"函数信息泄露漏洞、Linux Kernel '/proc/[pid]/stat'本地信息泄露漏洞、Linux Kernel 'CAP_NET_ADMIN'未授权访问漏洞。除 Linux Kernel 蓝牙"rfcomm_sock_getsockopt_old()"函数信息泄露漏洞、Linux Kernel 蓝牙"l2cap_sock_getsockopt_old()"函数信息泄露漏洞、Linux Kernel DCCP 选项长度远程拒绝服务漏洞、Linux Kernel CIFS 'O_DIRECT'空指针引用本地拒绝服务漏洞尚未发布补丁程序外，其余漏洞均已发布官方补丁。CNVD 提醒广大用户尽快下载补丁更新，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-2011-05461>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05415>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05366>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05365>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05426>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05413>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05396>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05395>

5、Symantec Backup Exec System Recovery 'GEARAspiWDM.sys'拒绝服务漏洞

Symantec Backup Exec System Recovery 是一款中小型企业经济型备份和恢复解决方案。Symantec Backup Exec System Recovery 中的 GEARAspiWDM.sys 驱动没有正确检查 IOCTL 的输入，攻击者只需修改输入参数的一个字节便可引发异常，进而利用该漏洞发起拒绝服务攻击。目前，互联网上已经出现该漏洞的攻击代码，主要影响 Symantec Backup Exec System Recovery 8.5 版本。目前厂商尚未发布漏洞的补丁程序，CNVD 提醒广大用户随时关注厂商主页获取最新版本。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-05464>

小结：本周，微软发布了 2011 年 5 月份的月度例行安全公告，修复了 Windows Internet Name Service (WINS) 和 Office 软件 PowerPoint 中存在的三个安全漏洞，攻击者可以利用这些漏洞远程执行任意代码，对广大 Microsoft 用户构成较为严重的威胁。Adobe 也在其官网发布 4 项安全公告，修复了 Flash Player、Flash Media Server、Audition 和 RoboHel

p/ RoboHelp Server 存在多个安全漏洞。HP 产品和 Linux Kernel 均出现了多个安全漏洞。此外, Symantec Backup Exec System Recovery 出现了一个拒绝服务漏洞, 且互联网上已经出现该漏洞的攻击代码, 主要影响 Symantec Backup Exec System Recovery 8.5 版本, 对使用该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、Google 发布升级程序, 修补 Chrome 多个安全漏洞

Google Chrome 是一款流行的 WEB 浏览器。本周, Google 发布升级程序, 修补了 Chrome 存在的多个安全漏洞。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 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/3866>

<http://www.cnvd.org.cn/patch/3867>

本周要闻速递

1. 火狐浏览器曝高危零日漏洞 影响中国版本用户

近日, 火狐浏览器的“火狐魔镜”插件出现一个高危 0day 漏洞, 影响几乎所有火狐中国版浏览器用户。据悉, “火狐魔镜”是一款被火狐中国版浏览器默认捆绑安装的应用插件。该功能本来主要用于拖拽网页中的文字来获取搜索结果, 现在却可能把木马直接“拖”入电脑。在某些技术论坛上, 已有黑客公开了火狐“魔镜”漏洞的攻击方法, 火狐浏览器用户因此面临严峻的安全威胁。安全专家介绍说, 黑客利用火狐“魔镜”漏洞发起攻击的方式是在网页面上挂马。一旦火狐浏览器的用户在此类网页上拖拽文字, 就会使恶意代码注入到“火狐魔镜”中, 导致浏览器插件接口被黑客利用, 使木马自动进入用户电脑。目前, “魔镜”漏洞的技术细节已经通报给火狐软件商。专家建议: 在“魔镜”漏洞得到修复前, 火狐浏览器用户应尽量访问大型知名网站, 避免点击来源可疑的网址链接, 可以降低被木马攻击的风险; 或暂时卸载“火狐魔镜”插件, 待漏洞修复后再重新安装。

参考链接: <http://www.7747.net/News/201105/90476.html>

2. 索尼网络系统仍存在大量安全漏洞

5 月 14 日消息, 据国外媒体报道, 互联网安全专家约翰·布姆加纳(John Bumgarner)日前表示, 在索尼 PSN 网络受到黑客攻击, 导致大量用户数据被泄露之后, 索尼计算机网络系统仍然存在大量安全漏洞, 依然容易受到攻击。安全专家布姆加纳日前通过互联网对索尼网络系统进行了远程研究, 在研究中发现, 索尼网络系统中仍存在大量安全漏洞, 黑客们

只需要使用网络浏览器和谷歌搜索引擎，并对互联网安全系统有基本的了解，就能利用潜在的机会。布姆加纳表示：“索尼仍然有数个外部安全问题需要解决。”

参考链接：<http://news.yesky.com/176/30093176.shtml>

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