

信息安全漏洞周报

2012 年 11 月 12 日-2012 年 11 月 18 日

2012 年第 45 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 125 个，其中高危漏洞 46 个、中危漏洞 76 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 112 个。本周收录的漏洞中，已有 88 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“Narcissus 远程命令执行漏洞”、“ReciPHP 'id'参数 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 125 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，High-Tech Bridge Security Research 及一位个人报送者向 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	112	0
绿盟科技	84	0
安天实验室	36	0
天融信	24	0
安氏领信	9	0
恒安嘉新	9	0
High-Tech Bridge Security Research	8	8
个人报送者	1	1
报送总计	283	9
录入总计	125（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 Microsoft、IBM 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	Microsoft	18	14%
2	WordPress	12	10%
3	IBM	5	4%
4	Drupal	6	5%
5	TYPO3	4	3%
6	Bugzilla	4	3%
7	Samsung	2	1%
8	Joomla!	1	1%
9	Oracle	1	1%
10	Linux	1	1%
11	其它	71	57%

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 125 个漏洞。其中操作系统漏洞 5 个，应用程序漏洞 60 个，WEB 应用漏洞 56 个，数据库漏洞 2 个，网络设备漏洞 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	5
应用程序漏洞	60
WEB 应用漏洞	56
安全产品漏洞	1
网络设备漏洞	1
数据库漏洞	2

表 3 漏洞按影响类型统计表

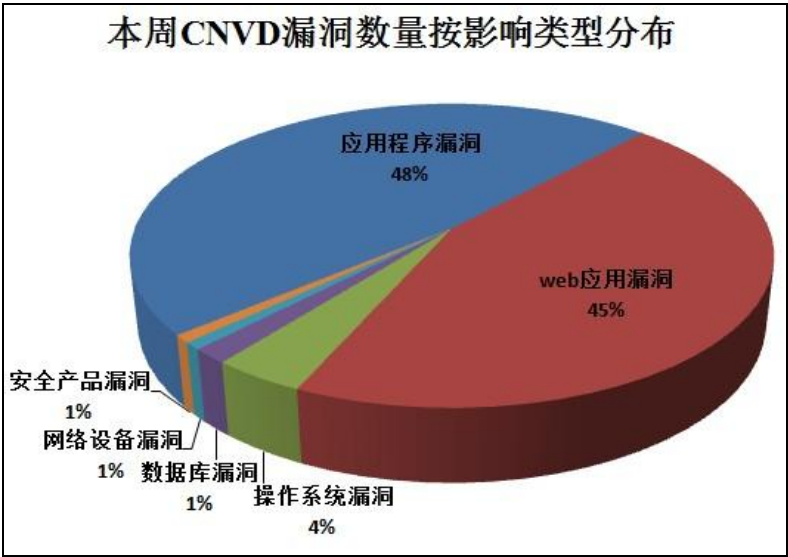


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 1 个网络设备漏洞：华为多个产品密码加密机制漏洞。该漏洞的综合评级为“中危”。目前，互联网上已经出现了针对该漏洞的攻击代码。厂商已经发布了漏洞修补程序。

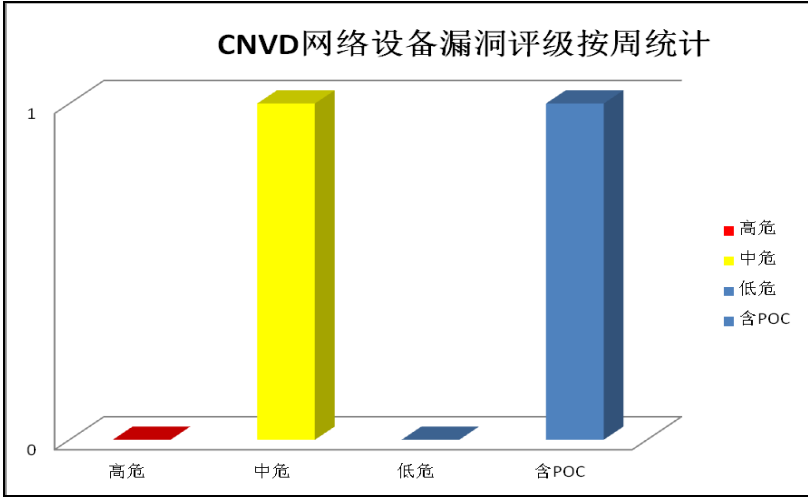


图 2 网络设备漏洞统计

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、Microsoft 产品安全漏洞

11 月 14 日，微软发布了 2012 年 11 月份的月度例行安全公告，共含 6 项更新，修复了 Microsoft Windows，Internet Explorer，Office，.NET Framework 多款产品中存在的

19 个安全漏洞。其中，4 项更新为最高级“严重”级别，其余两项为“重要”和“中等”。利用上述漏洞，攻击者可以远程执行代码，或窃取敏感信息。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。

CNVD 收录的相关漏洞包括：Microsoft Excel 内存破坏远程代码执行漏洞、Microsoft Excel 'SerAuxErrBar'堆溢出远程代码执行漏洞、Microsoft Windows Kernel 'Win32k.sys' 本地特权提升漏洞（CNVD-2012-15862、CNVD-2012-15863）、Microsoft .NET Framework 安全绕过漏洞、Microsoft Windows Briefcase 整数溢出远程代码执行漏洞、Microsoft .NET Framework 信息泄露漏洞、Microsoft .NET Framework DLL 加载代码执行漏洞等。上述漏洞的综合评级均为“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=61366
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=61365
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=61376
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=61377
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=61360
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=61375
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=61361
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=61362

2、IBM 产品安全漏洞

IBM WebSphere Application Server (WAS)是由 IBM 遵照开放标准，开发并发行的一款应用服务器；IBM Cognos 是一款集成商业智能（BI）和计划的解决方案；IBM WebSphere MQ 用于在企业中提供消息传输服务。本周，上述 IBM 产品被披露存在多个安全漏洞，攻击者利用漏洞可获得系统管理员权限，使应用程序崩溃，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：IBM WebSphere Application Server 远程权限提升漏洞、IBM Cognos BI 拒绝服务漏洞、IBM WebSphere MQ 队列管理器大型消息拒绝服务漏洞、IBM WebSphere Application Server 跨站请求伪造漏洞、IBM WebSphere Application Server 拒绝服务漏洞。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=61443
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=61442
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=61296
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=61240
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=61239

3、BabyGekko 安全漏洞

BabyGekko 是一款基于 PHP 的内容管理系统。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可劫持用户会话，获得数据库信息或控制应用系统。

CNVD 收录的相关漏洞包括：BabyGekko 跨站脚本漏洞、BabyGekko SQL 注入漏洞、BabyGekko 本地文件包含漏洞。其中，“BabyGekko SQL 注入漏洞”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=61415
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=61396
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=61397

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，攻击者利用漏洞可劫持用户会话，发起跨站和注入攻击，获得数据库等敏感信息。

CNVD 收录的相关漏洞包括：Wordpress 插件 Advanced Custom Fields 'acf_abspath' 参数远程文件包含漏洞、WordPress 插件 WP-Filebase 存在未明漏洞、WordPress 插件 Eco-annu 'eid'参数 SQL 注入漏洞、WordPress Kakao Theme 'ID'参数 SQL 注入漏洞、WordPress 插件 PHP Event Calendar 'cid'参数 SQL 注入漏洞、WordPress 插件 WP125 'editad'参数跨站脚本漏洞、WordPress 插件 WP125 'theid'参数跨站脚本漏洞、WordPress 插件 Buddystream 跨站脚本漏洞等。其中，“WordPress 插件 Eco-annu 'eid'参数 SQL 注入漏洞、WordPress Kakao Theme 'ID'参数 SQL 注入漏洞、WordPress 插件 PHP Event Calendar 'cid'参数 SQL 注入漏洞”的综合评级均为“高危”。目前，厂商已发布“WordPress 插件 WP125 'theid'参数跨站脚本漏洞、WordPress 插件 WP125 'editad'参数跨站脚本漏洞、WordPress 插件 WP-Filebase 存在未明漏洞、Wordpress 插件 Advanced Custom Fields 'acf_abspath'参数远程文件包含漏洞”的修复程序，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=61455
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=61460
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=61291
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=61292
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=61293
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=61294
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=61295
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=61457

5、Narcissus 远程命令执行漏洞

Narcissus 是一款基于 web 的在线图像生成软件。本周，该产品被披露存在一个综

合评级为“高危”的远程命令执行漏洞。攻击者利用漏洞可以以当前 WEB 用户权限执行任意指令，严重的可取得服务器主机控制权。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=61450

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-2012-15900	PHPCMS V9 getwebshell 漏洞	高	参考如下供应商提供的安全公告获得补丁信息: http://www.phpcms.cn
CNVD-2012-15901	ecshop gbk 宽字符注入漏洞	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://www.shopex.cn
CNVD-2012-15902	PHPMYWind 任意文件上传漏洞	高	暂无
CNVD-2012-15842	Eventy CMS 输入验证漏洞	高	暂无
CNVD-2012-15845	IDIC Blogs 'picture_upload.php'任意文件上传漏洞	高	暂无
CNVD-2012-15813	VMware Player/Workstation 不安全库加载漏洞	高	用户可参考如下厂商提供的安全公告获得补丁信息: http://www.vmware.com/security/advisories/VMSA-2012-0015.html
CNVD-2012-15826	Smadav 拒绝服务漏洞	高	暂无
CNVD-2012-15802	Intramaps SQL 注入漏洞	高	Intramaps 7.5.136 已经修复此漏洞，建议用户下载使用: http://www.mapsolutions.com.au/intramaps.aspx
CNVD-2012-15828	VBulletin vBay 模块 SQL 注入漏洞	高	暂无
CNVD-2012-15799	ESRI ArcGIS for Server 'where'表单字段 SQL 注入漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，微软发布了 2012 年 11 月份的月度例行安全公告，共含 6 项更新，修复了 Microsoft Windows, Internet Explorer, Office, .NET Framework 多款产品中存在的 19 个安全漏洞，包括 4 项标注最高风险等的更新；而 IBM 的多款产品被披露存在多个安全漏洞，有可能利用发起攻击获得系统管理权限。使用上述产品的企业和个人用户需及时更新，加强防护。

本周，BabyGekko、WordPress 及 PHPCMS v9、phpMywind 国内外网站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。此外，Narcissus 软件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、SAP 布升级程序，修补 NetWeaver 漏洞

SAP NetWeaver 是一款 SAP 业务套件解决方案。本周，SAP 修补了 NetWeaver 存在的多个漏洞。攻击者利用漏洞可构建恶意 Web 网页，诱使用户解析，执行恶意操作。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=25091
http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=25092

本周要闻速递

1. 微软发布 Surface 固件首次更新修复漏洞

近日，微软为其 SurfaceRT 平板电脑提供了首次更新。本次更新的大小仅有 400KB，但预计将能提升稳定性和性能。用户只需通过 Windows Update 并检查更新，即可进行升级，更新后需要重启 Surface。根据国外网站的测试人员称，升级之后，应用程序载入时间获得了提升，不过这次的更新暂没有解决音频播放不流畅的问题，同时更新中也修复了两个 Windows RT 的安全问题。

参考链接：http://www.chinadaily.com.cn/hqgj/jryw/2012-11-16/content_7527285.html

2. 苹果 iOS6.0 漏洞会导致音频流反复下载

有国外机构调查显示，苹果 iOS 6.0 系统下的音频流下载 AV Foundation framework 存在一个漏洞，它会导致设备反复发送下载音频文件的请求，造成流量浪费。该漏洞是由 Public Radio Exchange Labs (PRX) 最先发现。PRX 旗下的一款播客 (Podcast) 服务，在 iOS 6.0 平台上使用其服务时流量经常出现异常。

参考链接：<http://cd.qq.com/a/20121116/000099.htm>

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