国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2012 年 12 月 24 日-2012 年 12 月 30 日　　2012 年第 51 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 100 个，其中高危漏洞 42 个、中危漏洞 50 个、低危漏洞 8 个。上述漏洞中，可利用来实施远程攻击的漏洞有 95 个。本周收录的漏洞中，已有 47 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“Sony PC Companion 'DownloadURLToFile()'栈缓冲区溢出漏洞”、“MyBB HM_My Country Flags 插件'cnam' 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 7 家成员单位和多个合作伙伴报送了本周收录的全部 100 个漏洞。各单位报送情况如表 1 所示。其中，启明星辰、安天实验室等单位报送数量较多。此外，个人报送者向 CNVD 提交了 1 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	60	0
绿盟科技	30	0
安天实验室	47	0
恒安嘉新	23	0
天融信	31	0
知道创宇	14	0
东软	6	0
个人报送者	1	1
报送总计	212	1

录入总计	100（去重）	1

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、Android 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	Novell	5	5%
2	WordPress	4	4%
3	Drupal	4	4%
4	Cyclope	3	3%
5	MyBB	2	2%
6	Joomla!	1	1%
7	Linux	1	1%
8	IBM	1	1%
9	Microsoft	1	1%
10	EMC	1	1%
11	其它	77	77%

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 100 个漏洞。其中应用程序漏洞 59 个，WEB 应用漏洞 39 个，操作系统漏洞 1 个，网络设备漏洞 1 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	1
应用程序漏洞	59
WEB 应用漏洞	39
网络设备漏洞	1
数据库漏洞	0
安全产品漏洞	0

表 3 漏洞按影响类型统计表

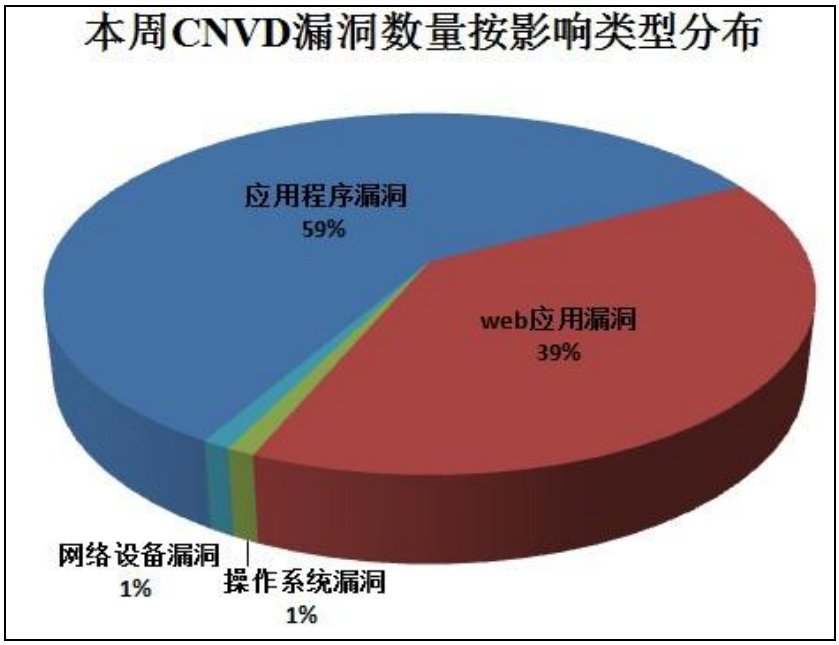

图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 1 个网络设备漏洞：BlackBerry PlayBook 存在未明信息泄露漏洞。且厂商已经发布了该漏洞修补程序。

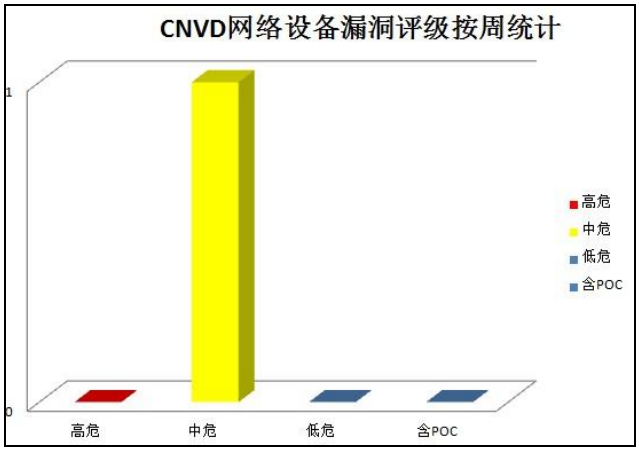

图 2 网络设备漏洞统计

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、SIEMENS 产品安全漏洞

SIEMENS SIMATIC S7-1200 是一款西门子开发的自动化应用产品。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拒绝服务攻击。

CNVD 收录的相关漏洞包括：SIEMENS SIMATIC SNMP 状态信息拒绝服务漏洞、SIEMENS SIMATIC TCP 报文拒绝服务漏洞。上述漏洞的综合评级均为“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-2012-18763

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-18765

2、Novell 产品安全漏洞

Novell iPrint Client 是一款允许用户向网络打印机发送文档的打印客户端程序；Novell eDirectory 是一款跨平台的目录服务软件。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或控制应用系统，执行任意代码，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Novell iPrint Client 'op-client-interface-version'远程代码执行漏洞、Novell eDirectory NCP 预验证缓冲区溢出漏洞、Novell eDirectory 授权机制绕过漏洞、Novell eDirectory 拒绝服务漏洞、Novell eDirectory 跨站脚本漏洞。其中，“Novell iPrint Client 'op-client-interface-version'远程代码执行漏洞”和“Novell eDirectory NCP 预验证缓冲区溢出漏洞”的综合评级均为“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-2012-18789

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-18787

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-18786

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-18784

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-18782

3、Yealink 产品安全漏洞

Yealink SIP-T20P IP Phone 是一款 IP 电话应用软件。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可使系统崩溃。

CNVD 收录的相关漏洞包括：Yealink SIP-T20P IP Phone Telnet 启用漏洞、Yealink SIP-T20P IP Phone shell 访问漏洞、Yealink SIP-T20P IP Phone 缓冲区溢出漏洞。其中，“Yealink SIP-T20P IP Phone 缓冲区溢出漏洞”的综合评级为“高危”。目前，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-2012-18775

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-18776

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-18777

4、CubeCart 安全漏洞

CubeCart 是一个电子商城购物车程序。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可以管理员权限控制网站服务器，构成信息泄露和运行安全风险。

CNVD 收录的相关漏洞包括：CubeCart 'redir'参数开放重定向漏洞、CubeCart 目录遍历漏洞、CubeCart 权限提升漏洞、CubeCart SQL 注入漏洞。其中，“CubeCart 权限提升漏洞”和“CubeCart SQL 注入漏洞”的综合评级均为“高危”，厂商已发布“CubeCart SQL 注入漏洞、CubeCart 目录遍历漏洞”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-2012-18801

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-18779

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-18780

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-18781

5、Sony PC Companion 'DownloadURLToFile()'栈缓冲区溢出漏洞

SonyPC Companion 是一款索尼手机管理工具。本周，该产品被披露存在一个综合评级为“高危”的缓冲区溢出漏洞。由于 SonyPC Companion 在处理分配给 Load 函数'File'项中的值时 PimData.dll 存在一个边界错误，攻击者利用漏洞可提交超长字符串触发栈缓冲区溢出，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=CNVD-2012-18767

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-2012-18824	WANem 存在多个远程命令执行漏洞	高	暂无
CNVD-2012-18829	tekno.Portal 'link.php' SQL 注入漏洞	高	暂无
CNVD-2012-18816	grep 超长行处理整数溢出漏洞	高	grep 2.11 及之后版本已经修复此漏洞，建议用户下载使用：http://www.gnu.org/software/grep
CNVD-2012-	WordPress Clockstone Theme	高	用户可参考如下供应商提供的安全公

18802	upload.php 任意文件上传漏洞		告获得补丁信息：http://www.attack-scanner.com/security/clockstone-and-other-various-cmsmasters-themes-flaw-patched/
CNVD-2012-18819	Ruby on Rails 'AuthLogic gem' SQL 注入漏洞	高	暂无
CNVD-2012-18792	Tiki Wiki CMS Groupware 'unserialize()'存在多个远程 PHP 代码执行漏洞	高	Tiki Wiki CMS Groupware 6.9 和 9.3 已经修复此漏洞，建议用户下载使用：http://info.tiki.org/Tiki Wiki CMS Groupware
CNVD-2012-18799	City Reviewer 'search.php'脚本 SQL 注入漏洞	高	暂无
CNVD-2012-18760	Computer Associates IdentityMinder 存在未明权限提升漏洞	高	用户可参考如下厂商提供的安全公告获得补丁信息：https://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID={FBA53B61-3A68-4506-9876-F845F6DD8A93}
CNVD-2012-18804	Feindura CMS 任意文件上传漏洞	高	暂无
CNVD-2012-18810	BRIM 'field'参数 SQL 注入漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，应用广泛的工业控制系统产品 SIEMENS SIMATIC S7-1200 被披露存在多个漏洞，攻击者利用漏洞可发起拒绝服务攻击，相关行业用户需及时进行修复。Yealink SIP-T20P IP Phone、Novell 多款产品、CubeCart 等企业用户软件产品被披露存在多个漏洞，攻击者利用漏洞可使系统崩溃，执行任意代码，取得设备或主机服务器控制权。本周， SonyPC Companion 被披露存在零日漏洞，有可能被利用发起挂马攻击，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、IBM 发布升级程序，修补 Tivoli NetView 产品漏洞

IBM Tivoli NetView 是一款网管软件。本周，IBM 修补了 Tivoli NetView 存在的权限提升漏洞。Unix 系统服务(USS)用户利用漏洞可以以 NetView 应用程序权限执行任意代码。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=26858

本周要闻速递

1. IE 6/7/8 曝 0day 漏洞

软件安全公司 FireEye 今日在其博客中表示，在对 12 月 21 日美国外交关系委员会（CFR）网站遭受黑客攻击的事件调查中发现了一个新的微软 Internet Explorer 浏览器 0day 漏洞。该漏洞只会影响到 IE 6/7/8 浏览器，IE 9/10 用户无需担心。这对于那些仍在使用 Windows XP 操作系统的用户来说无疑是一个最坏的消息，因为微软并未发布适用于该操作系统的 IE 9/10 浏览器。根据 FireEye 的介绍，黑客主要利用此次所发现的这个 0day 漏洞通过 JavaScripet 恶意代码加载名为“today.swf”的 Adobe Flash 文件来对 IE 浏览器实施 Heap Spray 攻击，并自动下载名为“xsainfo.jpg”的文件。虽然目前微软方面还未公布有关该漏洞的安全修复补丁，但 FireEye 建议用户可以通过使用微软增强减灾体验工具（EMET）以及禁用浏览器的 Flash ActiveX 和 Java 控件的运行来暂时降低遭遇攻击的风险。而比较彻底的解决办法则是安装更新版本的 Windows 操作系统和 IE 浏览器软件。

参考链接：http://tech.cnr.cn/list/201212/t20121230_511677626.html

2. 三星 S3 和 Note2 存高危漏洞

三星公司日前正式确认，在部分使用三星 CPU Exynos4210 或 4412 处理器的手机内核驱动上，确实存在上述漏洞及安全隐患，涉及范围主要是三星 Galaxy S3(盖世三)、Note2 及魅族 MX/MX2 等新款智能手机。造成这几款高端智能手机存在漏洞的主要原因在于三星提供的内核驱动程序存在安全隐患，其设备接口文件/dev/exynos-mem 未做适当的读写保护措施，导致黑客可通过该设备接口轻易操作手机内存，获取最高控制权限，来任意实施恶意行为。早前在这一漏洞公布之初，国外的 XDA 论坛上曾有网友提供了较为原始的简单解决办法，即直接通过将/dev/exynos-mem 文件设置成只读来临时解决这一问题，随后国内一些手机安全厂商也照此方法先后推出了自己的安全补丁，但据使用了该补丁的网友反映，这种比较初级的修补方法将会影响到部分手机的相机功能，甚至产生手机 HDMI 功能失效等副作用。

参考链接：http://news.china.com.cn/live/2012-12/27/content_17909305.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