

信息安全漏洞周报

2012 年 4 月 16 日-2012 年 4 月 22 日

2012 年第 16 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 158 个，其中高危漏洞 32 个、中危漏洞 101 个、低危漏洞 25 个。上述漏洞中，可利用来实施远程攻击的漏洞有 138 个。本周收录的漏洞中，已有 128 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“Joomla!组件（com_ponygallery）SQL 注入漏洞”、“Squid Proxy 'Host' HTTP 头安全绕过漏洞”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 7 家成员单位和多个合作伙伴报送了本周收录的全部 158 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、天融信等单位报送数量较多。此外，个人研究者上报了 3 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	127	0
绿盟科技	80	0
天融信	29	0
安天实验室	28	0
恒安嘉新	19	0
东软	3	0
安氏领信	4	0
个人研究者	3	3
报送总计	294	3
总计	158（去重）	3

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Oracle、Apache、ZOHO Corporation、Wordpress、HP 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	Oracle	82	51.9%
2	Apache	6	3.8%
3	ZOHO Corporation	4	2.5%
4	Wordpress	4	2.5%
5	HP	3	1.9%
6	IBM	2	1.3%
7	Drupal	2	1.3%
8	Linux	1	0.6%
9	Joomla!	1	0.6%
10	Samsung	1	0.6%
11	其它	52	33%

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 158 个漏洞。其中操作系统漏洞 10 个，应用程序漏洞 105 个，WEB 应用漏洞 26 个，数据库漏洞 17 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	10
应用程序漏洞	105
WEB 应用漏洞	26
网络设备漏洞	0
数据库漏洞	17
安全产品漏洞	0

表 3 漏洞按影响类型统计表

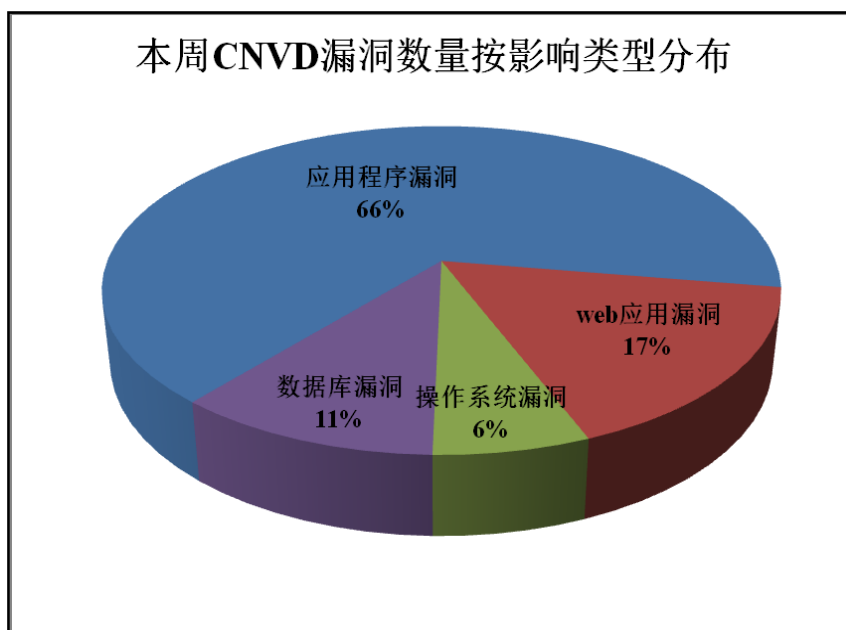


图 1 本周漏洞按影响类型分布

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、Oracle 产品安全漏洞

4 月 17 日，Oracle 发布了 2012 年 4 月的安全更新，共包含 88 个补丁，修复了多款产品的安全漏洞。产品涉及 Oracle 数据库（6 个）、中间件产品 Fusion Middleware（11 个）、企业管理器网格控制产品 Oracle Enterprise Manager Grid Control（6 个）、电子商务套装软件 Oracle E-Business Suite（4 个）、供应链套装软件 Oracle Supply Chain Products Suite（5 个）、PeopleSoft 产品（15 个）、FLEXCUBE 产品（17 个）、Siebel 临床试验管理系统（2 个）、Primavera 产品（1 个）、Sun 系列产品（15 个）和 MySQL 数据库（6 个）。上述漏洞补丁中，12 个为高危漏洞的补丁，79 个漏洞可被远程利用。其中，中间件产品中的 Oracle JRockit 漏洞，Oracle 官方对其给予的 CVSS 评分为 10.0（最危险的等级分）。

CNVD 收录的相关漏洞包括：Oracle Outside In Technology 远程漏洞（CNVD-2012-11377、CNVD-2012-11379、CNVD-2012-11381）、Oracle WebCenter Forms Recognition 远程漏洞（CNVD-2012-11303、CNVD-2012-11307）、Oracle Database Server RDBMS Core 远程漏洞（CNVD-2012-11319）、Oracle Supply Chain AutoVue Office 远程漏洞（CNVD-2012-11321）、Oracle Grid Engine 远程漏洞（CNVD-2012-11340）等。上述漏洞的综合评级均为“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=47581

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=47583
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=47585
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=47477
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=47462
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=47519
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=47521
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=47542

2、Apache 产品安全漏洞

Apache HTTP Server 是一款 HTTP 服务程序；Apache OFBiz 是一款开源的 ERP 系统。本周，上述 Apache 产品被披露存在多个安全漏洞，攻击者可以利用漏洞发起跨站脚本攻击或执行任意代码。CNVD 收录的相关漏洞包括：Apache HTTP Server 'LD_LIBRARY_PATH'不安全库装载任意代码执行漏洞、Apache OFBiz 存在未明远程代码执行漏洞、Apache OFBiz 跨站脚本漏洞（CNVD-2012-11276、CNVD-2012-11279、CNVD-2012-11278、CNVD-2012-11277）。其中，“Apache OFBiz 存在未明远程代码执行漏洞”的综合评级为“高危”。目前，Apache 已经发布这些漏洞的修补程序，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=47455
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=47415
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=47417
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=47419
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=47418
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=47416

3、ManageEngine Support Center Plus 安全漏洞

ManageEngine Support Center Plus 是一款客户关系管理工具。本周该产品被披露存在多个安全漏洞，攻击者可以利用漏洞发起 SQL 注入、跨站脚本攻击，执行未授权操作。CNVD 收录的相关漏洞包括：ManageEngine Support Center Plus SQL 注入漏洞、ManageEngine Support Center Plus 跨站脚本漏洞、ManageEngine Support Center Plus 存在漏洞（CNVD-2012-11283、CNVD-2012-11284）。其中，“ManageEngine Support Center Plus SQL 注入漏洞”的综合评级为“高危”。目前，厂商已经发布这些漏洞的修补程序，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=47435
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=47436
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=47438
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=47437

4、IBM 产品安全漏洞

IBM Tivoli Directory Server 是一款 LDAP 目录服务协议服务程序。本周，该产品被披露存在多个漏洞，远程攻击者可以利用此漏洞对应用服务进行拒绝服务攻击。CNVD 收录的相关漏洞包括：IBM Tivoli Directory Server 分页搜索拒绝服务漏洞（CNVD-2012-11304、CNVD-2012-11305）。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=47475
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=47463

5、Joomla!组件（com_ponygallery）SQL 注入漏洞

Joomla! 是一款开源的内容管理系统 (CMS)。本周，Joomla! 的一款组件 com_ponygallery 被披露存在一个 SQL 注入漏洞，远程攻击者可利用漏洞获取底层数据库信息，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。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=47735

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-2012-11385	musl libc 远程栈缓冲区溢出漏洞	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免攻击者可以利用漏洞以应用程序上下文执行任意代码： http://www.etalabs.net/musl/
CNVD-2012-11312	phpdisk 网盘系统 SQL 注入漏洞	高	暂无
CNVD-2012-11215	IrfanView FlashPix 插件堆缓冲区溢出漏洞（CNVD-2012-11215）	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免攻击者可以利用漏洞以应用程序上下文执行任意代码： http://www.irfanview.com/plugins.htm
CNVD-2012-11213	ActiveScriptRuby 'GRScript18.dll' ActiveX 控件 DLL 装载任意代码执行漏洞	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免攻击者可以利用漏洞以应用程序上下文执行任意 RUBY 命令： http://www.artonx.org/data/asr/ 或通过执行如下命令注销 COM 服务： regsvr32 /u ASR-1.8install directory\bin\GRScript18.dll
CNVD-2012-11288	OllyDBG 资源目录整数溢出漏洞	高	暂无
CNVD-2012-11223	ACC PHP eMail SQL 注入漏洞	高	暂无

CNVD-2012-11408	OpenSSL 'asn1_d2i_read_bio()' DER 格式数据处理漏洞	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免攻击者可以利用漏洞执行任意代码： http://secunia.com/advisories/48847/
CNVD-2012-11280	EmbryoCore CMS SQL 注入漏洞	高	暂无
CNVD-2012-11413	WordPress 插件 Nmedia Users File Uploader 存在未明漏洞	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免攻击者利用漏洞造成危害： http://wordpress.org/extend/plugins/nmedia-user-file-uploader/changelog/
CNVD-2012-11216	OpenJPEG Gray16 TIFF 图像文件内存破坏漏洞	高	暂无

表 3 部分高危漏洞列表

小结：4 月 17 日，Oracle 发布了 2012 年 4 月的安全更新，共包含 88 个补丁，修复了多款产品的安全漏洞。其中，12 个为高危漏洞的补丁，79 个漏洞可被远程利用。其中，中间件产品中的 Oracle JRockit 漏洞，Oracle 官方将其 CVSS 评分定为 10.0，对系统机密性、完整性、可用性构成全面影响。

本周，Apache 产品被披露存在多个安全漏洞，攻击者可以利用漏洞发起跨站脚本攻击或执行任意代码。ManageEngine Support Center Plus 被披露存在多个安全漏洞，攻击者可以利用漏洞发起 SQL 注入攻击、跨站脚本攻击。IBM Tivoli Directory Server 被披露存在多个漏洞，远程攻击者可以利用漏洞对应用服务进行拒绝服务攻击。此外，Joomla! 组件（com_ponygallery）则被披露存在零日漏洞。

请使用相关产品的用户注意加强防范。

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、Linux 发布升级程序，修补 Kernel 安全漏洞

本周，Linux 发布升级程序，修补了 Kernel 存在的安全漏洞。Linux 是一款开源的操作系统。Linux Kernel 装载 xfrm6_tunnel 模块时存在安全漏洞，导致 sk_buff 两次释放而使内核崩溃。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=16092

本周要闻速递

1. 四核 HTC One X 软件漏洞已修复

据悉，全球版的 HTC One X 出现电源管理问题。为了解决这一问题，目前 HTC 已经发布了补丁修补这一漏洞。用户需要通过 ADB 安装新的 APK，修复后的 HTC One X 将提升 10%至 20%的电池容量。同时，这一补丁也将修正关于手机不正常重启和死机的问题。

参考链接：<http://mobile.zol.com.cn/289/2894300.html>

2. 苹果上个季度安全漏洞数量增多

苹果系统和软件给人的印象一直是最安全、最不被攻击的。然而，趋势科技（Trend Micro）最近公布的结果却表明，用苹果安全的观点是不正确的。事实上，苹果在上个季度的安全漏洞数量是最多的，超过他们的竞争对手 Oracle、谷歌、Adobe，甚至微软。趋势科技对 2012 年第一季度各家公司的系统和软件安全性进行了一次调查，结果发现，苹果所有产品的安全漏洞总数达到 91 个，是业内安全漏洞最多的公司。前十家公司还包括甲骨文，总数为 78 个，谷歌的总数为 73 个，而微软的只有 43 个。

参考链接：<http://soft.zol.com.cn/289/2893609.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