

信息安全漏洞周报

2011 年 10 月 10 日-2011 年 10 月 16 日

2011 年第 41 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 137 个，其中高危漏洞 64 个、中危漏洞 71 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 115 个。网上已经出现针对“Joomla Component Time Returns SQL 注入漏洞”、“WordPress 插件 GD Star Rating 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 105 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 6 家成员单位报送了本周收录的全部 137 个漏洞，各单位报送情况如表 1 所示。其中，绿盟科技、启明星辰、安天实验室的数量较多。

报送单位或个人	漏洞报送数量	私有漏洞数量
绿盟科技	171	0
启明星辰	101	0
安天实验室	33	0
恒安嘉新	11	1
安氏领信	5	0
东软	3	0
总计	137（去重）	1

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Apple、Microsoft、WordPress、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	Apple	51	37.2%
2	Microsoft	24	17.5%
3	WordPress	5	3.6%
4	Google	3	2.2%
5	Joomla!	2	1.5%
6	Simple Machines	2	1.5%
7	VideoLAN	2	1.5%
8	Symmetrix Technologies	2	1.5%
9	Wireshark	2	1.5%
10	Novell	1	0.7%
11	其它	43	31.3%

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 10 月份的月度例行安全公告，修复了 Windows 操作系统和组件、Microsoft 服务器软件、Microsoft 开发工具和软件以及 Microsoft Remote Access 软件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，获得与本地用户相同的用户权限；提升本地特权，窃取敏感信息；发送特制数据包，导致系统拒绝服务。CNVD 收录的相关漏洞包括：Microsoft Internet Explorer 'OLEAuto32.dll' 内存破坏漏洞（CNVD-2011-07770）、Microsoft Internet Explorer 'Jscript9.dll' 内存破坏漏洞（CNVD-2011-07769）、Microsoft Internet Explorer Scroll Event 内存破坏漏洞（CNVD-2011-07768）、Microsoft Internet Explorer OnLoad Event 内存破坏漏洞（CNVD-2011-07767）、Microsoft Internet Explorer Option 元素内存破坏漏洞（CNVD-2011-07766）、Microsoft Internet Explorer 选择元素内存破坏漏洞（CNVD-2011-07765）、Microsoft Internet Explorer 体元素内存破坏漏洞（CNVD-2011-07763）、Microsoft Internet Explorer 虚函数表内存破坏漏洞（CNVD-2011-07762）。上述漏洞的综合评级均为“高危”。CNVD 提醒微软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-2011-07770>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07769>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07768>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07767>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07766>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07765>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07762>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07763>

2、Apple 产品安全漏洞

本周，Apple 发布安全更新，修复 Numbers for iOS、Pages for iOS、Safari、Mac OS X Server 等多个产品存在的安全漏洞。攻击者可以利用漏洞窃取敏感信息、发起拒绝服务攻击、执行任意代码或使设备重置。CNVD 收录的相关漏洞包括：Apple Safari 隐私浏览模式逻辑漏洞、Apple Safari 未初始化内存访问漏洞、Apple Safari 任意代码执行漏洞、Apple iPhone/iPad/iPod touch iOS5 之前版本存在漏洞（CNVD-2011-07803、CNVD-2011-07801、CNVD-2011-07800、CNVD-2011-07798、CNVD-2011-07797）。厂商已经发布上述漏洞的补丁程序，CNVD 提醒 Apple 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-2011-07804>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07802>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07799>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07803>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07801>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07800>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07798>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07797>

3、WebKit 产品安全漏洞

WebKit 是一款开源的浏览器引擎。本周，WebKit 被披露存在多个安全漏洞。远程攻击者可以利用漏洞发起跨站脚本攻击、导致应用程序崩溃或执行任意代码，严重地可控制受影响系统。CNVD 收录的相关漏洞包括：WebKit 非活动 DOM 窗口跨域脚本漏洞、WebKit 未明远程代码执行漏洞（CNVD-2011-07755、CNVD-2011-07754、CNVD-2011-07752、CNVD-2011-07751、CNVD-2011-07750、CNVD-2011-07748、CNVD-2011-07747）等。上述漏洞中，除“WebKit 非活动 DOM 窗口跨域脚本漏洞”外，其余漏洞的综合评级均为“高危”。厂商已经发布上述漏洞的补丁程序，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-2011-07786>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07755>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07754>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07752>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07751>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07750>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07748>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07747>

4、Google 产品安全漏洞

本周，Google 多款产品 App Engine、Chrome 被披露存在漏洞。攻击者可以利用漏洞执行任意代码，甚至控制受影响系统。CNVD 收录的相关漏洞包括：Google Chrome WebKit 引擎 Ruby 标签废弃指针漏洞、Google App Engine SDK 跨站请求伪造漏洞、Google App Engine 远程代码执行漏洞。上述漏洞中“Google App Engine 远程代码执行漏洞”的综合评级为“高危”，且攻击代码已出现在互联网上。目前，厂商尚已发布上述漏洞的补丁程序，CNVD 提醒相关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-2011-07828>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07782>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07759>

5、Joomla Component Time Returns SQL 注入漏洞

Joomla!是一款开源的网站内容管理系统。Joomla Component Time Returns 存在 SQL 注入漏洞。由于没有有效验证提交给 id 参数的用户输入，远程攻击者可利用此漏洞获取相关用户信息，或发起进一步的攻击。目前，互联网上已经出现针对该漏洞的攻击代码，主要影响 Time Returns Component 2.0 及之前版本。该漏洞的综合评级为“高危”。目前，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-2011-07700>

小结：本周，微软发布了 2011 年 10 月份的月度例行安全公告，修复了 Windows 操作系统和组件、Microsoft 服务器软件、Microsoft 开发工具和软件以及 Microsoft Remote Access 软件多个产品存在的安全漏洞。同时，Apple、WebKit 以及 Google 产品也被披露存在多个安全漏洞。此外，Joomla Component Time Returns 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相关安全防范措施。

本周重要漏洞修补信息

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 WebSphere ILOG 安全漏洞

IBM WebSphere ILOG 是一款提供 Web 应用服务的业务管理系统。本周，IBM 发布升级程序，修补了 WebSphere ILOG 的一个跨站脚本漏洞。攻击者可以利用漏洞执行任意 HTML 和脚本代码，导致敏感信息泄露或用户会话劫持。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/5341>

本周要闻速递

1. HTC 新款手机现安全漏洞 可能泄露大量私人信息

据国外媒体报道，专门报道 Android 新闻的科技博客网站周日发现，宏达电(HTC)最新款的 Android 手机，如 Thunderbolt、EVO 3D 和 EVO 4G，都存有一个重大安全漏洞，能够导致用户的电话号码、电子邮件、全球定位系统(GPS)定位以及短信内容被泄露出去。报道称，宏达电不久前刚发布了新修改注册信息工具，从而导致了这一安全漏洞的出现。该网站指出，当用户使用的应用要求接入互联网时，用户的个人信息就有可能受到攻击。宏达电官方发布更新将是修复这一安全漏洞的惟一方式，除非用户决定手动删除记录用户行为的“APK”文件。但是由于用户并不熟悉如何 ROOT 手机，因此手动删除“APK”文件并非是最合理的选择。除非宏达电发布官方的漏洞补丁，否则用户绝对不能下载任何看上去邪恶的应用，特别是那些新发布的应用。

参考链接：<http://news.ctocio.com.cn/115/12172115.shtml>

2. 微软 10 月最新补丁发布 IE 所有版本存在安全隐患

北京时间 10 月 12 日凌晨，微软向全球用户发布 8 款安全补丁，用于修复 Windows 内核驱动、IE 浏览器等软件的 23 处漏洞。其中，编号为 KB2586448 的补丁更是一举修复了 IE 全系列版本的 8 处高危漏洞，IE9 也未能幸免。安全专家指出，此次微软安全更新对于 IE 用户防御恶意网页攻击具有一定作用，网民应及时打好补丁。据介绍，IE 浏览器的漏洞大多为远程代码执行漏洞，可能导致用户电脑在浏览网页时自动感染木马病毒。为此，用户不仅需要根据 Windows update 提示打好补丁，平时上网也应该注意开启安全软件防护，拦截挂马、钓鱼等恶意网页。微软安全公告显示，除了针对 IE 浏览器的漏洞补丁外，此次微软还发布了 1 款高危漏洞补丁和 6 款重要漏洞补丁，影响 Windows XP、Vista 以及 Windows7 等不同版本操作系统。

参考链接：<http://finance.ifeng.com/roll/20111013/4810661.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