国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2012 年 10 月 22 日-2012 年 10 月 28 日　　2012 年第 42 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 119 个，其中高危漏洞 38 个、中危漏洞 75 个、低危漏洞 6 个。上述漏洞中，可利用来实施远程攻击的漏洞有 114 个。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。本周互联网上出现“FirePass SSL VPN 'refreshURL'参数 URI 重定向漏洞”、“VAM Shop 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加强防范。

成员单位报送漏洞统计

本周，共 6 家成员单位和多个合作伙伴报送了本周收录的全部 119 个漏洞。各单位报送情况如表 1 所示。其中，启明星辰、绿盟科技等单位报送数量较多。此外，恒安嘉新公司和一位个人报送者向 CNVD 提交了 9 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
启明星辰	82	0
绿盟科技	56	0
安天实验室	38	0
天融信	43	0
恒安嘉新	49	8
安氏领信	7	0
个人报送者	1	1
报送总计	276	9
录入总计	119（去重）	9

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Drupal、WordPress、Adobe 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	Drupal	13	11%
2	WordPress	11	9%
3	Adobe	7	6%
4	Arial Software LLC	5	4%
5	phpMyBitTorrent	4	3%
6	Microsoft	3	2%
7	IBM	3	2%
8	Interspire Pty. Ltd.	3	2%
9	Linux.	2	1%
10	F5	2	1%
11	其它	66	59%

表 2 漏洞产品涉及厂商分布统计表

漏洞按影响类型统计

本周，CNVD 收录了 119 个漏洞。其中操作系统漏洞 3 个，应用程序漏洞 68 个，WEB 应用漏洞 43 个，网络设备漏洞 3 个，数据库漏洞 1 个，安全产品漏洞 1 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	3
应用程序漏洞	68
WEB 应用漏洞	43
网络设备漏洞	3
安全产品漏洞	1
数据库漏洞	1

表 3 漏洞按影响类型统计表

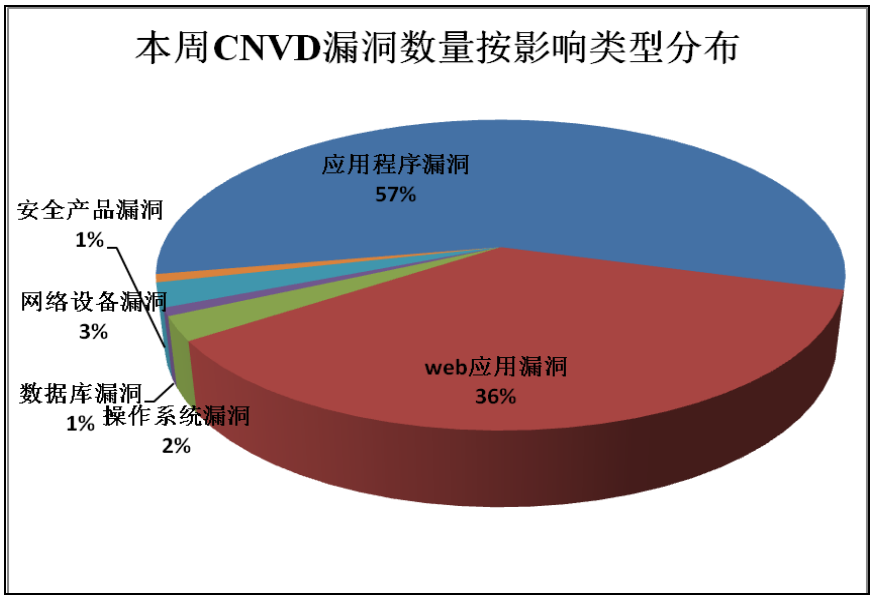

图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 3 个网络设备漏洞：多个 HP 产品信息泄露漏洞、F5 FirePass 远程 SQL 注入漏洞、Broadcom BCM4325 和 BCM4329 无线芯片越界读拒绝服务漏洞。其中，“多个 HP 产品信息泄露漏洞”和“F5 FirePass 远程 SQL 注入漏洞”的综合评级均为“高危”。相关厂商已经修复了上述漏洞。

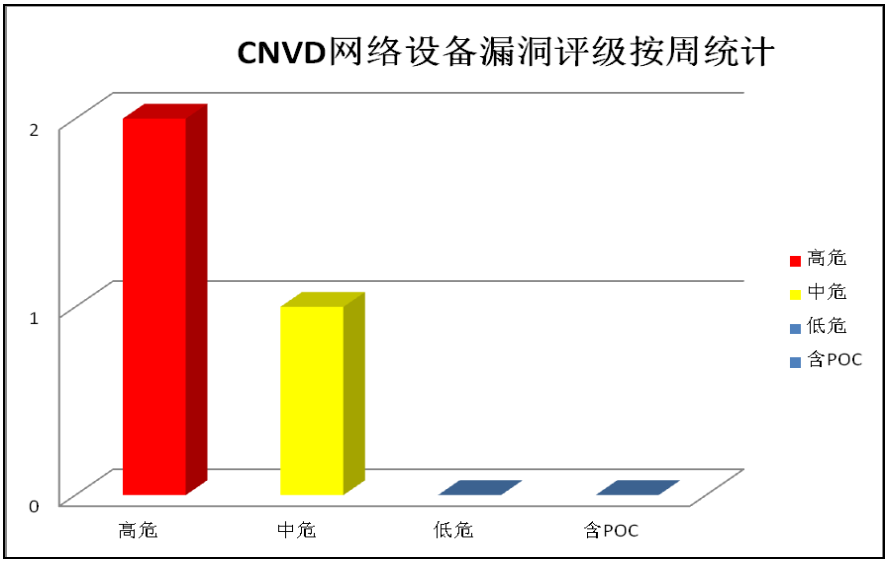

图 2 网络设备漏洞统计

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、Exim 邮件服务软件堆缓冲区溢出漏洞

Exim 是由英国剑桥大学的研究组织开发的一款开源邮件服务软件，主要用于搭建邮件服务器或用作接收和发送邮件的客户端代理程序。该软件由于配置简单，功能灵活，可运行于大多数类 UNIX 系统上，如：Solaris、AIX、Linux 等，近年来在国内外应用较为广泛。一些厂商发行的 Linux 操作系统版本中也默认集成了 Exim 软件或 Exim 软件源，如：Redhat、Debian、Ubuntu 等。

CNVD 收录的相关漏洞包括：Exim 堆缓冲区溢出漏洞，漏洞的综合评级为“高危”。Exim 默认安装下集成启用的用于支持 DKIM（域名密钥识邮件标准）的功能模块中存在漏洞，由于该模块未能正确处理相应参数，导致堆缓冲区溢出。攻击者可以向服务器发起远程攻击，严重的可以获得服务器主机管理权限。目前，厂商已经修复了上述漏洞，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=59995

2、Adobe 产品安全漏洞

Adobe Shockwave Player 是一款播放器插件。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Shockwave Player 索引错误漏洞、Adobe Shockwave Player 缓冲区溢出漏洞（CNVD-2012-15426、CNVD-2012-15428、CNVD-2012-15429、CNVD-2012-15431、CNVD-2012-15433）。上述漏洞的综合评级均为“高危”。目前，厂商已经修复了上述漏洞，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=59859
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59861
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59862
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59864
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59866
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59865

3、WordPress 插件安全漏洞

WordPress 是一款使用 PHP 语言开发的内容管理系统。本周，该产品的多个插件被披露存在多个安全漏洞，攻击者利用漏洞可获得敏感信息，发起跨站脚本攻击和浏览器点击劫持攻击，执行任意代码。

CNVD 收录的相关漏洞包括：WordPress 插件 White Label CMS 跨站脚本漏洞、WordPress 插件 White Label CMS 跨站请求伪造漏洞、WordPress 插件 Wordfence 'email' 跨站脚本漏洞 WordPress 插件 Thank You Counter Button'paged'跨站脚本漏洞、WordPress 插件 Zingiri Bookings 'error'跨站脚本漏洞、WordPress 插件 Zingiri Form Builder'error'跨站脚本漏洞、WordPress Spider Calendar 插件'many_sp_calendar'跨站脚本漏洞、WordPress

插件 UnGallery 'search'参数远程任意命令执行漏洞等。其中，“WordPress 插件 UnGallery 'search'参数远程任意命令执行漏洞”的综合评级为“高危”。目前，厂商已经修复了上述漏洞，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=59824
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59823
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59831
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59869
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59870
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59868
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59911
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59855

4、IBM 产品安全漏洞

IBM XIV Storage System 是海量磁盘存储系统；IBM DB2 Universal Database Server 是一款大型的商业关系数据库；IBM AIX 是一款商业性质的操作系统。本周，上述 IBM 产品被披露存在多个安全漏洞，攻击者利用漏洞可访问其他受限文件，触发基于栈的缓冲区溢出，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：IBM AIX FTP 客户端安全绕过漏洞、IBM DB2 产品远程栈缓冲区溢出漏洞、多个 IBM XIV Storage System 产品拒绝服务漏洞。其中，“IBM DB2 产品远程栈缓冲区溢出漏洞”和“多个 IBM XIV Storage System 产品拒绝服务漏洞”的综合评级均为“高危”。厂商已经修复了上述漏洞，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=59790
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59789
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59792

5、Interspire Email Marketer 安全漏洞

Interspire Email Marketer 是一个基于 Web 的电子邮件营销解决方案。本周，该产品被披露存在多个漏洞，远程攻击者利用漏洞可访问或修改数据，或利用基础数据库中的潜在漏洞，执行恶意 HTML 和脚本代码。

CNVD 收录的相关漏洞包括：Interspire Email Marketer SQL 注入漏洞、Interspire Email Marketer 存在多个 HTML 注入漏洞、Interspire Email Marketer 'Action'跨站脚本漏洞。其中，“Interspire Email Marketer SQL 注入漏洞”的综合评级为“高危”。厂商尚未发布上述漏洞的修补程序，CNVD 提醒广大用户随时关注厂商主页以获取最新版本，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=59957
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59956

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59955

6、VAM Shop SQL 注入漏洞

VAM Shop 是一款基于 WEB 的应用程序。本周，VAM Shop 被披露存在一个综合评级为“高危”的 SQL 注入漏洞。攻击者利用漏洞可获得数据库信息或控制应用系统。目前，互联网上已经出现了针对该漏洞的攻击代码，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=59906

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-2012-15452	TIBCO Formvine 未授权访问安全绕过漏洞	高	TIBCO Formvine 3.2.1 已经修复此漏洞，建议用户下载使用：http://www.tibco.com/index.html
CNVD-2012-15440	Kunena 'search'参数 SQL 注入漏洞	高	暂无
CNVD-2012-15439	Symphony 'symphony/system/authors/edit' SQL 注入漏洞	高	暂无
CNVD-2012-15427	F5 FirePass 远程 SQL 注入漏洞	高	F5 FirePass 7.0.0 HF-70-7 或 6.1.0 HF-610-9 已经修复此漏洞，建议用户下载使用：http://support.f5.com/kb/en-us/solutions/public/13000/800/sol13826.html http://support.f5.com/kb/en-us/solutions/public/13000/800/sol13818.html http://support.f5.com/kb/en-us/solutions/public/13000/600/sol13656.html
CNVD-2012-15414	Joomla Tags 组件'tag'参数 SQL 注入漏洞	高	暂无
CNVD-2012-15374	Drupal 任意 PHP 代码执行漏洞（CNVD-2012-15374）	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：http://drupal.org/node
CNVD-2012-15421	Dolibarr 存在多个 SQL 注入漏洞	高	暂无
CNVD-2012-15424	多个 HP 产品信息泄露漏洞	高	用户可参考如下厂商提供的安全公告获得补丁信息：https://h20566.www2.hp.com/portal/site

			/hpsc/public/kb/docDisplay?docId=emr_na-c03515685
CNVD-2012-15410	ATutor AContent 安全绕过密码修改漏洞	高	暂无
CNVD-2012-15377	Campaign Enterprise 'UID' SQL 注入漏洞	高	Campaign Enterprise 11.0.551 已经修复此漏洞，建议用户下载使用：http://www.arialsoftware.com/enterprise.htm

表 3 部分高危漏洞列表

本周，Adobe Shockwave Player、Interspire Email Marketer 以及 WordPress 的多款插件被披露存在多个安全漏洞，攻击者利用漏洞可获得敏感信息或执行任意代码。IBM 的多款产品也被披露存在多个漏洞，攻击者利用漏洞可访问其他受限文件，触发栈缓冲区溢出，发起拒绝服务攻击。VAM Shop 被披露存在零日漏洞，建议采用该软件的用户随时关注厂商主页，及时获取修复补丁或解决方案。

本周，互联网上应用广泛的开源邮件服务软件 Exim 被披露存在一个高危漏洞(CNVD 收录编号：CNVD-2012-15485)。利用漏洞可以发起针对邮件服务器的远程攻击，构成信息泄露和运行安全风险。CNVD 发布了关于开源邮件服务软件 Exim 存在高危漏洞的重要安全通报，建议相关用户及时下载软件最新版本，完成可用性测试后做好升级部署。如因业务关系暂时无法升级的，可以通过临时禁用支持 DKIM 功能来防范漏洞攻击威胁。

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、Avaya 布升级程序，修补 Aura Presence Services 漏洞

Avaya Aura Presence Services 是一款统一通信应用解决方案。本周，Avaya 修补了 Aura Presence Services 存在的漏洞。本地攻击者可以利用漏洞进行拒绝服务攻击或获得敏感信息。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=24194

本周要闻速递

1. Google Play 内大量免费应用携带 SSL 漏洞

10 月 25 日消息，研究人员近来发现 GooglePlay 商店中有应用程序有错误的加密，

防毒应用程序因为 SSL 防护不足，骇客可以轻易下载恶意病毒凭证。IT 商业新闻网获悉，安卓市场的程序已经有 1.85 亿供使用者下载，这些使用者的网络银行资料、社交网站资料、电子邮件与即时讯息内容都暴露在危险中。据台媒最新报道，研究人员从 Google Play 市场中下载了 1 万 3 千 5 百项免费应用程序后透过静态均衡分析发现共 41 项应用程序持续泄露敏感资讯，其中以冰淇淋三明治版本的操作系统为甚，只要将此版本的手机连上 WLAN，科学家就能轻松打破安全机制，显示 SSL 与 TLS 协议有问题，因此所有网站与使用者间的凭证都受到影响。对此，Google 发言系统拒绝回应，毕竟所谓的 41 项应用程序并未被点名，也没有证据显示这些脆弱的应用程序是由 Google 直接开发。值得注意的是，这些安全漏洞包括接受未验证内容的防毒应用程序、某应用程序的付费过程泄露登入帐密资讯、某颇受欢迎的 Web 2.0 应用程序在使用者登入其他网站时会泄露 Facebook 与 Google 帐户个资、某使用者高达 5000 万人的跨平台通讯应用程序会泄露使用者通讯录中的所有电话号码等。

参考链接：http://news.xinhuanet.com/tech/2012-10/25/c_123870733.htm

2. MySQL 漏洞可令攻击者绕过密码验证

安全研究人员已披露了 MySQL 服务器上一个漏洞的细节，该漏洞有可能会让潜在的攻击者不必输入正确的身份证书便可访问 MySQL 数据库。该漏洞被确认为 CVE-2012-2122 号漏洞，已经在五月发布的 MySQL 5.1.63 和 5.5.25 版本中得以修复。但是很多服务器管理员或许尚未意识到这个漏洞可能带来的影响，因为上述两个新版本中的变更日志关于这一安全漏洞的信息非常之少。这个漏洞只有在 MySQL 所运行的系统中，当 memcmp()功能可返回超出-128 到 127 范围的值时才能被利用。也就是说，只有在 Linux 系统使用 SSE 优化库(GNU C 库)的场合下才能被利用。目前尚没有用于 MySQL 5.0x 的官方补丁，因为这一版本 Oracle 已不再支持。不过，有些 Linux 厂商可能会从 MySQL 5.1 或 5.5 向下移植这一补丁。

参考链接：http://security.ctocio.com.cn/476/12455476.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