

信息安全漏洞周报

2012 年 12 月 03 日-2012 年 12 月 09 日

2012 年 第 48 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 148 个，其中高危漏洞 33 个、中危漏洞 102 个、低危漏洞 13 个。上述漏洞中，可利用来实施远程攻击的漏洞有 131 个。本周收录的漏洞中，已有 90 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“Free Hosting Manager 'id'参数 SQL 注入漏洞”、“Oracle MySQL SELECT UpdateXML 命令拒绝服务漏洞”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 148 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、天融信、安天实验室等单位报送数量较多。此外，High-Tech Bridge Security Research Lab 及个人报送者向 CNVD 提交了 6 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	120	0
绿盟科技	40	0
安天实验室	44	0
恒安嘉新	19	0
天融信	33	0
安氏领信	6	0
知道创宇	3	0
High-Tech Bridge Security Research Lab	4	4

个人报送者	1	1
CNCERT	1	1
报送总计	271	6
录入总计	148（去重）	6

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Red Hat、Oracle、IBM、XenSource 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	Red Hat	12	8%
2	Oracle	8	5%
3	IBM	7	5%
4	XenSource	7	5%
5	Drupal	5	3%
6	Apache	4	3%
7	HP	4	3%
8	Qualcomm Innovation Center	3	2%
9	RSA	2	1%
10	ISC	1	1%
11	其它	95	64%

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 148 个漏洞。其中应用程序漏洞 103 个，WEB 应用漏洞 30 个，数据库漏洞 9 个，安全产品漏洞 3 个，网络设备漏洞 3 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	0
应用程序漏洞	103
WEB 应用漏洞	30
网络设备漏洞	3
安全产品漏洞	3
数据库漏洞	9

表 3 漏洞按影响类型统计表

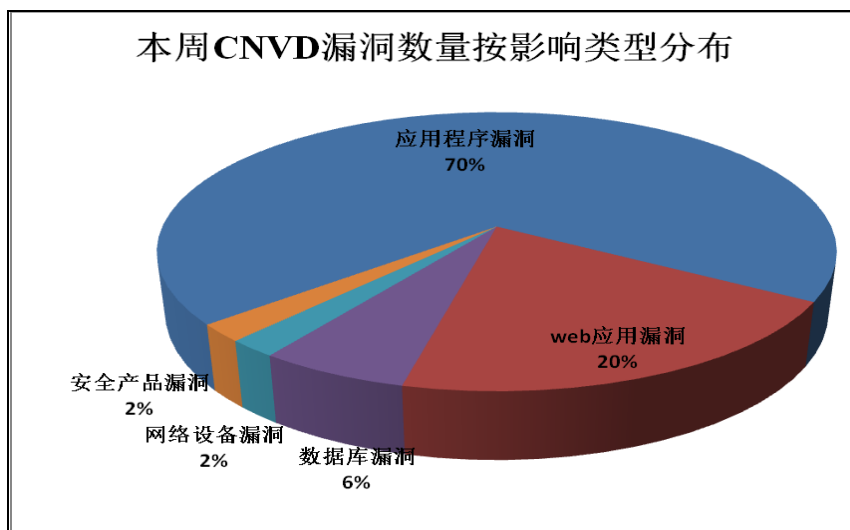


图 1 本周漏洞按影响类型分布

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：KYOCERA 非法 Email 拒绝服务漏洞、HP LaserJet/Color LaserJet 跨站脚本漏洞、HP LaserJet Pro 400 多功能打印机远程未授权访问漏洞。其中，“KYOCERA 非法 Email 拒绝服务漏洞”的综合评级为“高危”。相关厂商已经发布了漏洞修补程序。

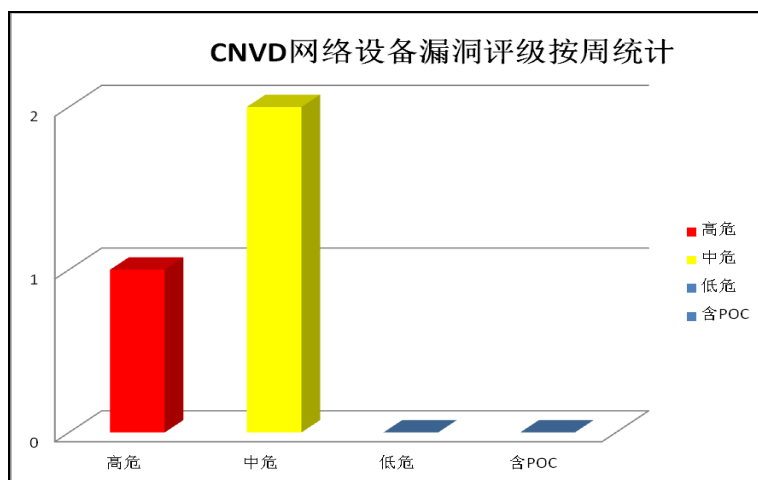


图 2 网络设备漏洞统计

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、IBM 产品安全漏洞

IBM WebSphere Message Broker 是一款企业服务总线(ESB)解决方案；IBM Lotus Symphony 是 IBM 公司推出的一款免费办公软件；IBM Tivoli Monitoring 用于提供基本

系统资源的监控特性，以检测系统瓶颈和潜在的问题。本周，上述产品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，发起跨站攻击，读取系统文件内容。

CNVD收录的相关漏洞包括：IBM Tivoli Monitoring HTTP监视控制台跨站脚本漏洞、IBM Lotus Symphony 'vclmi.dll'整数溢出漏洞、IBM Lotus Symphony数据泄露漏洞、IBM Lotus Symphony清单处理漏洞、IBM Lotus Symphony PPT文件存在漏洞、IBM WebSphere Portal theme组件目录遍历漏洞、IBM WebSphere Message Broker文件系统不安全文件权限漏洞。其中“IBM Lotus Symphony 'vclmi.dll'整数溢出漏洞”的综合评级为“高危”。目前，厂商已发布了漏洞修补程序。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-2012-16665

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16609

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16608

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16606

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16607

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16591

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16594

2、Oracle 产品安全漏洞

MySQL 是一款开源关系型数据库管理系统。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，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Oracle MySQL GRANT FILE 命令缓冲区溢出漏洞、Oracle MySQL Scanner/MySQL Server 远程漏洞、Oracle MySQL 账号提权漏洞、Oracle MySQL SELECT UpdateXML 命令拒绝服务漏洞、Oracle MySQL Server 用户枚举漏洞、Oracle MySQL Server 堆溢出漏洞、Oracle MySQL Server 权限提升漏洞。目前，厂商尚未发布相关漏洞的修补程序，且互联网上已经公开了攻击代码。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-2012-16635

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16643

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16641

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16634

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16639

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16637

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16638

3、N-able 产品安全漏洞

N-able N-central 是一款网络 and 系统管理应用解决方案。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可发起跨站攻击，获得敏感信息。

CNVD 收录的相关漏洞包括：N-able N-central 'URL'信息泄露漏洞、N-able N-central 不安全访问漏洞、N-able N-central 数据库破坏漏洞、N-able N-central 'openfire'信息泄露漏洞、N-able N-central 用户账户信息泄露漏洞、N-able N-central 跨站请求伪造漏洞。目前，厂商已发布了漏洞修补程序。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-2012-16654

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16650

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16651

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16652

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16653

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16655

4、HP 产品安全漏洞

HP Intelligent Management Center 是惠普公司发行的一款智能管理应用软件；HP LaserJet Pro 400 是一款激光打印机设备；HP Network Node Manager i 是一款网络服务智能插件 (iSPI)，用于进一步扩展现有软件的可用性功能。本周，上述 HP 产品被披露存在多个安全漏洞，攻击利用漏洞可获得未授权的访问，执行任意代码。

CNVD 收录的相关漏洞包括：HP Intelligent Management Center User Access Manager 任意代码执行漏洞、HP LaserJet Pro 400 多功能打印机远程未授权访问漏洞、HP Network Node Manager i 远程未授权访问漏洞。其中，“HP Intelligent Management Center User Access Manager 任意代码执行漏洞”的综合评级为“高危”，厂商已经发布了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=CNVD-2012-16693

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16695

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16696

5、Free Hosting Manager 'id'参数 SQL 注入漏洞

Free Hosting Manager 是一款开源 CPanel/WHM 管理系统。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 Free Hosting Manager packages.php 脚本未能正确过滤'id'参数，攻击者利用漏洞可进行 SQL 注入攻击，获得数据库信息。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-2012-16582

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-2012-16691	Ektron CMS 'XslCompiledTransform'类远程代码执行漏洞	高	Ektron CMS version 8.5 已经修复此漏洞, 建议用户下载使用: http://www.ektron.com
CNVD-2012-16700	Achievo SQL 注入漏洞	高	暂无
CNVD-2012-16699	ClipBucket 存在多个 SQL 注入漏洞	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://forums.clip-bucket.com/showthread.php?12527-Security-Fix-ClipBucket-2-6-SQL-Injections-fix-(Updated)
CNVD-2012-16680	Xen 'XENMEM_exchange'本地权限提升漏洞	高	Xen xsa29-4.1.patch 和 Xen xsa29-4.2-unstable.patch 已经修复此漏洞, 建议用户下载使用: http://lists.xen.org/archives/html/xen-announce/2012-12/bine8fz_3fsRs.bin http://lists.xen.org/archives/html/xen-announce/2012-12/bin8kM8Q8ogTn.bin
CNVD-2012-16672	Sourcefabric Newscoop 'f_email' SQL 注入漏洞	高	暂无
CNVD-2012-16660	bogofilter 堆内存破坏漏洞	高	用户可参考如下厂商提供的补丁程序: http://bogofilter.svn.sourceforge.net/viewvc/bogofilter?view=revision
CNVD-2012-16673	WordPress Nest Theme 'codigo' SQL 注入漏洞	高	暂无
CNVD-2012-16666	Opera Web Browser 内存破坏拒绝服务漏洞	高	暂无
CNVD-2012-16681	ISC BIND DNS64 畸型查询请求拒绝服务漏洞	高	ISC BIND 9.8.4-P1 或 9.9.2-P1 已经修复此漏洞, 建议用户下载使用: http://www.isc.org/downloads/all
CNVD-2012-16630	MyBB kingchat Plugin 'username'参数 SQL 注入漏洞	高	暂无

表 3 部分高危漏洞列表

小结： 本周，IBM 和 HP 公司的多款产品和 N-able N-central 软件被披露存在多个漏洞，攻击者利用漏洞可发起跨站攻击，拒绝服务攻击或执行任意代码。Free Hosting Manager 管理系统和 Oracle MySQL 数据库被披露存在多个零日漏洞，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。。

根据漏洞报送者提供的信息，CNVD 获知国内一款 CMS 软件 Xycms 采购信息发布系统存在远程命令执行等多个漏洞，攻击者利用漏洞可重置用户密码为默认密码，上传网站后门文件，取得网站服务器主机控制权。CNVD 已经着手协调厂商处置漏洞事件，待后续反馈更新。

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、ISC 布升级程序，修补 BIND 漏洞

ISC BIND 是一款 DNS 解析服务器软件。本周，ISC 修补了 BIND 存在拒绝服务漏洞。攻击者利用漏洞可构建特制的 DNS 查询触发 REQUIRE 断言，使服务程序崩溃。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=26111

本周要闻速递

1. Windows 8 发布安全更新修复系统漏洞

近日，微软公司推送了 11 月份安全更新，Windows 8、Windows RT 迎来了 6 个安全补丁。其中有 3 个严重级别的补丁需要 Windows 8 用户安装，它们修复了 Windows Shell、Windows 内核模式驱动程序和 .NET Framework 中的远程代码执行漏洞。安装这些补丁后，Windows 8 的版本也升级了，当前的最新版本号为 6.2.9200.16442。用户可以通过“Win + x”快捷键，在“运行”中输入“msinfo32”命令查看系统信息。早在今年 10 月初的时候，微软为 Windows 8 RTM 发布了一个累计更新 KB 2756872，将 Windows 8 RTM 版本号由 6.2.9200.16384 升级到了 6.2.9200.16420。

参考链接：http://www.chinadaily.com.cn/micro-reading/dzh/2012-12-09/content_7719343.html

2. Twitter 表示已修补短信攻击漏洞

Twitter 允许用户利用手机传送短信到 Twitter 的代表门号来使用许多指令，包含追踪、取消追踪、发布消息、转推信息、修改个人资料等。早期许多用户利用短信操作 Twitter，但在改用智能手机之后已经不再通过短信操作，却未取消设定。在部分国家 Twitter 与电信厂商合作使用特殊的短信号码，用户如果使用该电信厂商的号码，在

Twitter 帐号内设定手机号码之后，可以通过该短信号码操作。Facebook 及付款机制 Venmo 也有类似的问题，但在接获研究人员的报告之后，分别于 8 月及 11 月修补该问题，唯有 Twitter 尚未解决，因此研究人员决定直接公开此问题，Twitter 隔日(12 /4)以电子邮件表示问题已经解决。

参考链接：<http://site.qudong.com/2012/1206/131587.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