

信息安全漏洞周报

2012 年 11 月 26 日-2012 年 12 月 02 日

2012 年第 47 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 188 个，其中高危漏洞 43 个、中危漏洞 132 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 170 个。本周收录的漏洞中，已有 91 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“SmartCMS 'index.php' SQL 注入漏洞”、“PHP-Nuke 'sid'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 188 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、安天实验室等单位报送数量较多。此外，上海交通大学及个人报送者向 CNVD 提交了 5 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	129	0
绿盟科技	83	0
安天实验室	38	0
恒安嘉新	58	0
天融信	29	0
安氏领信	6	0
上海交通大学	3	3
个人报送者	2	2
报送总计	348	5

录入总计	188（去重）	5
------	---------	---

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、Drupal、Wireshark、Google 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	17	9%
2	Drupal	10	5%
3	Wireshark	10	5%
4	Google	9	5%
5	Xen	7	4%
6	Mahara	7	4%
7	Bulb Security LLC	5	3%
8	ownCloud	4	2%
9	Greenstone	4	2%
10	IBM	3	2%
11	其它	112	59%

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 188 个漏洞。其中操作系统漏洞 5 个，应用程序漏洞 96 个，WEB 应用漏洞 86 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	5
应用程序漏洞	96
WEB 应用漏洞	86
网络设备漏洞	1
安全产品漏洞	0
数据库漏洞	0

表 3 漏洞按影响类型统计表

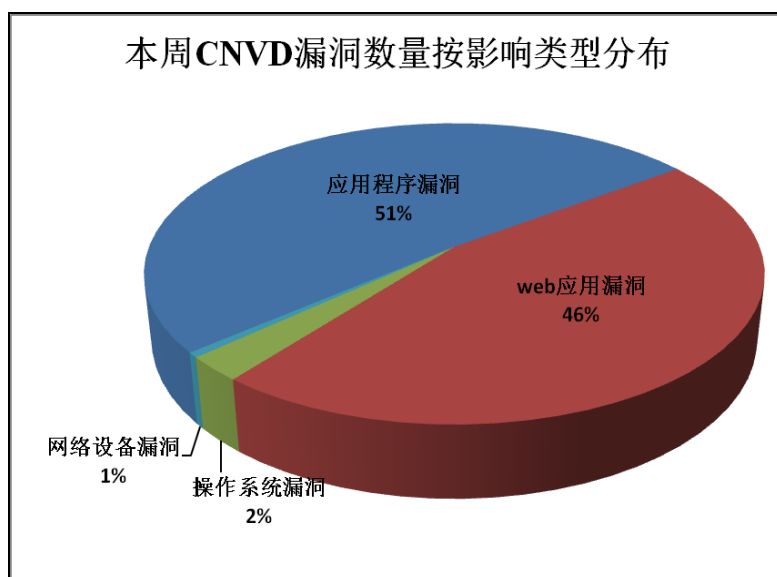


图 1 本周漏洞按影响类型分布

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：Samsung 打印固件后门未授权访问漏洞。该漏洞的综合评级为“高危”。目前，相关厂商已经发布了漏洞修补程序。

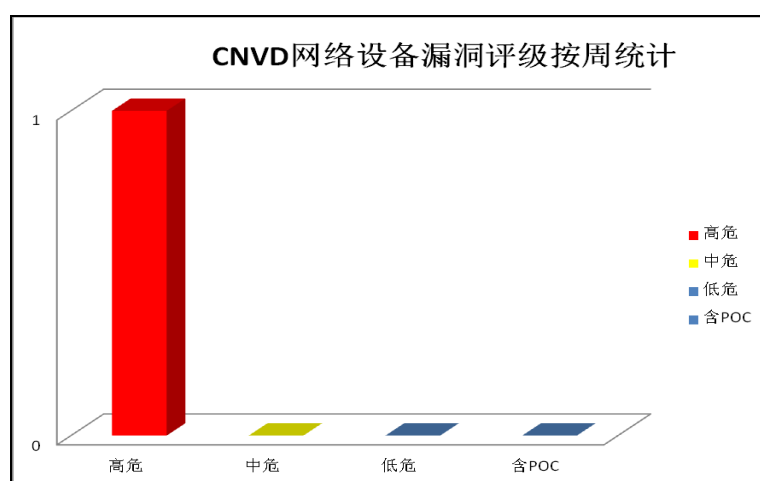


图 2 网络设备漏洞统计

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、Google 产品安全漏洞

Google Chrome 是一款开源的 WEB 浏览器；Google Cityhash 提供了字符串的 hash 函数实现。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可构建恶意 WEB 页，诱使用户解析，执行任意代码或发起拒绝服务攻击。

CNVD收录的相关漏洞包括：Google CityHash哈希碰撞拒绝服务漏洞、Google Chrome分块编码浏览器崩溃漏洞、Google Chrome SVG过滤器内存错误引用漏洞、Google Chrome Skia越界读漏洞（CNVD-2012-16404）、Google Chrome libxml缓冲区下溢漏洞、Google Chrome输入元素处理漏洞、Google Chrome打印内存错误引用漏洞。其中“Google Chrome打印内存错误引用漏洞、Google Chrome输入元素处理漏洞、Google Chrome libxml缓冲区下溢漏洞、Google Chrome SVG过滤器内存错误引用漏洞”的综合评级均为“高危”。除“Google CityHash哈希碰撞拒绝服务漏洞”外，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-2012-16498

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16407

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16409

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16404

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16383

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16387

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16385

2、Moodle 安全漏洞

Moodle 是一款开源的网络教学应用程序。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可通过高级搜索绕过限制，上传并执行文件。

CNVD 收录的相关漏洞包括：Moodle 文件上传漏洞、Moodle 'lib/formslib.php'访问限制绕过漏洞、Moodle 绕过限制读取敏感信息漏洞、Moodle 安全绕过信息读取漏洞、Moodle 'moodle/role:manage'安全绕过漏洞、Moodle 访问其他用户 Dropbox 漏洞。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-2012-16107

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16105

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16106

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16109

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16110

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16103

3、Xen 安全漏洞

Xen 是一款开放源代码的虚拟机监视器。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使系统崩溃或执行任意代码。

CNVD 收录的相关漏洞包括：Xen Transcendent Memory 整数溢出漏洞、Xen 系统崩溃漏洞、Xen 'do_tmem_op'函数拒绝服务漏洞、Xen 'do_tmem_get'函数拒绝服务漏洞、Xen 'do_tmem_control'函数权限提升漏洞、Xen Transcendent Memory 拒绝服务漏洞、Xen 'do_tmem_destroy_pool'函数拒绝服务漏洞。目前，厂商尚未发布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-2012-16125

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16131

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16122

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16123

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16126

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16128

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16130

4、Mahara 安全漏洞

Mahara 是一个开源的社会化网络应用软件，提供电子文件夹、网络日志、履历表生成器以及 SNS 等应用功能。本周，该产品被披露存在多个安全漏洞，攻击利用漏洞可获得敏感信息或劫持用户会话。

CNVD 收录的相关漏洞包括：Mahara 'query'跨站脚本漏洞、Mahara 点击劫持漏洞、Mahara 任意文件读取漏洞、Mahara 'xhtml'跨站脚本漏洞、Mahara 任意程序执行漏洞、Mahara 'artefact/file/'跨站脚本漏洞、Mahara 'CSV'跨站脚本漏洞。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-2012-16389

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16384

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16379

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16381

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16382

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16386

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16391

5、SmartCMS 'index.php' SQL 注入漏洞

SmartCMS 是一款网站内容管理系统软件。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 SmartCMS 'index.php'未能过滤'idx'参数数据，远程攻击者利用漏洞可进行 SQL 注入攻击，获得数据库敏感信息。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-2012-16397

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-2012-16482	Piwik 被入侵源包被植入后门漏洞	高	用户可联系厂商重新安装和下载 Piwik: http://piwik.org/
CNVD-2012-16479	razorCMS 文件和目录验证绕过漏洞	高	Morgan Integrated Systems razorCMS 1.2.1 STABLE 已经修复此漏洞, 建议用户下载使用: http://razorcms.co.uk/
CNVD-2012-16474	YABSoft Advanced Image Hosting Script 'view_comments.php' SQL 注入漏洞	高	暂无
CNVD-2012-16502	MobileCartly 'savepage.php'任意文件写入漏洞	高	暂无
CNVD-2012-16544	OSClass 'oc-admin/ajax/ajax.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://osclass.org/blog/2012/01/16/osclass-2-3-5/
CNVD-2012-16522	op5 Monitor 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.op5.com/
CNVD-2012-16542	ASUS Net4Switch 'ipswcom.dll' ActiveX 远程缓冲区溢出漏洞	高	暂无
CNVD-2012-16547	concrete5 存在多个漏洞	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.concrete5.org/
CNVD-2012-16500	MobileCartly 远程文件上传漏洞	高	暂无
CNVD-2012-16408	Apple OSX 驱动渲染破坏漏洞	高	Google Chrome 23.0.1271.91 已经修复此漏洞, 建议用户下载使用: https://chrome.google.com

表 3 部分高危漏洞列表

小结: 本周, 应用广泛的浏览器软件 Google Chrome 以及 Linux 平台下虚拟机软件 Xen 被披露存在多个漏洞, 攻击者利用漏洞可执行任意代码, 有可能被利用发起大规模

模挂马攻击，或攻击相关主机操作系统。而 Moodle 和 Mahara 等面向教育机构和社交网络的应用软件被披露存在多个安全漏洞，利用漏洞可获得敏感信息或上传执行文件。

此外，SmartCMS 系统以及涉及国内用户较广的 ASUS Net4Switch 华硕电脑网络管理软件被披露存在零日漏洞，可以导致主机拒绝服务或取得主机权限，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。本周值得关注的还有开源网站访问统计系统软件 Piwik 官方网站源码包被植入后门的安全事件，11 月 26 日当天下载部署相关源码包的用户应及时更换软件，排查后门隐患。

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、EMC 布升级程序，修补 Smarts Network Configuration Manager 漏洞

EMC Smarts Network Configuration Manager 是一款网络配置和变更管理软件。本周，EMC 修补了 Smarts Network Configuration Manager 存在的多个漏洞。攻击者利用漏洞对密码进行解密，获得数据库信息。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=25646
http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=25647

本周要闻速递

1. Xbox 主机更新修正多处服务漏洞及错误

微软表示已经为 Xbox 360 游戏主机提供了新的不定期软件更新来修复 SmartGlass 服务目前所存在的一直问题。本次更新修复了诸如用户通过 Xbox 360 启动 SmartGlass 播放列表时文件名称显示不正确，Xbox Video 字幕功能以及 Xbox Muisc 服务等一些已知的问题和漏洞。此次更新将是强制性的，用户会在登录 Xbox LIVE 时收到更新提示，如果你已经登录到了 Xbox LIVE 当中，那么你的账号将会被迫暂时下线，并在完成更新后重新上线，整个过程只需短短的几分钟时间。

参考链接：<http://game.dbw.cn/system/2012/11/29/054406767.shtml>

2. 三星打印机被曝存安全漏洞

北京时间 11 月 29 日消息，据美国计算机紧急响应小组（US-CERT）发布报告称，由三星制造的三星打印机和部分戴尔品牌的打印机存在一个硬编码帐户，该帐户可致黑客入侵设备并访问设备上的敏感信息。报告称，该后门管理员帐户被硬编码在打印机固件中，可被黑客用于更改打印机配置，获取敏感信息，如设备和网络信息，或通过执行恶意代码发动一步攻击等。据悉，硬编码帐户无需验证，可以通过打印机的简单网络

管理协议（以下简称“SNMP”）访问，甚至是在 SNMP 被禁用的情况下。“未经身份验证的远程攻击者可以特权管理员身份访问存在问题的设备，且可造成更多影响，其中包括：能够更改设备配置、访问敏感信息（比如设备和网络信息，安全认证以及传递到打印机的信息），并能够利用执行任意代码实施进一步的攻击”。据了解，不仅三星品牌的打印机存在该后门管理员帐户，由三星制造的戴尔品牌打印机同样存在该问题。去年，哥伦比亚大学两名研究人员曾在惠普 LaserJet 打印机中发现严重安全漏洞，允许黑客完全控制打印机。

参考链接：http://www.chinadaily.com.cn/hqcj/xfly/2012-11-29/content_7634086.html

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