

信息安全漏洞周报

2011 年 12 月 26 日-2012 年 1 月 1 日

2011 年第 52 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 35 个、中危漏洞 63 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 98 个。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。本周互联网上出现“Stream Down 应答处理缓冲区溢出漏洞”、“Joomla Simple File Upload 'index.php' 远程代码执行漏洞”等的零日攻击代码，请使用相关产品的用户注意加强防范。

成员单位报送漏洞统计

本周，共 6 家成员单位和 1 家合作伙伴报送了本周收录的全部 100 个漏洞，其中包含 4 个原创漏洞。

各单位报送情况如表 1 所示。其中，启明星辰、恒安嘉新、安天实验室报送数量均较多。

报送单位或个人	漏洞报送数量	原创漏洞数量
启明星辰	51	0
恒安嘉新	45	0
安天实验室	31	0
安氏领信	13	1
东软	3	0
奇虎 360	1	1
广西网络信息安全等级保护测评有限公司	2	2
总计	100（去重）	4

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Joomla!、Microsoft、HP、FreeBSD、IBM 等多家厂商的产品，部分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	Joomla!	7	7%
2	Microsoft	5	5%
3	WordPress	5	5%
4	op5	4	4%
5	Websense	4	4%
6	Blueberry Software	3	3%
7	HP	3	2%
8	FreeBSD	2	2%
9	IBM	1	1%
10	Apache	1	1%
11	其它	65	65%

表 2 漏洞产品涉及厂商分布统计表



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 .NET Framework 安全漏洞

本周，Microsoft 发布安全公告，修复了 .NET Framework 存在的多个安全漏洞。 .NET Framework 又称 .NET 框架，是由微软公司开发的一款软件开发工具包。远程攻击者可以利用上述产品的漏洞执行任意命令、重定向用户连接、获得敏感信息或进行拒绝服务攻击。CNVD 收录的相关漏洞包括：Microsoft .NET Framework ASP.NET 表单安全绕过漏洞（CNVD-2011-09223）、Microsoft .NET Framework ASP.NET 表单安全绕过漏洞（CNVD-2011-09225）、Microsoft .NET Framework 表单验证 URI 伪造漏洞（CNVD-2011-09226）、Microsoft ASP.NET 哈希拒绝服务漏洞。上述漏洞中，除“Microsoft .NET Framework ASP.NET 表单安全绕过漏洞（CNVD-2011-09225）”外，其余漏洞的综合评级为“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/sites/main/preview/ldgg_preview.htm?tid=36188
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=36190
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=36191
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=36131

2、CoCSoft Stream Down 应答处理缓冲区溢出漏洞

CoCsoft Stream Down 是一个流媒体文件下载工具。本周，CoCsoft Stream Down 被披露存在一个缓冲区溢出漏洞。由于应用程序在处理服务器应答时存在边界错误，向应用程序发送包含超长字符串的应答请求时会触发栈缓冲区溢出。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。该漏洞的综合评级为“高危”。目前，互联网上已经出现针对该漏洞的攻击代码，主要影响 CoCsoft Stream Down 6.8.0.0 版本。目前，厂商尚未发布该漏洞的修补程序，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/sites/main/preview/ldgg_preview.htm?tid=36110

3、HP 产品安全漏洞

HP Database Archiving Software 是惠普公司开发的一款数据库归档软件。本周，HP Database Archiving Software 存在多个未明安全漏洞。远程攻击者可以利用漏洞控制应用系统。CNVD 收录的相关漏洞包括：HP Database Archiving Software 存在未明漏洞（CNVD-2011-09208、CNVD-2011-09209、CNVD-2011-09210）。目前，HP 已经发布上述漏洞的修补程序，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/sites/main/preview/ldgg_preview.htm?tid=36128

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=36129

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=36130

4、FreeBSD 产品安全漏洞

FreeBSD 是一款类 UNIX 操作系统。本周，FreeBSD 被披露存在两个综合评级为“高危”的安全漏洞。远程攻击者可以利用漏洞提升特权或进行缓冲区溢出攻击，进而可执行任意代码。CNVD 收录的相关漏洞包括：FreeBSD Chrooted 'ftpd' 远程特权提升漏洞、FreeBSD 'telnetd' 守护进程远程缓冲区溢出漏洞。目前，厂商已经发布上述漏洞的修补程序，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/sites/main/preview/ldgg_preview.htm?tid=35772

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35773

5、Joomla! 产品安全漏洞

Joomla! 是一款开源的网站内容管理系统（CMS）。本周，Joomla! 被披露存在多个综合评级为“高危”的安全漏洞。远程攻击者可以利用漏洞进行 SQL 注入攻击或执行任意代码。CNVD 收录的相关漏洞包括：Joomla! QContacts 组件 'filter_order' 参数 SQL 注入漏洞、Joomla! Simple File Upload 'index.php' 远程代码执行漏洞、Joomla! 'com_caproduct prices' 组件 'id' 参数 SQL 注入漏洞、Joomla! 'com_tsonymf' 组件 'idofitem' 参数 SQL 注入漏洞、Joomla! 'com_matrimony' 组件 'id' 参数 SQL 注入漏洞、Joomla 组件 'com_dshop' SQL 注入漏洞。上述漏洞攻击代码均已在互联网上出现，且厂商尚未发布这些漏洞的修补程序，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/sites/main/preview/ldgg_preview.htm?tid=36395
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=36348
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=36398
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35988
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=36008
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35930

更多高危漏洞如表 3 所示, 详细信息可根据 CNVD 编号, 在 CNVD 官网进行查询。

参考链接: <http://www.cnvd.org.cn/publish/main/52/index.html>

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2011-09247	Akiva WebBoard 'name' SQL 注入漏洞	高	Akiva WebBoard 8 SR 1 版本已修复此漏洞, 建议用户下载使用: http://www.akiva.com/Products_WB.htm
CNVD-2011-09174	BB Flashback SDK FBRecorder ActiveX 控件远程代码执行漏洞 (CNVD-2011-09174)	高	Blueberry Software BB FlashBack SDK 2.0.0.214 已经修复此漏洞, 建议用户下载使用: http://www.bbsoftware.co.uk/BBFlashBackSDK.aspx
CNVD-2011-09256	PHP City Portal 'profile.php' SQL 注入漏洞	高	暂无
CNVD-2011-09267	OrangeHRM SQL 注入漏洞	高	OrangeHRM 2.6.11.2 版本已修复此漏洞, 建议用户下载使用: http://www.orangehrm.com/
CNVD-2011-09252	webERP SQL 注入漏洞 (CNVD-2011-09252)	高	webERP 4.06RC2 及之后版本已经修复此漏洞, 建议用户下载使用: http://www.weberp.org/HomePage/history
CNVD-2011-09236	DIY-CMS blog mod SQL 注入漏洞	高	目前厂商已发布补丁升级程序, 请关注厂商主页以便及时下载更新: http://www.diy-cms.com/download/view_file/downid_1
CNVD-2011-09238	AjaxChat SQL 注入漏洞	高	暂无
CNVD-2011-09239	Open Conference/Journal/Harvester Systems 存在多个远程执行代码漏洞	高	目前厂商已发布补丁升级程序, 请关注厂商主页以便及时下载更新: http://pkpsfu.ca/download
CNVD-2011-09219	appRain CMF SQL 注入漏洞	高	暂无

CNVD-2011-09204	Kerberos telnetd 缓冲区溢出漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2011-008.txt
-----------------	--------------------------	---	---

表 3 部分高危漏洞列表

小结：本周，微软在官网发布了安全公告，修复了 .NET Framework 存在的安全漏洞，避免远程攻击者可以利用漏洞执行任意命令、重定向用户连接、获得敏感信息或进行拒绝服务攻击。FreeBSD 操作系统、HP 应用产品和包括 Joomla! 内容管理系统在内的多个 web 应用程序存在多个综合评级为“高危”的安全漏洞，对个人用户和企业信息化应用安全构成威胁。此外，使用 CoCsoft Stream Down 流媒体文件下载工具的用户需注意防范该产品本周出现的零日漏洞，防范由此出现的网页挂马攻击。

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 Tomcat 安全漏洞

本周，Apache 发布升级程序，修补了 Tomcat 的安全漏洞。Apache Tomcat 是一款开源的 JSP 应用服务器程序。利用上述产品漏洞，远程攻击者可以进行拒绝服务攻击。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/sites/main/preview/bdgg_preview.htm?tid=6831

本周要闻速递

1. 工信部介入信息泄露事件 要求网站及时修复漏洞

针对近期部分互联网站信息泄露事件，工信部发布通告要求，各互联网站要开展全面的安全自查，及时发现和修复安全漏洞。据介绍，近期天涯社区等网站发生用户信息泄露事件后，工信部立即启动应急预案，组织相关通信管理局、国家计算机网络应急技术处理协调中心、网络安全专家和部分互联网企业，了解核实事件情况，评估事件影响和危害，研究提出应对措施。工信部要求，各互联网站要高度重视用户信息安全工作，把用户信息保护作为关系行业健康发展和企业诚信建设的重要工作抓好抓实。发生用户信息泄露的网站，要妥善做好善后工作，尽快向用户发出警示，提醒用户修改用户名和密码。

参考链接：http://news.xinhuanet.com/tech/2011-12/30/c_122507221.htm

2. 国家互联网应急中心发布信息泄露事件跟踪情况通报

12月30日，国家互联网应急中心（CNCERT）通过网站发布了《关于相关网站用户信息泄露事件的通报》，通报了近期CNCERT掌握的信息泄露事件有关情况。

截至12月29日，CNCERT通过公开渠道获得疑似泄露的数据库有26个，涉及帐号、密码2.78亿条。其中，具有与网站、论坛相关联信息的（例如，被声称属于某个网站的数据）数据库有12个，涉及数据1.36亿条；无法判断网站、论坛关联性的数据库有14个，涉及数据1.42亿条。

CNCERT对所曝光的数据进行了抽查核实，发现部分数据是有效的，经过与相关网站、论坛联系核对后，确认CSDN社区、天涯社区两家网站发生了用户数据泄漏事件，但泄漏原因还有待进一步分析；对于其他网站、论坛，虽然曝光数据中个别条目有效，但不能判定发生了网站、论坛用户数据泄漏事件。

由于部分互联网用户在不同网站注册帐号时习惯使用相同用户名和密码，因此一旦在某个网站注册的帐号、密码等信息被泄漏，该用户在其他网站注册的帐号和密码也面临被泄漏的风险；此外，部分用户设置的密码比较简单（例如，使用用户名拼音、电话号码等），容易被黑客猜解。因此，部分黑客利用上述隐患，大肆对各个网站的用户注册信息进行探测猜解，甚至利用个别网站泄漏的用户数据作为“字典”，在其他网站上做恶意尝试，这两种被形象地称为“暴力破解”和“撞库”的恶意行为，极大地威胁到互联网用户的信息安全。根据各网站的验证结果，目前网上流传的泄漏库中，部分数据是有效的，但也有大量的数据是虚假的、无效的。例如，根据CSDN和天涯的测试结果，网上曝光的相关数据库中有一部分并不是其用户的数据。

尽管曝光的数据有真有假，但是不可否认的是此次事件的确给互联网用户带来了严重的个人信息安全威胁。被泄漏真实信息的用户，其网站个人账户中的信息可能会被窃取，甚至帐号被盗用；很多用户注册帐号时留下了电子邮件帐号，如果泄漏的密码与电子邮件密码相同，则会带来个人邮件的泄漏风险；黑客甚至可以利用这些邮件帐号冒用用户名义，在其他网站上利用密码重置功能进一步窃取更多帐号。此外，这些大量被泄漏的帐号也可能被黑客用于发送虚假、欺诈信息，危害其他用户安全和社会稳定。

事件发生以来，CNCERT在工业和信息化部的指导下，紧急联系各个网站、论坛开展应急处置，并组织召开专家研判会议。CSDN社区和天涯社区分别在各自网站发布公告，确认事件并提醒用户采取应对措施，对泄露账户密码进行有效性测试、临时锁定帐号并通知用户修改密码。其他网站、论坛也分别对网上泄漏数据进行比对测试，通知“命中”用户采取应对措施。各个网站、论坛也根据专家建议，着手采取系统安全防护工作，提高用户信息保密强度、用户登录验证难度等。

3.广东出入境网存漏洞 公安部门称已修复

12月29日，继多家商业网站被爆出用户信息外泄后，有网友披露，广东省公安厅出入境政务服务网存在安全漏洞，几百万申请者信息存在外泄风险。29日，某网站公开了两个网站安全漏洞，其中一个名为“广东省公安厅出入境政务服务网网上申请数据泄

露”。网站介绍，该漏洞提交日期为 11 月 29 日，目前已得到国家互联网应急中心确认，该中心广东分中心正在处置。对于危害等级，网站描述为“低”。有知情人士透露，29 日中午，他访问了广东省公安厅出入境政务服务网后台，“444 万申请者真实姓名、港澳通行证号码、出生年月日和电话号码都可以看到。”29 日晚，广东省公安厅官方微博发布信息：“近日，网上有消息称，广东省公安厅出入境政务服务网存在技术漏洞问题。经初步调查，该网站确实存在技术漏洞，现已修补完毕。”

参考链接：http://www.shxb.net/html/20111231/20111231_300962.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