

信息安全漏洞周报

2012 年 10 月 29 日-2012 年 11 月 04 日

2012 年第 43 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**低**。

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 113 个，其中高危漏洞 32 个、中危漏洞 79 个、低危漏洞 2 个。上述漏洞中，可利用来实施远程攻击的漏洞有 106 个。本周收录的漏洞中，已有 55 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“Microsoft Office Excel 2010 内存破坏拒绝服务漏洞”、“TP-LINK TL-WR841N 路由器本地文件包含漏洞”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 113 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 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	122	0
绿盟科技	85	0
安天实验室	35	0
天融信	17	0
恒安嘉新	26	0
安氏领信	7	0
东软	6	0
High-Tech Bridge Security Research	2	2
个人报送者	4	4
报送总计	304	6
录入总计	113（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 Wordpress、Drupal、Microsoft 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	16	14%
2	Drupal	15	13%
3	Best Practical Solutions	6	5%
4	Layton	6	5%
5	Microsoft	5	4%
6	Apple	3	3%
7	Mozilla	3	3%
8	TYPO3	2	2%
9	Cisco	2	2%
10	Linux	1	1%
11	其它	54	48%

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 113 个漏洞。其中操作系统漏洞 4 个，应用程序漏洞 39 个，WEB 应用漏洞 65 个，网络设备漏洞 5 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	4
应用程序漏洞	39
WEB 应用漏洞	65
网络设备漏洞	5
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

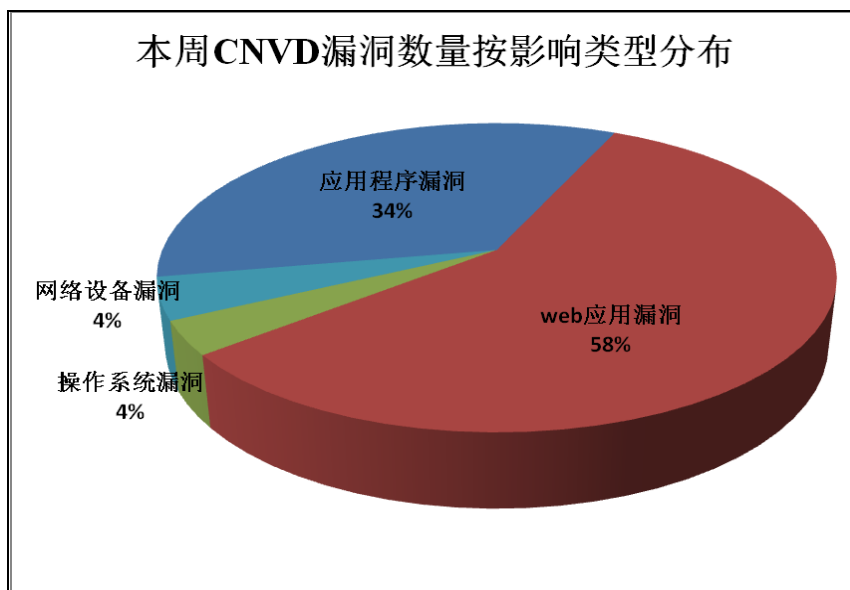


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 5 个网络设备漏洞：TP-LINK TL-WR841N 路由器本地文件包含漏洞、D-Link Wireless N300 云路由器 CAPTCHA 处理缓冲区溢出漏洞、Linksys WAP4400N SNMPv3 组件存在未明漏洞、NETGEAR NTV300 NeoTV 无线 SSID 系统调用注入任意命令执行漏洞、NETGEAR NTV300 NeoTV 默认未加密 root 账户漏洞。其中，“D-Link Wireless N300 云路由器 CAPTCHA 处理缓冲区溢出漏洞”和“Linksys WAP4400N SNMPv3 组件存在未明漏洞”的综合评级均为“高危”。目前，互联网上已经出现了针对“TP-LINK TL-WR841N 路由器本地文件包含漏洞”和“D-Link Wireless N300 云路由器 CAPTCHA 处理缓冲区溢出漏洞”的攻击代码。

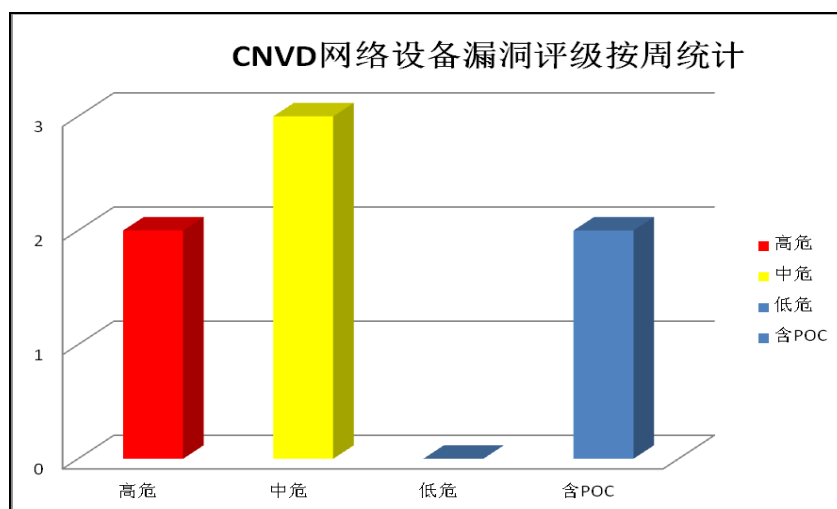


图 2 网络设备漏洞统计



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

Microsoft Virtual PC 是一款虚拟机软件；Microsoft Excel 是一款微软开发的电子表格处理程序；Microsoft Office Publisher 是一款微软提供的桌面出版应用软件；Microsoft Paint 是一款 windows 系统自带的画图工具；Microsoft Windows Help program 是一款 windows 系统帮助程序。本周，上述微软产品被披露存在多个安全漏洞，攻击者利用漏洞可使设备崩溃，发起拒绝服务攻击，执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Virtual PC 2007 特制 X86 指令序列处理本地拒绝服务漏洞、Microsoft Office Excel 2010 内存破坏拒绝服务漏洞、Microsoft Office Publisher '.pub'文件拒绝服务漏洞、Microsoft Paint '.bmp'文件拒绝服务漏洞、Microsoft Windows Help Viewer 内存破坏拒绝服务漏洞。其中，除“Microsoft Virtual PC 2007 特制 X86 指令序列处理本地拒绝服务漏洞”外，其余漏洞的综合评级均为“高危”。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=60476
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60198
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60199
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60200
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60201

2、Drupal 模块安全漏洞

Drupal 是一款基于 PHP 的内容管理系统。本周，该系统的多个模块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劫持用户会话，或重定向用户到任意 WEB 页，发起钓鱼攻击。

CNVD 收录的相关漏洞包括：Drupal Location 模块安全绕过漏洞、Drupal Excluded Users 模块跨站脚本漏洞、Drupal Secure Login 模块重定向漏洞、Drupal Email Field 模块信息泄露漏洞、Drupal Mime Mail 模块安全绕过漏洞、Drupal Announcements 模块安全绕过漏洞、Drupal Commons 模块安全绕过敏感信息泄露漏洞、Drupal Custom Publishing Options 模块跨站脚本漏洞等。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=60358
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60363
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60359
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60368

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60366

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60369

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60357

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60367

3、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。

CNVD 收录的相关漏洞包括：Mozilla Firefox/SeaMonkey/Thunderbird 'CheckURL()' 函数跨站脚本漏洞、Mozilla Firefox/SeaMonkey/Thunderbird 'valueOf'方法跨站脚本漏洞、Mozilla Firefox/SeaMonkey/Thunderbird Location 对象安全绕过漏洞。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=60203

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60202

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60204

4、Apple 产品安全漏洞

Apple iOS 是一款苹果公司开发的移动设备上的操作系统。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可获得敏感信息，执行任意代码。

CNVD 收录的相关漏洞包括：Apple iOS API 信息泄露漏洞、Apple iOS Passbook pass 本地安全绕过漏洞、Apple iOS WebKit 远程代码执行漏洞。其中，“Apple iOS WebKit 远程代码执行漏洞”的综合评级为“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=60415

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60435

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60495

5、TP-LINK TL-WR841N 路由器本地文件包含漏洞

TP-LINK TL-WR841N 是一款家用型无线路由器设备。本周，TP-LINK TL-WR841N 路由器被披露存在一个本地文件包含漏洞。攻击者在取得一定管理权限后利用漏洞可以查看设备固件系统文件内容。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=60206

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-2012-15562	Awstats awredir.pl 存在未明漏洞	高	AWStats 7.1 已经修复此漏洞，建议用户下载使用： http://awstats.sourceforge.net
CNVD-2012-15577	OrangeHRM 'sortField'参数 SQL 注入漏洞	高	OrangeHRM 2.7.1 已经修复此漏洞，建议用户下载使用： http://www.orangehrm.com/download.php
CNVD-2012-15587	Cisco Prime 数据中心网络管理器远程命令执行漏洞	高	Cisco Prime Data Center Network Manager 6.1(1)已经修复此漏洞，建议用户下载使用： http://www.cisco.com/cisco/software/navigator.html
CNVD-2012-15542	D-Link Wireless N300 云路由器 CAPTCHA 处理缓冲区溢出漏洞	高	暂无
CNVD-2012-15544	Real Networks RealPlayer '.3g2'文件写访问冲突内存破坏漏洞	高	暂无
CNVD-2012-15549	TYPO3 Formhandler Extension SQL 注入漏洞	高	TYPO3 Formhandler Extension 1.4.1 版本已修改此漏洞，建议用户下载使用： http://typo3.org/
CNVD-2012-15528	Arora 'wintab32.dll' DLL 装载任意代码执行漏洞	高	暂无
CNVD-2012-15526	piafhms 'bills.php' SQL 注入漏洞	高	暂无
CNVD-2012-15525	libunity-webapps 内存错误引用内存破坏漏洞	高	libunity-webapps 2.3.3 版本已修改此漏洞，建议用户下载使用： https://launchpad.net/libunity-webapps
CNVD-2012-15538	Real Networks RealPlayer 远程栈缓冲区溢出漏洞	高	暂无

表 3 部分高危漏洞列表

本周，Apple iOS 以及 Microsoft 的多款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，执行任意代码或发起拒绝服务攻击。Mozilla 的多款产品以及 Drupal 多个模块也被披露存在多个漏洞，攻击者利用漏洞可获得敏感信息或劫持用户会话，发起跨站脚本攻击或钓鱼攻击。TP-LINK TL-WR841N 无线路由器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。



CNVD 整理和发布以下重要安全修补信息。

1、Linux 布升级程序，修补 Kernel 漏洞

Linux 是一款开源的操作系统。本周，Linux 修补了 Kernel 存在的漏洞。本地非特权用户可利用漏洞使系统崩溃。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=24494

本周要闻速递

1. 谷歌证实所有 Android 版本均存短信欺诈漏洞

据国外媒体报道，北卡罗来纳州州立大学（NC State University）研究员日前在进行一项有关智能手机的研究项目中发现了一个存在于 Android 平台的“短信欺诈”（Smishing）漏洞。据悉，该漏洞可以允许应用在 Android 平台上进行短信伪装，且在所有版本的 Android 软件中都存在这一漏洞。这一漏洞可以令恶意应用在不需要用户任何许可的前提下进行攻击。研究员透露，谷歌告诉他们“将在未来的 Android 系统升级中修复这一漏洞。”到目前为止，谷歌尚没有收到有用户因为该漏洞而受到攻击的报告。

参考链接：http://tech.qq.com/a/20121105/000141.htm? A_C_21=13864

2. 泄露 132 万 Facebook 账户的漏洞暴露

Facebook 已经迅速地关闭了一个漏洞：没有密码就能访问账户。漏洞暴露后被发布到了黑客新闻网站上。消息包含一个搜索字符串，在谷歌上搜索时，可以搜索到可以链接到 132 万 Facebook 账户的一个列表。点击一个登录账户的链接不需要密码，所有的链接暴露了 Facebook 用户的电子邮件地址。Facebook 方面又称：“我们一直都有通过提供一个额外的安全层来保护在这些私人链接，但我们已经禁用了这项的功能并最近开始修正使用这个功能的这些账户。”

参考链接：<http://mobile.163.com/12/1105/13/8FI4GO540011665S.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