

信息安全漏洞周报

2011 年 8 月 29 日-2011 年 9 月 4 日

2011年第35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 100 个，其中高危漏洞 43 个、中危漏洞 53 个、低危漏洞 4 个。上述漏洞中，可利用来实施远程攻击的漏洞有 95 个。网上已经出现针对“Adobe ColdFusion 'name' 跨站脚本执行漏洞”、“Groovy Media Player '.m3u' 文件远程堆缓冲区溢出漏洞”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 57 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 7 家成员单位报送了本周收录的全部 100 个漏洞，各单位报送情况如表 1 所示。其中，恒安嘉新、绿盟科技、启明星辰报送的数量较多。

报送单位或个人	漏洞报送数量	私有漏洞数量
恒安嘉新	82	0
绿盟科技	26	0
启明星辰	13	0
东软	3	0
安氏领信	2	0
总计	100（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 WordPress、IBM、Drupal、Linux、Red Hat 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	WordPress	20	20%
2	IBM	4	4%

3	Drupal	4	4%
4	Vincent Ryan Ong	4	4%
5	Red Hat	3	3%
6	TIBCO Software Inc.	3	3%
7	Linux	2	2%
8	Apple	2	2%
9	HP	2	2%
10	Joomla!	2	2%
11	其它	54	54%

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、深信服 SSL VPN 安全漏洞

本周，CNVD 在官网发布了深圳市深信服电子科技有限公司的 SSL VPN 产品存在的多个安全漏洞。8 月 16 日，CNVD 接到国内多名安全研究者报告，称深信服 SSL VPN N4.25 版本产品存在安全漏洞，可被利用绕过获得系统管理权限或上传恶意代码文件。CNVD 收录的漏洞包括：深信服 SSL_VPN 系统控制台验证绕过漏洞、深信服 SSL_VPN 文件上传漏洞。其中，“深信服 SSL_VPN 系统控制台验证绕过漏洞”的综合评级为“高危”。目前，CNVD 正在进一步协调厂商开发漏洞的修补程序，如用户需要自行修正，建议采取以下措施：1) 服务器端设置 Cookie 为没有过期时间的 Session Cookie；2) 针对 CGI 和 Apache 模块，限制只允许运行某一路径下的 PHP 文件；3) 针对上传文件进行 PHP 后缀名检查，同时对上传目录的读写权限进行控制。广大用户可参考 CNVD 官网的漏洞公告获取更多信息。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06812>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06811>

2、IBM 产品安全漏洞

本周，IBM 的产品 Websphere Application Server、HTTP Server、Rational Build Forge 存在多个安全漏洞。攻击者可以利用漏洞进行拒绝服务攻击或窃取敏感信息。CNVD 收录的漏洞包括：IBM HTTP Server ByteRange Filter 拒绝服务漏洞、IBM Rational Build Forge 'EditSecurity' 信息泄露漏洞、IBM WebSphere Application Server Tomcat Webdav Servlet 存在未明漏洞、IBM WebSphere Application Server 信息披露漏洞。目前，厂商已经发布上述漏洞的补丁程序，CNVD 提醒广大 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-2011-07090>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07078>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07057>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07047>

3、Apple 产品安全漏洞

本周,Apple QuickTime 播放器和 WebKit 浏览器引擎被披露存在多个内存损坏漏洞,攻击者可以利用漏洞执行任意代码或使应用程序崩溃。CNVD 收录的相关漏洞包括:Apple QuickTime 内存损坏漏洞、WebKit 内存破坏远程代码执行漏洞。其中,“Apple QuickTime 内存损坏漏洞”的综合评级均为“高危”。目前,厂商已发布“Apple QuickTime 内存损坏漏洞”漏洞的修补程序,但尚未发布“WebKit 内存破坏远程代码执行漏洞”的补丁。CNVD 提醒广大用户随时关注厂商主页以获取最新版本,对于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-2011-07097>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07038>

4、WordPress 插件安全漏洞

WordPress 是一款使用 PHP 语言开发的 Web 内容管理系统(CMS)。本周,WordPress 多款插件被披露存在多个安全漏洞,攻击者可以利用漏洞提升特权、访问或修改数据或执行任意脚本代码。CNVD 收录的相关漏洞包括:WordPress 插件 Donation 'exporttocsv.php' SQL 注入漏洞、WordPress WP Bannerize 'ajax_clickcounter.php' SQL 注入漏洞、WordPress 插件 SearchAutocomplete SQL 注入漏洞、WordPress 插件 PureHTML 'id'参数 SQL 注入漏洞、WordPress 插件 Couponer 'ID'参数 SQL 注入漏洞、WordPress 插件 Yolink Search 'from_id'参数 SQL 注入漏洞、WordPress 插件 Event Registration 'id'参数 SQL 注入漏洞、WordPress 插件 Advertizer 'id'参数 SQL 注入漏洞。上述漏洞的综合评级均为“高危”,且部分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 提醒广大 WordPress 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-2011-07080>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07079>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07073>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07061>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07060>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07059>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07050>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07049>

5、Adobe ColdFusion 'name'跨站脚本执行漏洞

Adobe ColdFusion 是一个动态 Web 服务器。本周, Adobe ColdFusion 被披露存在一个跨站脚本执行漏洞。远程攻击者可利用此漏洞执行跨站脚本执行攻击。目前, 互联网上已经出现针对该漏洞的攻击代码, 主要会影响 Adobe ColdFusion 9.x 版本。厂商尚未发布该漏洞的修补程序, 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-2011-07005>

小结: 本周, CNVD 在官网发布了深圳市深信服电子科技有限公司的 SSL VPN 产品存在的多个安全漏洞, 相关用户可参考 CNVD 官网的漏洞公告获取更多信息。此外, CNVD 还收录了 IBM、APPLE 产品和 Wordpress 插件的多个漏洞。Adobe ColdFusion 'name'跨站脚本执行漏洞为 Oday 漏洞, 有可能引发互联网上的大规模网络攻击事件。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、Apache 发布升级程序, 修补 Tomcat 安全漏洞

Apache Tomcat 是一款开源的 JSP 应用服务器程序。本周, Apache 修补了 Tomcat 存在的安全漏洞。攻击者可以利用漏洞绕过某些安全限制。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/4948>

本周要闻速递

1. Skype 发现严重安全漏洞

来自国外媒体的最新消息显示, 德国安全研究人员近日表示在 Skype 上发现了一个比较严重的安全漏洞, 通过这个安全漏洞攻击者可以将有害的代码注入到用户的电脑当中, 并实现运行程序的命令以及执行相关的脚步。这样一个漏洞对 Skype 5.5.0.113 有重大的安全影响, 通过这样一个漏洞攻击者可以通过网页等方式来进行代码的注入并获得操作系统底层的权限, 而所有的这些只需要一个特别设计的外部网站上的恶意 JavaScript 文件就可以完成。

参考链接: http://www.cnii.com.cn/internet/content/2011-08/30/content_911930.htm

2. 公积金查询网站出现漏洞

国内知名安全公司向网民发出警告, 公积金查询网站 www.nms139.com 出现安全漏洞, 其查询页面被搜索引擎抓取后, 至少有数百个公积金账户的详细信息被泄漏到网上, 包括公积金账户姓名、身份证号、公积金余额、所在单位等一览无遗。据安全专家介绍

说，这可能是公积金查询网站没有设定好搜索引擎抓取策略导致。安全专家提醒广大用户，由于公积金账户包含了大量用户的个人信息，其中包括身份证号、与公积金绑定的银行账号等，一旦外泄即可被黑客利用来进行钓鱼、网络诈骗等，带来极大安全风险。凡是近期在该网站查询过公积金的用户，均可能面临个人资料外泄的风险，应把自己的银行卡密码、各种账号密码普遍进行更换，以免被黑客利用进行攻击。

参考链接：<http://news.163.com/11/0831/00/7COBKGRA00014AED.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