

信息安全漏洞周报

2011 年 8 月 8 日-2011 年 8 月 14 日

2011年第32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 121 个，其中高危漏洞 31 个、中危漏洞 88 个、低危漏洞 2 个。上述漏洞中，可利用来实施远程攻击的漏洞有 108 个。网上已经出现针对“Apple iPhone/iPod 下的 Phone Drive 目录遍历漏洞”、“Mambo CMS 'zorder'参数 SQL 注入漏洞”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 91 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 4 家成员单位报送了本周收录的全部 121 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	106	0
恒安嘉新	19	0
东软	3	0
安氏领信	2	0
总计	121（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、Adobe、Linux、Mozilla、HP 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	24	19.8%
2	Adobe	23	19.0%
3	Linux	7	5.8%

4	Mozilla	7	5.8%
5	HP	5	4.1%
6	Novell	4	3.3%
7	Hesk	3	2.5%
8	Apple	2	1.7%
9	WordPress	2	1.7%
10	Symantec	2	1.7%
11	其它	42	34.6%

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、Adobe 产品安全漏洞

本周，Adobe 在官网发布安全公告，修复 Adobe Flash Player、Flash Media Server、Shockwave Player 等多个产品的安全漏洞。攻击者可以利用这些漏洞进行拒绝服务和执行任意代码等攻击，或获取敏感信息、劫持用户会话。CNVD 收录的漏洞包括：Adobe Photoshop '.GIF'文件远程内存破坏漏洞、Adobe Shockwave Player 内存破坏漏洞（CVE-2011-2423）、Adobe RoboHelp Server 和 RoboHelp 跨站脚本漏洞（CVE-2011-2133）、Adobe Flash Media server 内存破坏远程拒绝服务漏洞、Adobe Flash Player 跨站脚本漏洞（CVE-2011-2139）、Adobe Flash Player 远程整数溢出漏洞（CVE-2011-2416）、Adobe Flash Player 远程缓冲区溢出漏洞（CVE-2011-2130、CVE-2011-2134）等。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-2011-06778>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06776>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06760>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06758>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06756>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06754>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06753>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06752>

2、HP 产品安全漏洞

本周，HP 多款产品 webOS、OpenView Performance Insight 和 Easy Printer Care Software 被披露存在多个安全漏洞。攻击者可以利用这些漏洞执行任意代码，获得敏感

信息或劫持用户会话。CNVD 收录的漏洞包括：HP webOS 日历应用程序远程脚本代码注入漏洞、HP webOS 联系人应用程序远程脚本代码注入漏洞、HP OpenView Performance Insight 任意代码执行漏洞（CVE- 2011- 2406）、HP Easy Printer Care Software 'HPTicketMgr.dll' ActiveX 控件远程代码执行漏洞、HP OpenView Performance Insight 未授权访问漏洞（CVE- 2011 -2407）。上述漏洞中，“HP webOS 日历应用程序远程脚本代码注入漏洞”、“HP OpenView Performance Insight 任意代码执行漏洞（CVE- 2011 - 2406）”和“HP Easy Printer Care Software 'HPTicketMgr.dll' ActiveX 控件远程代码执行漏洞”的综合评级为“高危”。目前，厂商已经发布这些漏洞的补丁程序，CNVD 提醒广大 HP 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-2011-06746>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06749>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06767>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06770>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06771>

3、Linux Kernel eCryptfs 安全漏洞

eCryptfs 是 Linux 平台下的企业文件加密系统。本周，Linux Kernel eCryptfs 被披露存在多个安全漏洞。攻击者可以利用漏洞获得敏感信息、绕过安全限制、操作数据，或进行拒绝服务和特权提升攻击。CNVD 收录的漏洞包括：Linux Kernel eCryptfs 任意文件覆盖漏洞（CVE-2011-1837）、Linux Kernel eCryptfs 权限处理漏洞（CVE-2011-1836）、Linux Kernel eCryptfs 密钥处理漏洞（CVE-2011-1835）、Linux Kernel eCryptfs 安装点卸载漏洞（CVE-2011-1834）、Linux Kernel eCryptfs 任意目录安装漏洞（CVE-2011-1833）、Linux Kernel eCryptfs 安装点权限检查漏洞（CVE-2011-1832、CVE-2011-1831）。目前，厂商已经发布了补丁程序修复这些漏洞，CNVD 提醒相关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-2011-06764>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06763>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06762>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06761>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06759>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06757>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06755>

4、Microsoft 产品安全漏洞

本周，微软发布了 2011 年 8 月份的月度例行安全公告，包含 13 项安全更新，共修复 22 个漏洞。其中，2 项更新的综合评级为“严重”，9 项更新评级为“重要”，其余 2 项更新则为“中等”。此次更新修复了 Microsoft Windows、Internet Explorer、Office、.

NET Framework 等多个产品存在的安全漏洞。攻击者可以利用漏洞远程执行任意代码、提升特权、获取敏感信息或进行拒绝服务攻击。CNVD 收录的相关漏洞包括：Microsoft Visual Studio 报告查看器控件跨站脚本漏洞、Microsoft Internet Explorer 样式对象内存破坏远程代码执行漏洞、Microsoft Visio 远程代码执行漏洞（CVE-2011-1979）、Microsoft Remote Desktop Web Access 跨站脚本漏洞（CVE-2011-1263）、Microsoft Internet Explorer XSLT 内存破坏远程代码执行漏洞、Microsoft 远程桌面协议拒绝服务漏洞（CVE-2011-1968）、Microsoft Visio 远程代码执行漏洞、Microsoft .NET Framework 套接字限制绕过漏洞等。上述漏洞中，“Microsoft Internet Explorer 样式对象内存破坏远程代码执行漏洞”和“Microsoft Internet Explorer XSLT 内存破坏远程代码执行漏洞”的综合评级均为“高危”。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-2011-06735>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06734>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06733>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06732>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06731>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06730>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06729>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06728>

5、Apple iPhone/iPod 下的 Phone Drive 目录遍历漏洞

Phone Drive 可以把 iOS 设备变成具有分享功能的移动存储设备。本周，Phone Drive 被披露存在一个目录遍历漏洞。由于 Phone Drive 未能正确解析用户提交的包含“..%2f”目录遍历序列的字符，攻击者可以利用漏洞获取读取服务器 root 目录之外的任意文件。目前，互联网上已经出现针对该漏洞的攻击代码，主要影响 Phone Drive 1.1.1 版本。厂商尚未发布该漏洞的修补程序，CNVD 随时关注厂商主页以获取最新版本。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06777>

小结：本周，微软发布了 2011 年 8 月份的月度例行安全公告，修复了 Microsoft Windows、Internet Explorer、Office、.NET Framework 等多个产品存在的安全漏洞。攻击者可以利用漏洞远程执行任意代码、提升特权、获取敏感信息或进行拒绝服务攻击，对使用 Microsoft 产品的用户构成较为严重的威胁。同时，Adobe 和 HP 产品以及 Linux Kernel Cryptfs 也被披露存在多个安全漏洞。此外，Phone Drive 零日漏洞也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、Novell 发布升级程序，修补 Data Synchronizer Mobility Pack 安全漏洞

Novell Data Synchronizer Mobility Pack 是用于与移动设备进行应用程序数据同步的解决方案。本周，Novell 发布升级程序，修补了 Data Synchronizer Mobility Pack 存在的多个安全漏洞。攻击者可以利用漏洞获得敏感信息或者劫持用户会话。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/4669>

<http://www.cnvd.org.cn/patch/4670>

<http://www.cnvd.org.cn/patch/4671>

<http://www.cnvd.org.cn/patch/4673>



本周要闻速递

1.Google+的 Google Talk 功能中存在漏洞

据国外媒体报道，谷歌已经承认，Google+的 Google Talk 功能中存在一个漏洞，可能会让用户在某些情况下看到共享电脑上的其他用户的 IM 联系人清单和通话记录，甚至可能造成用户聊天被实时监听。谷歌表示，公司正在研究解决该问题的办法。据悉，这个漏洞还会影响到拥有多个谷歌帐户的用户，这说明 Google+也许需要通过某种方式来将用户的不同帐户链接起来。Google+为用户提供了一个 Google Talk 聊天功能，允许用户进行即时通讯。谷歌的 Gmail 中也整合了类似的功能。这些功能通常与谷歌的即时通讯服务联系在一起，也许这就是该漏洞的问题所在。

参考链接：http://news.ccidnet.com/art/1032/20110811/2516105_1.html

2. 安全专家称多个 Android 应用存在安全漏洞

移动安全专家莱利·哈塞尔(Riley Hassell)称，Android 系统中多个流行应用存在安全漏洞，极易遭受黑客攻击。哈塞尔本打算在上周举行的黑帽黑客大会上发布这些漏洞，但最终决定不公布，以免被犯罪分子利用。他表示，许多应用没有遵照安全指南编写代码，因此在面对外部攻击时非常脆弱，有些甚至使用短信即可入侵应用或手机。哈塞尔拒绝透露这些应用的名字，以免黑客去攻击这些应用，但表示已通知谷歌这些漏洞。谷歌发言人表示，经过 Android 安全专家与哈塞尔等人的讨论，确认这些漏洞并非属于 Android 本身。

参考链接：<http://www.2cto.com/News/201108/100063.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