

信息安全漏洞周报

2011 年 9 月 26 日-2011 年 10 月 9 日

2011年第39、40期合刊

本周漏洞基本情况

9 月 26 日至 10 月 9 日期间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)在 9 月 26 日至 10 月 9 日期间共收集、整理信息安全漏洞 229 个,其中高危漏洞 115 个、中危漏洞 102 个、低危漏洞 12 个。上述漏洞中,可利用来实施远程攻击的漏洞有 212 个。网上已经出现针对“WordPress 插件 Mingle Forum 'edit_post_id'参数 SQL 注入漏洞”、“PcVue ActiveX 控件数组溢出漏洞”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 133 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

6 家成员单位报送了 9 月 26 日至 10 月 9 日收录的全部 229 个漏洞,各单位报送情况如表 1 所示。其中,启明星辰、安天实验室、绿盟科技的数量较多。

报送单位或个人	漏洞报送数量	私有漏洞数量
启明星辰	185	0
安天实验室	98	0
绿盟科技	67	0
恒安嘉新	51	1
东软	9	0
安氏领信	3	0
总计	229 (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 Cisco、Mozilla、Red Hat、Novell、IBM、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	Cisco	25	10.9%
2	Mozilla	12	5.2%
3	Red Hat	9	3.9%
4	Novell	9	3.9%
5	IBM	8	3.5%
6	Google	7	3.1%
7	Sunway	7	3.1%
8	TYPO3	6	2.6%
9	SonicWALL	5	2.1%
10	Linux	5	2.1%
11	其它	136	59.6%

表 2 漏洞产品涉及厂商分类统计

本周重要漏洞信息

9月26日至10月9日，CNVD 整理和发布以下重要安全漏洞信息。

1、联软安全管理接入系统安全漏洞

本周，CNVD 在官网发布了深圳市联软科技有限公司的产品联软安全管理接入系统存在的多个安全漏洞。9月13日，CNVD 接到中国电力科学研究院信息安全实验室上报该漏洞。漏洞可被利用通过构造字符跳转目录、获取服务器完全控制权限、窃取用户与服务器 web 交互的权限或读取磁盘中任意文件。CNVD 收录的漏洞包括：联软安全接入管理系统目录遍历漏洞、联软安全接入管理系统任意文件上传漏洞、联软安全接入管理系统跨站脚本漏洞、联软安全接入管理系统任意文件读取漏洞。其中，“联软安全接入管理系统任意文件上传漏洞”的综合评级为“高危”。目前，联软公司并未提供漏洞补丁。CNVD 将继续跟踪处置情况。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07274>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07273>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07272>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07271>

2、IBM 产品安全漏洞

IBM 多款产品 Websphere Application Server、Tivoli Common Reporting 等存在安全漏洞。远程攻击者可以利用漏洞执行任意代码或进行钓鱼攻击。CNVD 收录的相关漏洞包括：IBM WebSphere 应用服务器未明跨站点请求伪造漏洞、IBM Rational AppScan 'ZIP'文件远程命令执行漏洞、IBM Rational AppScan '.scan'文件远程命令执行漏洞、IBM

Tivoli Monitoring Eclipse 帮助服务器伪造漏洞、IBM Tivoli Monitoring Eclipse 帮助服务器跨站脚本漏洞、IBM WebSphere 应用服务器跨站请求伪造漏洞。上述漏洞中“IBM Rational AppScan 'ZIP'文件远程命令执行漏洞、IBM Rational AppScan '.scan'文件远程命令执行漏洞”的综合评级为“高危”。除“IBM Rational AppScan 'ZIP'文件远程命令执行漏洞”外，厂商已经发布其余漏洞的补丁程序，CNVD 提醒 IBM 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-2011-07696>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07657>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07645>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07615>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07614>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07495>

3、Google Chrome 安全漏洞

Google 发布安全更新，修复 Chrome 浏览器存在的多个漏洞。远程攻击者可以利用漏洞绕过部分安全限制、执行任意代码或使应用程序崩溃。CNVD 收录的相关漏洞包括：Google Chrome shader translator 内存破坏漏洞、Google Chrome v8 隐藏对象处理漏洞、Google Chrome v8 binding 内存错误引用漏洞、Google Chrome lifetime 和线程处理漏洞、Google Chrome 跨域访问处理漏洞、Google Chrome SVG 文本处理漏洞、Google Chrome 文本行框处理漏洞。上述漏洞的综合评级均为“高危”。CNVD 提醒 Google 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-2011-07665>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07664>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07662>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07661>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07660>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07659>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07658>

4、Mozill 产品安全漏洞

Mozilla Firefox/SeaMonkey/Thunderbird 是 Mozilla 所发布的 WEB 浏览器/新闻组客户端/邮件客户端。上述 Mozilla 产品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窃取敏感信息。CNVD 收录的漏洞包括：Mozilla Firefox/SeaMonkey/Thunderbird 跨域脚本漏洞（CNVD-2011-07594）、Mozilla Firefox JSSubScriptLoader 安装任意插件漏洞、Mozilla Firefox RegExp 远程整数下溢漏洞、Mozilla Firefox 远程内存破坏漏洞（CNVD-2011-07555、CNVD-2011-07553、CNVD-2011-07550）、Mozilla Firefox/SeaMonkey 远程缓冲区溢出漏洞（CNVD-2011-07552）、Mozilla Firefox/

Thunderbird/SeaMonkey OGG 头内存破坏漏洞。上述漏洞中，除“Mozilla Firefox/SeaMonkey/Thunderbird 跨域脚本漏洞（CNVD-2011-07594）”的综合评级为“中危”且未发布补丁程序外，Mozilla 已经发布了其余标注为“高危”的漏洞的补丁程序，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-2011-07594>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07558>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07556>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07555>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07553>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07552>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07550>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07548>

5、WordPress 插件安全漏洞

本周，WordPress 多款插件被披露存在多个漏洞。攻击者可以利用该产品漏洞获得敏感信息、执行任意代码或控制应用程序。CNVD 收录的相关漏洞包括：WordPress Web Minimalist Theme index.php 跨站脚本漏洞、WordPress Atahualpa Theme 's'参数跨站脚本漏洞、WordPress 插件 Mingle Forum 'edit_post_id'参数 SQL 注入漏洞、WordPress 插件 AdRotate 'track'参数 SQL 注入漏洞、WordPress 插件 Link Library 'searchll'参数 SQL 注入漏洞、WordPress 插件 CevherShare 'cevhershare-admin.php' SQL 注入漏洞。其中，除“WordPress Web Minimalist Theme index.php 跨站脚本漏洞、WordPress Atahualpa Theme 's'参数跨站脚本漏洞”外，其他漏洞的综合评级均为“高危”。上述漏洞的攻击代码已在互联网出现。目前，厂商尚未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-2011-07588>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07586>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07544>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07501>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07500>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07498>

6、CiscoIOS 安全漏洞

Cisco IOS 是一个为网际互连优化的操作系统。本周，Cisco IOS 存在多个安全漏洞。攻击者可以利用漏洞执行任意代码、发起拒绝服务攻击或触发内存泄露。CNVD 收录的相关漏洞包括：Cisco IOS UDP 报文上特制 SIP NAT 拒绝服务漏洞（CNVD-2011-07593、CNVD-2011-07592）、Cisco IOS UDP 报文上 SIP 运行商多协议标记交换 NAT 拒绝服务漏洞（CNVD-2011-07591）、Cisco IOS TCP 上 SIP NAT 漏洞（CNVD-2011-07590）、Ci

sco IOS H.323 报文 NAT 拒绝服务漏洞 (CNVD-2011-07589)、Cisco IOS LDAP 网络地址转换漏洞 (CNVD-2011-07587)、Cisco IOS SIP 拒绝服务漏洞 (CNVD-2011-07584、CNVD-2011-07583)。上述漏洞的综合评级均为“高危”，目前，Cisco 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-2011-07593>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07592>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07591>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07590>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07589>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07587>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07584>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07583>

7、Novell 产品安全漏洞

本周，Novell Identity Manager 和 GroupWise 存在多个安全漏洞。攻击者可以利用漏洞执行任意代码、获得敏感信息或劫持用户会话。CNVD 收录的相关漏洞包括：Novell GroupWise Internet Agent Yearly RRULE 变量解析远程代码执行漏洞、Novell GroupWise 'TZNAME'变量解析远程代码执行漏洞、Novell GroupWise Internet Agent HTTP 接口栈缓冲区溢出漏洞、Novell GroupWise 8 WebAccess 'Directory.Item'参数跨站脚本漏洞、Novell GroupWise 拒绝服务漏洞 (CNVD-2011-07491、CNVD-2011-07492)、Novell GroupWise Weekly Calendar 变量解析远程代码执行漏洞、Novell Identity Manager 'apwaDetail' 跨站脚本漏洞 (CNVD-2011-07643)。上述漏洞中“Novell GroupWise Internet Agent Yearly RRULE 变量解析远程代码执行漏洞、Novell GroupWise 'TZNAME'变量解析远程代码执行漏洞、Novell GroupWise Internet Agent HTTP 接口栈缓冲区溢出漏洞、Novell GroupWise Weekly Calendar 变量解析远程代码执行漏洞”的综合评级均为“高危”，目前，Novell 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-2011-07510>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07508>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07507>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07493>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07492>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07491>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07489>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07643>

8、PcVue ActiveX 控件安全漏洞

本周，PcVue ActiveX 控件被披露存在多个安全漏洞。攻击者可以利用漏洞执行任意代码、破坏本地文件。CNVD 收录的相关漏洞包括：PcVue ActiveX 控件数组溢出漏洞、PcVueActiveX 控件本地文件破坏漏洞、PcVue ActiveX 控件内存修改漏洞、PcVue ActiveX 控件任意代码执行漏洞。上述漏洞的攻击代码已在互联网出现。目前，厂商尚未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-2011-07525>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07524>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07521>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07517>

小结：9 月 26 日至 10 月 9 日期间，CNVD 在官网发布了深圳市联软科技有限公司的产品联软安全管理接入系统存在的多个安全漏洞。漏洞可被利用通过构造字符跳转目录、获取服务器完全控制权限、窃取用户与服务器 Web 交互的权限或读取磁盘中任意文件。Mozilla、Cisco、Novell、IBM 产品也被披露存在多个漏洞。此外，PcVue ActiveX 控件和 Wordpress 插件的零日漏洞也对使用该产品的用户造成较严重威胁，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

CNVD 整理和发布以下重要安全修补信息。

1、Apache 发布升级程序，修补多个产品安全漏洞

本周，Apache 发布升级程序，修补了 Tomcat 和 HTTP Server 的多个安全漏洞。攻击者可以利用漏洞绕过部分安全限制、发送恶意请求。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/5271>
<http://www.cnvd.org.cn/patch/5207>

本周要闻速递

1.移动安全首成问题

安全研究部门最近公布数据表示，2010 年到 2011 年间，移动安全漏洞的数量有望比去年增加一倍，新的漏洞和更复杂的电话黑客技术最终会对新兴移动网络技术形成威胁。事实上越来越多的人将自己的个人信息输入到手机中，甚至包含自己的工作内容，

而这些恰好是黑客们最关注的内容。该报告敦促消费者谨慎下载应用程序，特别是来自第三方应用程序商店和商店外的应用，包含恶意软件的几率较高，除此之外还要记得加密系统，备份数据，安装系统更新和被盗或者遗失后有能力跟踪和删除自己手机上的信息。

参考链接: <http://www.enet.com.cn/article/2011/1008/A20111008920112.shtml>

2.中国七成团购网站存在安全隐患

近期一份安全报告显示，在进行安全检测的近 300 家团购网站中，带有高危漏洞的网站比例达到 70.6%，主要为中小型网站。知名大型团购网站的安全状况则相对较好，存在高危漏洞的网站比例为 25.0%。按此比例测算，国内存在高危漏洞的团购网站数量超过了 3500 家。分析人士认为，大量“微型”企业涌入团购市场，自身又不具备检测和修复漏洞的能力，是造成七成团购网站存在高危漏洞的主要原因。报告同时显示，许多团购网站在建站时就存在安全意识淡薄的问题，如使用开源团购程序时忽视了修复其中的漏洞，导致黑客无需密码便可登录网站管理员帐号，篡改网站页面；利用上述漏洞，黑客还可登录其他团购用户帐号，查看消费记录或窃取消费凭据。统计结果显示，这部分团购网站的比例高达 41.5%。据了解，团购网站漏洞容易导致三类风险：第一，用户密码、商品消费凭据等消费者资料泄露；第二，网站首页、商品价格等网页内容被恶意篡改；第三，网站服务器被植入脚本后门，整个网站甚至服务器系统完全被黑客控制。

参考链接: <http://www.bianews.com/news/37/n-363937.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