

信息安全漏洞周报

2011 年 9 月 12 日-2011 年 9 月 18 日

2011 年第 37 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 117 个，其中高危漏洞 54 个、中危漏洞 56 个、低危漏洞 7 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“ModbusTagServer 和 ScadaPhone 远程缓冲区溢出漏洞”、“Wav Player '.pll'文件缓冲区溢出漏洞”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 67 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 117 个漏洞，各单位报送情况如表 1 所示。其中，启明星辰、安天、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	100	0
安天	97	0
绿盟科技	60	0
恒安嘉新	7	0
中国电力科学研究院 信息安全实验室	4	4
国家电网信息网络安全 实验室	1	1
总计	117（去重）	5

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、Red Hat、IBM、Linux 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	15	12.8%
2	Adobe	13	11.1%
3	Red Hat	7	6.0%
4	SAP	3	2.6%
5	EMC	2	1.7%
6	IBM	2	1.7%
7	Linux	2	1.7%
8	WordPress	2	1.7%
9	Google	1	0.9%
10	Apache	1	0.9%
11	其它	69	58.9%

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 产品安全漏洞

本周，微软发布了 2011 年 9 月份的月度例行安全公告，包含 5 项安全更新，共修复 15 个漏洞。这 5 项更新评级均为“重要”。此次更新修复了 Microsoft Windows 操作系统和组件、Office 办公套件和 Microsoft 服务器软件等多个产品存在的安全漏洞。攻击者可以利用这些漏洞远程执行任意代码，获得与本地用户相同的用户权限；或进一步提升特权，窃取敏感信息。CNVD 收录的相关漏洞包括：Microsoft SharePoint 'Source'参数 URI 开放重定向漏洞、Microsoft SharePoint XML 处理远程文件泄露漏洞、Microsoft SharePoint 日历脚本注入漏洞（CVE-2011-0653）、Microsoft SharePoint 'EditForm.aspx' 脚本注入漏洞（CVE-2011-1890）、Microsoft SharePoint 跨站脚本漏洞（CVE-2011-1893）、Microsoft SharePoint 联系方式跨站脚本漏洞（CVE-2011-1891）、Microsoft Office 未初始化对象指针漏洞、Microsoft Office 共享组件 DLL 装载任意代码执行漏洞（CVE-2011-1980）。其中，“Microsoft Office 未初始化对象指针漏洞”、“Microsoft Office 共享组件 DLL 装载任意代码执行漏洞（CVE-2011-1980）”的综合评级为“高危”。CNVD 提醒 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-2011-07300>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07268>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07267>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07266>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07265>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07264>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07263>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07262>

2、Adobe 产品安全漏洞

Adobe Reader/Acrobat 是处理 PDF 文件的应用程序。本周，Adobe Reader/Acrobat 被披露存在多个安全漏洞。攻击者可以利用漏洞以应用程序上下文执行任意代码或提升特权。CNVD 收录的漏洞包括：Adobe Acrobat 和 Reader 远程栈缓冲区溢出漏洞（CVE-2011-2441）、Adobe Acrobat/Reader U3D Tiff 远程堆缓冲区溢出漏洞、Adobe Acrobat 和 Reader 远程堆缓冲区溢出漏洞（CVE-2011-2435）、Adobe Acrobat 和 Reader 远程安全绕过漏洞（CVE-2011-2431）、Adobe Acrobat 和 Reader 远程堆缓冲区溢出漏洞（CVE-2011-2433）、Adobe Acrobat 和 Reader 远程堆缓冲区溢出漏洞（CVE-2011-2434）、Adobe Acrobat 和 Reader 内存泄露远程代码执行漏洞（CVE-2011-2439）、Adobe Acrobat 和 Reader 远程栈缓冲区溢出漏洞（CVE-2011-2436）。上述漏洞的综合评级均为“高危”。目前，Adobe 已经发布了这些漏洞的补丁程序，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-2011-07275>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07252>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07251>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07250>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07249>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07248>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07247>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07246>

3、Red Hat 产品安全漏洞

本周，Red Hat 的产品 Network Satellite Server 被披露存在多个漏洞。Red Hat Network Satellite Server 是一款系统管理解决方案。攻击者可以利用该产品漏洞获得敏感信息、劫持用户会话或重新定向目标用户到任意页面。CNVD 收录的相关漏洞包括：Red Hat Network Satellite Server URI 开放重定向漏洞、Red Hat Network Satellite Server 跨站脚本漏洞（CVE-2011-3344、CVE-2011-2927、CVE-2011-2920、CVE-2011-2919）。目前，厂商已经发布上述漏洞的补丁程序，CNVD 提醒广大 Red Hat 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-2011-07325>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07324>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07322>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07321>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07320>

4、SAP 产品安全漏洞

SAP Web 应用服务器（也称为 WebAS）是 SAP 应用的运行时环境。本周，SAP Web 应用服务器存在多个安全漏洞，攻击者可以利用漏洞进行跨站脚本攻击或导致拒绝服务。CNVD 收录的相关漏洞包括：SAP WebAS 'cachetest' 服务拒绝服务漏洞、SAP WebAS 恶意 SAP 快捷方式生成远程命令注入漏洞、SAP WebAS webrfc 跨站脚本漏洞。其中，“SAP WebAS 'cachetest' 服务拒绝服务漏洞”的综合评级为“高危”。除该漏洞已发布补丁程序外，其余漏洞尚未发布补丁程序，CNVD 提醒广大 SAP 用户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-2011-07328>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07327>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07312>

5、ScadaTEC ModbusTagServer 和 ScadaPhone 远程缓冲区溢出漏洞

ScadaTEC ModbusTagServer 和 ScadaPhone 存在缓冲区溢出漏洞，远程攻击者可以利用漏洞以应用程序上下文执行任意代码，上述攻击未执行成功也可以导致系统拒绝服务。互联网上已经出现针对该漏洞的攻击代码，主要影响 Scadatec ScadaPhone 5.3.11.12 30 版本和 Scadatec ModbusTagServer 4.1.1.81 版本。厂商尚未发布该漏洞的补丁程序，CNVD 提醒广大用户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-2011-07238>

小结：本周，微软发布了月度例行安全公告，同时发布了修复 Microsoft Windows 操作系统和组件、Office 办公套件和 Microsoft 服务器软件等多个产品安全漏洞的补丁。本周，Adobe、Red Hat 和 SAP 产品广泛应用的产品也被批露了存在多个漏洞。此外，ScadaTEC ModbusTagServer 和 ScadaPhone 远程缓冲区溢出漏洞为 0day 漏洞，攻击代码已在互联网上出现，有可能引发针对相关目标的网络攻击事件。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、IBM 发布升级程序，修补多个产品安全漏洞

本周，IBM 发布补丁程序，修补了 WebSphere Commerce、Tivoli Security Information 和 Event Manager 存在的安全漏洞。攻击者可获得敏感信息或劫持用户会话。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/5042>

<http://www.cnvd.org.cn/patch/5090>



本周要闻速递

1. 微软急修文本病毒漏洞

日前，最新曝出的 Windows 漏洞(MS11-071)使记事本文本(txt)中毒成为现实。微软于北京时间 9 月 14 日凌晨发布的 9 月补丁中，已修复了这一严重漏洞，建议广大网民尽快予以修复。据安全专家介绍，“文本病毒”漏洞影响所有 Windows 操作系统，可使文本文件(.txt)、富文本文件(.rtf)以及 Word 文档(.doc)成为病毒载体。如果上述文件所在目录存在黑客恶意构造的 dll 病毒，用户电脑在打开文本时就会自动激活病毒，目前只有安装微软官方补丁才能彻底封堵此类攻击方式。黑客针对‘文本病毒’漏洞的攻击主要有两种，第一种是把文本文档和 dll 病毒打包在一起，通过聊天软件、电子邮件等途径发给攻击目标；第二种是直接在热门网站的页面插入恶意代码，使访问者电脑不知不觉间感染木马病毒。安全专家建议，广大网民在修复该 Windows 漏洞前，应避免打开可疑的文本文档，并使用有效的安全软件防御恶意网页。微软安全公告显示，MS11-071(补丁编号：kb 2570947)漏洞细节已被外界公开披露，漏洞危害级别定为“重要”，建议 Windows 用户尽快修复。据悉，此次微软 9 月补丁一共发布了 5 款补丁，用于修复 Windows 系统和 Office 软件中的 15 处漏洞。

参考链接：http://it.southcn.com/9/2011-09/14/content_29853970.htm

2. Chrome 14 修复 32 个安全漏洞

据国外媒体报道，Chrome 14 稳定版已经正式发布，新版 Chrome 增加了一些新的功能，包括 Native Client（本地客户端），新的音频技术，以及修复了安全漏洞。Chrome 14 是首个支持 Native Client 技术的浏览器，Native Client 是一项开源技术，可以保证 C 和 C++语言代码在浏览器中安全运行。本质上，该技术是让软件在两个受保护沙盒中运行，理论上可大幅减少基于浏览器的威胁。Native Client 目前仍然处于开发阶段，完整版 Native Client 可以让 Web 应用可以与安装在硬盘中的程序一样流畅地运行。在 Chrome 14 中，Native Client 仅支持 Chrome Web Store 程序，但 Chrome 计划让 Native Client 最终支撑整个浏览器。另外，Chrome 14 还修复了 32 个安全漏洞。其中一个高危漏洞的发现者获得了 2337 美元的奖励。

参考链接：<http://news.newhua.com/news/2011/0919/132595.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