

信息安全漏洞周报

2012 年 12 月 17 日-2012 年 12 月 23 日

2012 年 第 50 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 136 个，其中高危漏洞 35 个、中危漏洞 98 个、低危漏洞 3 个。上述漏洞中，可利用来实施远程攻击的漏洞有 125 个。本周收录的漏洞中，已有 65 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“PHP Address Book 'group'参数跨站脚本漏洞”、“Kiwi Syslog Web Access 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 5 家成员单位和多个合作伙伴报送了本周收录的全部 136 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、恒安嘉新等单位报送数量较多。此外，广西网信、上海交通大学及 High-Tech Bridge Security Research Lab 向 CNVD 提交了 8 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	89	0
绿盟科技	65	0
安天实验室	38	0
恒安嘉新	48	0
天融信	33	0
High-Tech Bridge Security Research Lab	5	5
广西网信	2	2
上海交通大学	1	1

报送总计	281	8
录入总计	136（去重）	8

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 WordPress、IBM、Drupal、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	WordPress	16	12%
2	IBM	15	11%
3	Drupal	6	4%
4	Adobe	4	3%
5	Real Networks	2	2%
6	Oracle	2	2%
7	Opera	2	2%
8	Dell	1	1%
9	Siemens	1	1%
10	Microsoft	1	1%
11	其它	86	61%

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 136 个漏洞。其中应用程序漏洞 72 个，WEB 应用漏洞 53 个，操作系统漏洞 5 个，网络设备漏洞 5 个，数据库漏洞 1 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	5
应用程序漏洞	72
WEB 应用漏洞	53
网络设备漏洞	5
数据库漏洞	1
安全产品漏洞	0

表 3 漏洞按影响类型统计表

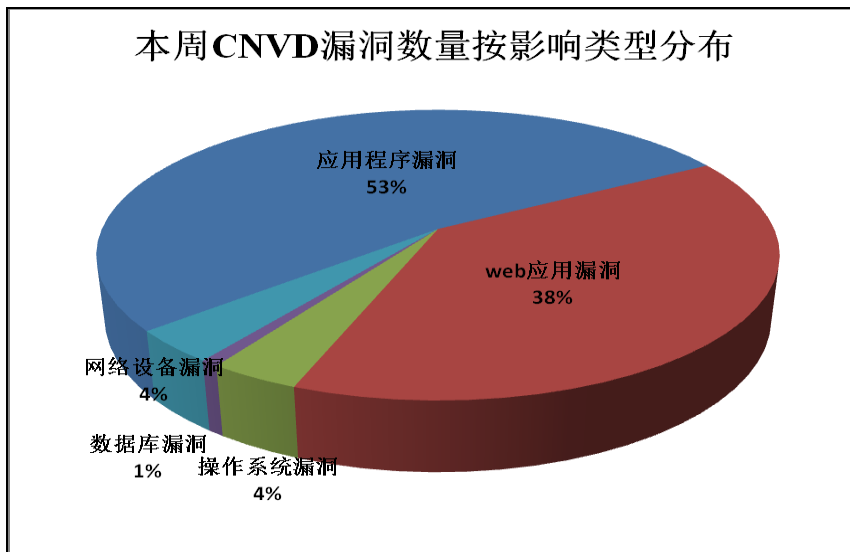


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 5 个网络设备漏洞：Samsung SmartPhones 本地权限提升漏洞、Carlo Gavazzi EOS-BOX 管理员密码获取安全绕过漏洞、Carlo Gavazzi EOS-BOX SQL 注入漏洞、D-Link DCS-932L 信息泄露漏洞、Loadbalancer Enterprise R16 HTML 注入漏洞。其中，“Carlo Gavazzi EOS-BOX 管理员密码获取安全绕过漏洞、Carlo Gavazzi EOS-BOX SQL 注入漏洞”的综合评级均为“高危”。目前，互联网上已经出现了针对“Samsung SmartPhones 本地权限提升漏洞”的攻击代码。相关厂商已经发布了漏洞修补程序。

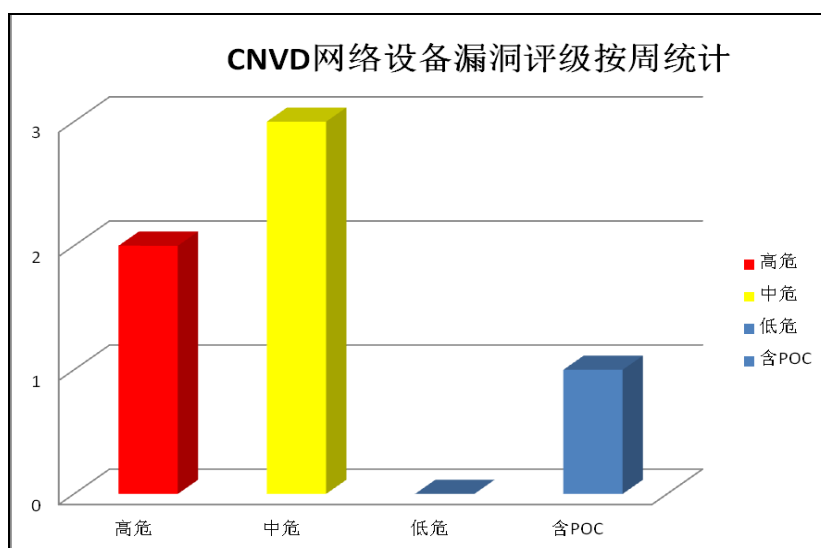


图 2 网络设备漏洞统计



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、Adobe 产品安全漏洞

Adobe Flash Player 是一款 Flash 文件处理程序；Adobe Shockwave Player 是一款用于播放使用 Director Shockwave Studio 制作的网页的软件。本周，上述 Adobe 产品被披露存在多个安全漏洞，攻击者利用漏洞可使应用程序崩溃，执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Shockwave Player 'Xtra'远程代码执行漏洞、Adobe Shockwave Player 远程代码执行漏洞、Adobe Shockwave Player ActiveX 控件安全等级下降漏洞、Adobe Flash Player 内存破坏拒绝服务漏洞。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=CNVD-2012-16922

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16924

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16921

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16920

2、IBM 产品安全漏洞

IBM Rational ClearQuest 是一款软件变更、追踪管理解决方案；IBM Lotus Notes 服务器是一款基于 WEB 协同工作的应用程序架构；IBM Intelligent Operations Center 是一款智能运行中心软件；IBM InfoSphere Information Server 是一款数据集成软件平台；IBM Tivoli Storage Manager 是一款遵循 ANSI SAN 标准的可扩展解决方案，用于发现、监控和管理企业 SAN 架构组件，并可分配和自动操纵企业的附加磁盘存储资源。本周，上述 IBM 产品被披露存在多个安全漏洞，攻击者利用漏洞可绕过安全限制，获得服务器或数据库敏感信息。

CNVD 收录的相关漏洞包括：IBM Tivoli Storage Manager for Space Management 本地未授权访问漏洞、IBM Tivoli Storage Manager for Space Management 远程未授权访问漏洞、IBM Intelligent Operations Center HTML 注入漏洞、IBM InfoSphere Information Server InfoCenter 组件安全绕过漏洞、IBM InfoSphere Information Server Java 组件安全绕过漏洞、IBM InfoSphere Information Server Web 控制台组件安全绕过漏洞、IBM Lotus Notes Web 应用跨站脚本漏洞、IBM Rational ClearQuest SQL 错误消息攻击漏洞等。其中，“IBM Tivoli Storage Manager for Space Management 本地未授权访问漏洞”的综合评级为“高危”。目前，厂商已发布了上述漏洞修补程序。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=CNVD-2012-16952

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16953

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16929

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16895

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16897

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16898

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16870

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16871

3、Drupal 模块安全漏洞

Drupal 是一款基于 PHP 的内容管理系统。本周，该产品的多个模块被披露存在多个安全漏洞，攻击者利用漏洞可提交特殊请求绕过安全限制获得对未授权内容的访问。

CNVD 收录的相关漏洞包括：Drupal Core 任意 PHP 代码执行漏洞、Drupal Context 模块信息泄露漏洞、Drupal Core 访问绕过漏洞（CNVD-2012-16949）、Drupal Core 访问绕过信息泄露漏洞、Drupal CAPTCHA 模块访问绕过漏洞、Drupal Apache Solr Autocomplete 模块跨站脚本漏洞。其中，“Drupal Core 任意 PHP 代码执行漏洞”的综合评级为“高危”。目前，厂商已发布了上述漏洞修补程序。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=CNVD-2012-16951

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16948

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16949

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16950

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16941

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16942

4、WordPress 插件安全漏洞

WordPress 是一款基于 PHP 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，上传任意文件，执行任意代码。

CNVD 收录的相关漏洞包括：WordPress 插件 PDW File Browser 'upload.php'任意文件上传漏洞、WordPress 插件 Hungred Post Thumbnail 'hpt_file_upload.php'任意文件上传漏洞、WordPress 多个 CMSMasters 主题'upload.php'任意文件上传漏洞、WordPress 插件 TimThumb 跨站脚本漏洞、WordPress 插件 TimThumb 存在多个安全绕过漏洞、WordPress 插件 TimThumb 任意文件上传漏洞、WordPress 插件 TimThumb 信息泄露漏洞、WordPress 插件 TimThumb 拒绝服务漏洞等。其中，“WordPress 插件 PDW File Browser 'upload.php'任意文件上传漏洞”和“WordPress 插件 Hungred Post Thumbnail 'hpt_file_upload.php'任意文件上传漏洞”的综合评级均为“高危”，厂商尚未发布了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。

参考链接:

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16938

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16936

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16945

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16910

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16911

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16912

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16913

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16914

5、Kiwi Syslog Web Access SQL 注入漏洞

Kiwi Syslog 是一款用于集中管理的日志服务器。本周,该产品被披露存在一个综合评级为“高危”的 SQL 注入漏洞。由于 Kiwi Syslog Web Access 多个脚本未能正确处理 _TSM_HiddenField_和 _TSM_CombinedScripts_ 参数数据,攻击者利用漏洞可获得敏感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=CNVD-2012-16961

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-2012-16947	Carlo Gavazzi EOS-BOX SQL 注入漏洞	高	Carlo Gavazzi EOS-Box 1.0.0.1080_2.1.10 已经修复此漏洞,建议用户下载使用: http://www.carlogavazzi.com
CNVD-2012-16960	MyBB Profile Xbox Live ID Plugin 'xli'注入漏洞	高	暂无
CNVD-2012-16955	LemonLDAP::NG SAML XML 签名封装安全漏洞	高	LemonLDAP-NG 1.2.3 已经修复此漏洞,建议用户下载使用: http://jira.ow2.org/secure/attachment/11153/lemonldap-ng-saml-signature-verification.patch
CNVD-2012-16928	GIMP XWD 文件处理缓冲区溢出漏洞	高	用户可参考如下厂商提供补丁修复此漏洞: http://git.gnome.org/browse/gimp/commit/?id=2873262fccba12af144ed96ed91be144d92ff2e1

CNVD-2012-16937	Schoolhos CMS 'index.php'脚本 SQL 注入漏洞	高	暂无
CNVD-2012-16908	Real Networks RealPlayer RealAudio 非法指针漏洞	高	Real Networks RealPlayer 16.0.0.282 已经修复此漏洞，建议用户下载使用： http://service.real.com
CNVD-2012-16939	WHMCS 'googlecheckout.php' SQL 注入漏洞	高	暂无
CNVD-2012-16880	TWiki shell 命令执行漏洞	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://archives.neohapsis.com/archives/fulldisclosure/current/0157.html
CNVD-2012-16940	Joomla! Spider Calendar Lite 组件 'date' SQL 注入漏洞	高	暂无
CNVD-2012-16873	'tog-pegasus'哈希碰撞拒绝服务漏洞	高	pegasus 2.12 已经修复此漏洞，建议用户下载使用： http://bugzilla.openpegasus.org/show_bug.cgi?id=9374

表 3 部分高危漏洞列表

小结：本周，Adobe 和 IBM 的多款产品被披露存在多个漏洞，攻击者利用漏洞可获得敏感信息或执行任意代码。Drupal、WordPress 内容管理系统软件被披露存在多个漏洞，攻击者利用漏洞进一步发起篡改、后门攻击，或窃取用户敏感信息。本周，Kiwi Syslog 日志服务器被披露存在零日漏洞，建议采用相关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、Red Hat 布升级程序，修补 JBOSS 产品漏洞

JBOSS 是一款基于 J2EE 的开源应用服务器。本周，Red Hat 修补了 JBOSS 存在的安全绕过漏洞。攻击者利用漏洞可绕过安全限制执行未授权操作。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=26704

本周要闻速递

1. 三星手机漏洞可轻易获 root 权限

近日，来自国外最大安卓论坛消息，ID 为 Alephzain 的用户声称，其已在多款三星

Exynos 设备上发现了漏洞，利用漏洞可以访问设备全部的物理内存。这意味着，利用已公布的源码和这个漏洞，可轻易的访问设备的数据，同时，实现手机的 root。三星也察觉到了这个问题，承诺将尽快为用户提供修补漏洞的软件升级。

参考链接：<http://tech.xinmin.cn/2012/12/24/17800192.html>

2. JavaScript 漏洞或许会影响 Safari 用户

如果你最近在你的 iOS 6 设备上使用 Safari，你或许会注意到当访问部分与应用相关的网站时，会自动弹出一个新的应用广告。根据国外媒体 AppleInsider 的报道，即使你已经把弹出来的新广告关闭，但它们依然会在没经过你的同意之下通过重新启用 JavaScript 弄乱你的用户设置。Mac 软件安全公司表示：“目前这个问题尚未构成威胁，但是我们将会继续监视它，使它无法更进一步影响用户。”重新启用 JavaScript 事实上并不构成任何的隐私问题，因此我们可以将这个问题完全忽视。

参考链接：http://tech.ifeng.com/digi/mobile/soft/ios/detail_2012_12/22/20426273_0.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