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 15 日-2012 年 10 月 21 日　　2012 年 第41 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**高**。

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 229 个，其中高危漏洞 55 个、中危漏洞 125 个、低危漏洞 49 个。上述漏洞中，可利用来实施远程攻击的漏洞有 200 个。本周收录的漏洞中，已有 191 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“QQ Player 'quartz.dll'堆缓冲区溢出漏洞”、“BSW Gallery 'uploadpic.php'任意文件上传漏洞”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 8 家成员单位和多个合作伙伴报送了本周收录的全部 229 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、安天实验室、天融信等单位报送数量较多。此外，上海交通大学以及 High-Tech Bridge Security Research 向 CNVD 提交了 15 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
绿盟科技	155	1
启明星辰	196	0
安天实验室	32	0
天融信	57	0
恒安嘉新	12	0
安氏领信	10	0
知道创宇	5	5
东软	3	0
上海交通大学	2	2

个人报送者	1	1
High-Tech Bridge Security Research	13	13
报送总计	486	22
录入总计	229（去重）	22

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、WordPress、Drupal、Samsung 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	132	58%
2	WordPress	8	3%
3	Drupal	5	2%
4	Samsung	5	2%
5	visual tools	5	2%
6	GE Fanuc Automation, Inc.	3	1%
7	Mozilla	3	1%
8	Joomla!	3	1%
9	RedHat	1	1%
10	Novell	1	1%
11	其它	63	28%

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 229 个漏洞。其中操作系统漏洞 15 个，应用程序漏洞 148 个，WEB 应用漏洞 43 个，网络设备漏洞 4 个，数据库漏洞 17 个，安全产品漏洞 2 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	15
应用程序漏洞	148
WEB 应用漏洞	43
网络设备漏洞	4
安全产品漏洞	2
数据库漏洞	17

表 3 漏洞按影响类型统计表

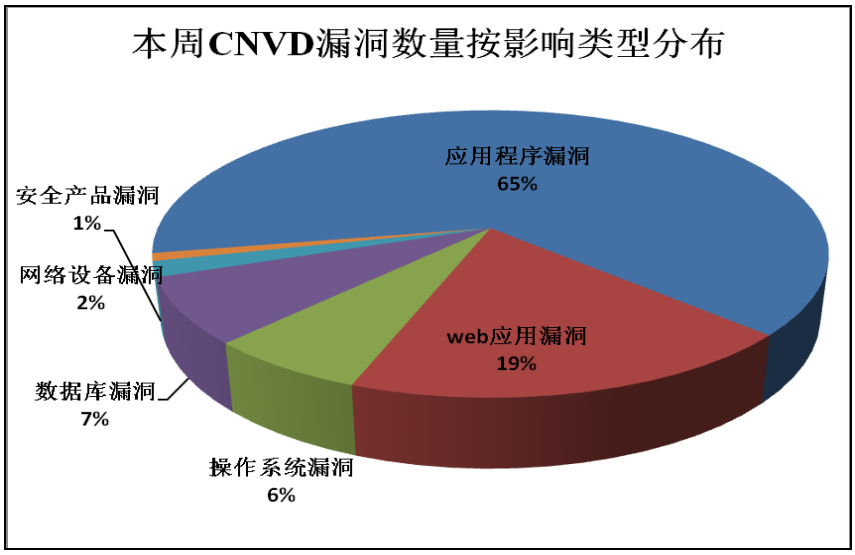

图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 4 个网络设备漏洞：BigPond Wireless Broadband Gateway 命令注入漏洞、BigPond Wireless Broadband Gateway 内置账户权限漏洞、P1 Modem 默认密码安全绕过漏洞、Legrand-003598/Bticino-F454 信息泄露漏洞。上述漏洞评级均为“中危”。其中，相关厂商已经修复了“Legrand-003598/Bticino-F454 信息泄露漏洞”。

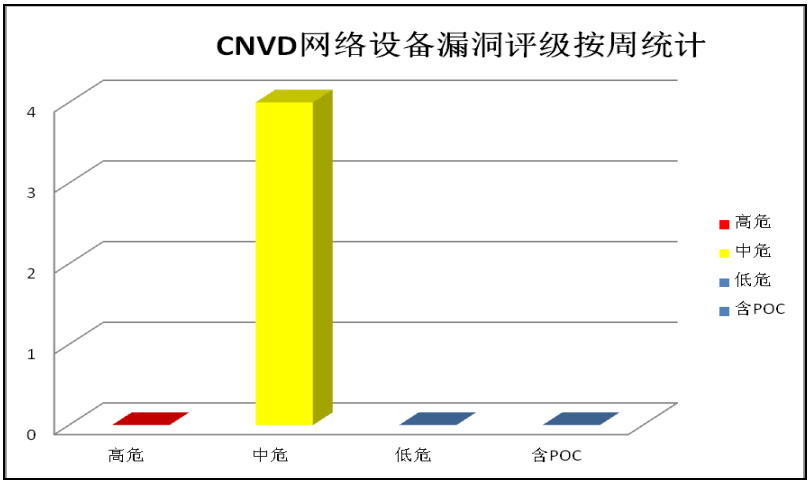

图 2 网络设备漏洞统计

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、Oracle 产品安全漏洞

近期，Oracle 发布了 2012 年第四季度的安全更新，修复了其多款产品存在的 139

个安全漏洞。产品涉及 Oracle 数据库（5 个）、中间件产品 Fusion Middleware（26 个）、供应链套装软件 Oracle Supply Chain Products Suite（9 个）、电子商务套装软件 Oracle E-Business Suite（9 个）、Industry Applications（2 个）、Financial Services（13 个）、Virtualization（2 个）、PeopleSoft 产品（9 个）、Java SE（30 个）、Oracle Siebel 托管型 CRM 软件（2 个）、Sun 系列产品（18 个）和 MySQL 数据库（14 个）。上述漏洞补丁中，24 个为高危漏洞补丁，116 个漏洞可被远程利用。CNVD 提醒广大 Oracle 用户，请及时下载补丁更新，避免引发漏洞相关的安全事件。

CNVD 收录的相关漏洞包括：Oracle Java SE 远程漏洞（CNVD-2012-15270、CNVD-2012-15273、CNVD-2012-15271、CNVD-2012-15222）、 Oracle Sun Solaris 本地漏洞（CNVD-2012-15292、CNVD-2012-15288）、Oracle Sun Solaris 远程漏洞（CNVD-2012-15302、CNVD-2012-15286）等。上述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=59540
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59543
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59562
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59572
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59541
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59556
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59558
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59489

2、 Mozilla 产品安全漏洞

Mozilla Firefox/SeaMonkey/Thunderbird 是 Mozilla 所发布的 WEB 浏览器/新闻组客户端/邮件客户端。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，发起跨站脚本攻击和浏览器点击劫持攻击。

CNVD 收录的相关漏洞包括：Mozilla Firefox/Thunderbird/SeaMonkey 页面跳转点击劫持漏洞、Mozilla Firefox/SeaMonkey/Thunderbird ChromeObjectWrapper 跨站脚本漏洞（CNVD-2012-15155）、Mozilla Firefox/SeaMonkey 信息泄露漏洞（CNVD-2012-15157）。其中，“Mozilla Firefox/SeaMonkey/Thunderbird ChromeObjectWrapper 跨站脚本漏洞（CNVD-2012-15155）”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=59315
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59216
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59198

3、Samsung 产品安全漏洞

Samsung Kies 是一款用于在 PC 端管理三星手机信息的应用软件（含驱动信息），使用 Samsung Kies 可将 PC 与三星手机连接，同步数据和查找新软件。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和修改任意文件及目录，或修改系统注册表当前用户的权限。

CNVD 收录的相关漏洞包括：Samsung Kies 空指针引用漏洞、Samsung Kies 任意文件修改漏洞、Samsung Kies 任意文件执行漏洞、Samsung Kies 任意注册表修改漏洞、Samsung Kies 任意目录修改漏洞。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=59436
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59439
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59437
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59442
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59440

4、airVision NVR 安全漏洞

airVision NVR 是一款视频监控系统软件。本周，该产品被披露存在两个漏洞，远程攻击者利用漏洞发起 SQL 注入攻击，获得数据库信息或控制应用系统；或以 WEB 权限查看系统文件内容。

CNVD 收录的相关漏洞包括：airVision NVR SQL 注入漏洞、airVision NVR 'views/file.php' Path 参数文件包含漏洞。其中，“airVision NVR SQL 注入漏洞”的综合评级为“高危”。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，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=59276
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=59275

5、BSW Gallery 'uploadpic.php'任意文件上传漏洞

BSW Gallery 是一款基于 PHP 的图库软件。本周，BSW Gallery 被披露存在一个综合评级为“高危”的文件上传漏洞。由于 BSW Gallery uploadpic.php 脚本未能正确过滤用户提交的输入，攻击者利用漏洞可上传任意文件，以 WEB 权限执行任意代码。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=59705

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-2012-15323	Videosmate Organizer 'admin/admin.php'安全绕过漏洞	高	暂无
CNVD-2012-15319	Subrion CMS 'plan_id' POST 参数 SQL 注入漏洞	高	Subrion 2.2.3 已经修复此漏洞，建议用户下载使用：http://www.subrion.com/forums/announcements/934-subrion-2-2-3-open-source-cms-core-available.html
CNVD-2012-15208	Sisfokol 文件上传漏洞	高	暂无
CNVD-2012-15210	GE Proficy Real-Time Information Portal 拒绝服务漏洞（CNVD-2012-15210）	高	用户可参考如下厂商提供的安全补丁：http://www.us-cert.gov/control_systems/pdf/ICSA-12-234-01.pdf
CNVD-2012-15321	AContent 'field' HTTP POST 参数 SQL 注入漏洞	高	用户可参考如下厂商提供的安全补丁：http://update.atutor.ca/acontent/patch/1_2/
CNVD-2012-15205	WordPress 插件 Spider Calendar SQL 注入漏洞	高	用户可联系供应商获得补丁信息：http://wordpress.org
CNVD-2012-15183	Novell ZENWorks Asset Management 信息泄露漏洞（CNVD-2012-15183）	高	暂无
CNVD-2012-15191	php168 CMS 'member/list.php' SQL 注入漏洞	高	暂无
CNVD-2012-15193	PBBoard 'Engine.class.php'参数 SQL 注入漏洞	高	暂无
CNVD-2012-15188	PHPCMS 'phpcmd/modules/wap/index.php' 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://www.phpcms.cn
CNVD-2012-15185	ContentDrome CMS SQL 注入漏洞	高	暂无

表 3 部分高危漏洞列表

本周，Oracle 发布了 2012 年第四季度的安全更新，修复了其多款产品存在的 139 个安全漏洞，为较大规模的一次安全更新，涉及 Oracle 公司多个产品的高危漏洞，企业和个人用户需及时进行更新部署。而 Samsung Kies、airVision NVR 以及 Mozilla 的多款产品也被披露存在多个安全漏洞，攻击者利用漏洞可获得软件目录或文件敏感信息，严重的还可以获得后台数据库信息或取得应用系统后台管理权。此外，BSW Gallery 图库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，国内一些广泛应用的网站内容管理系统软件，如：PHPCMS、PHP 168 等，被发现存在 SQL 注入高危漏洞，对网站用户信息安全和运行安全构成较为严重的威胁，一些软件厂商还尚未提供解决方案，建议企业和个人用户在网站服务器端先行加强对 SQL 注入的防范过滤。

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 Linux 漏洞

Red Hat 是一款基于 linux 内核的发行版本。本周，Red Hat 修补了 linux 存在的漏洞。本地攻击者可以利用此漏洞获得配置文件中的敏感信息。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=23742

本周要闻速递

1. iPhone5 内核漏洞

要在搭载 IOS6 系统 iPhone5 上实现完美越狱并不是一件容易的事情，随着 iOS 系统的成熟，苹果已经将越狱漏洞封锁得差不多，越狱也变得越来越艰难。今天 ChronicDevTeam 团队成员 Planetbeing 宣布 iPhone5 越狱已取得重大突破，他已经找到新的 iPhone5 内核漏洞用来越狱。目前 iPhone5 已经可以实现不完美越狱，但该方法需要用到开发者账号，不适合普通用户使用。

参考链接：http://info.tele.hc360.com/2012/10/220946402736.shtml

2. 部分 Android App 带有严重的 SSL 漏洞

来自两所德国大学的研究团队最近发布一项研究声称，在 Google Play Store 提供的最流行的免费 app 应用程序中，许多都可能带有导致 man-in-the-middle(MITM)攻击的漏洞，这将严重威胁到用户隐私。来自汉诺威和马尔堡大学的专家们对 Play store 中 13500 个最流行的免费软件进行了 SSL 和 TLS 漏洞研究。他们发现，1074 个 app 程序包含 SSL 特定代码，这些代码要么接受所有认证，要么接受所有认证主机名，由此成为潜在 MITM 攻击的漏洞。此外，科学家们还对 100 个 app 应用程序进行了手动审计，结果发现，由于 SSL 漏洞的存在，41 个程序对 MITM 攻击是开放的。专家们表示，漏洞 app 应用程序可能被利用，攻击者得以窃取高度敏感的用户信息，包括他们在 Facebook、WordPress、Twitter、Google、Yahoo，甚至网上银行的用户名和密码。专家表示，“Google's Play 市

场数据表明，目前，带有这种漏洞的 app 程序累积安装量在 3950 万~18500 万之间。实际安装数量可能会更大，因为这还没有包括其他安卓 app 市场的安装量。”
参考链接：http://www.cnbeta.com/articles/210670.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