

信息安全漏洞周报

2012 年 12 月 10 日-2012 年 12 月 16 日

2012 年第 49 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 138 个，其中高危漏洞 52 个、中危漏洞 75 个、低危漏洞 11 个。上述漏洞中，可利用来实施远程攻击的漏洞有 123 个。本周收录的漏洞中，已有 73 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“VLC Media Player 'swf'文件栈缓冲区溢出漏洞”、“MyBB DyMy User Agent 插件 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 138 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、恒安嘉新等单位报送数量较多。此外，奇虎 360、High-Tech Bridge Security Research Lab、JVN 及个人报送者向 CNVD 提交了 7 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	93	0
绿盟科技	74	0
安天实验室	39	0
恒安嘉新	58	0
天融信	39	0
东软	1	0
奇虎 360	1	1
High-Tech Bridge Security Research Lab	1	1

个人报送者	1	1
JVN	4	4
报送总计	311	7
录入总计	138（去重）	7

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、MyBB、Adobe、Cisco 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	10	7%
2	MyBB	8	6%
3	Adobe	6	4%
4	Cisco	6	4%
5	Joomla!	4	3%
6	Huawei	3	2%
7	Symantec	3	2%
8	Citrix	2	1%
9	Ubuntu	2	1%
10	HP	2	1%
11	其它	91	69%

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 138 个漏洞。其中应用程序漏洞 75 个，WEB 应用漏洞 37 个，操作系统漏洞 13 个，网络设备漏洞 13 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	13
应用程序漏洞	75
WEB 应用漏洞	37
网络设备漏洞	13
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

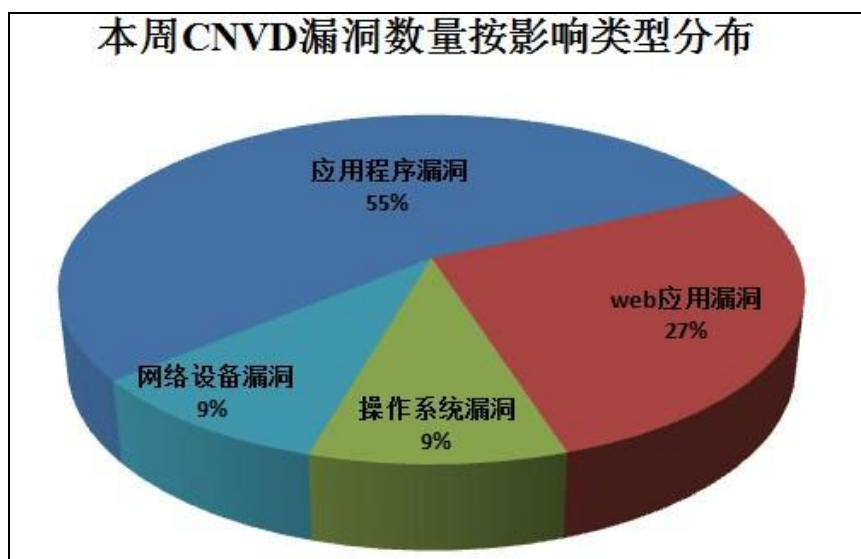


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 13 个网络设备漏洞：Cisco DPC2420 配置文件下载漏洞、Cisco DPC2420 文件泄露漏洞、Cisco DPC2420 路由器登录验证漏洞、Mesh OS 不充分熵漏洞、UPnP 设备便携式 SDK unique_service_name()缓冲区溢出漏洞、D-Link DSL2730U Telnet Shell 远程命令注入漏洞、Cisco Wireless LAN Controller 拒绝服务漏洞、Cisco Wireless LAN Controller 跨站请求伪造漏洞、Cisco Wireless LAN Controller 跨站脚本漏洞、Huawei E585 pocket wifi 2 device 授权验证绕过漏洞、Huawei E585 pocket wifi 2 device 目录遍历漏洞、Huawei E585 pocket wifi 2 device 拒绝服务漏洞、Samsung Smart Tv 附带存储设备读取漏洞。

其中，“UPnP 设备便携式 SDK unique_service_name()缓冲区溢出漏洞、Huawei E585 pocket wifi 2 device 目录遍历漏洞、Samsung Smart Tv 附带存储设备读取漏洞”的综合评级均为“高危”。目前，互联网上已经出现了针对“Cisco Wireless LAN Controller 拒绝服务漏洞、Cisco Wireless LAN Controller 跨站请求伪造漏洞、Cisco Wireless LAN Controller 跨站脚本漏洞、Huawei E585 pocket wifi 2 device 目录遍历漏洞”的攻击代码。相关厂商已经发布了漏洞修补程序。

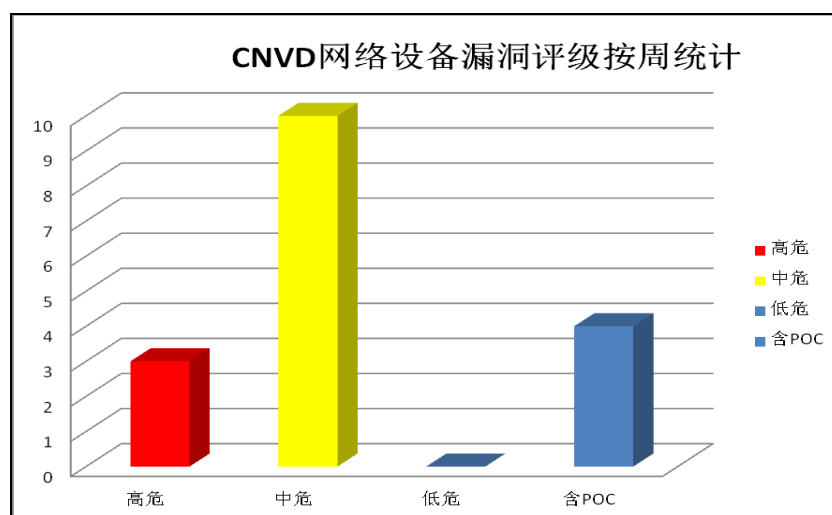


图 2 网络设备漏洞统计

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、Adobe 产品安全漏洞

本周，Adobe 发布了 APSB12-26 号和 APSB12-27 号安全公告，用于修复 ColdFusion、Flash Player、AIR 产品存在的多个安全漏洞。上述漏洞影响 Windows、Macintosh、Android、Linux、UNIX 和 SDK 多个平台。利用漏洞，攻击者可以构建恶意 WEB 页，诱使用户解析，绕过安全限制或以应用程序上下文执行任意代码。CNVD 提醒广大 Adobe 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：Adobe ColdFusion 安全绕过漏洞、Adobe Flash Player/AIR 远程缓冲区溢出漏洞、Adobe Flash Player/AIR 远程整数溢出漏洞、Adobe Flash Player/AIR 远程内存破坏漏洞。除“Adobe ColdFusion 安全绕过漏洞”外，其余漏洞的综合评级均为“高危”。

参考链接：

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16785

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16787

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16789

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16791

2、Microsoft 产品安全漏洞

本周，微软发布了 2012 年 12 月份的月度例行安全公告，共含 7 项更新，修复了涉及 Microsoft Windows、Internet Explorer、Office、Server 软件（Exchange Server、SharePoint Server、Office Web Apps）多款产品中存在的多个安全漏洞。其中，5 项更新为最高级“严重”级别，其余两项为“重要”。利用上述漏洞，攻击者可以远程执行代码，或绕过安

全限制。

CNVD 收录的相关漏洞包括：Microsoft Exchange Server RSS 种子远程拒绝服务漏洞、Microsoft Internet Explorer CMarkup 内存错误引用远程代码执行漏洞、Microsoft Internet Explorer InjectHTMLStream 函数远程代码执行漏洞、Microsoft Internet Explorer 不正确 Ref 计数远程代码执行漏洞、Microsoft Windows 远程代码执行漏洞、Microsoft Windows OpenType Font (OTF)驱动远程代码执行漏洞、Microsoft Windows TrueType Font 远程代码执行漏洞、Microsoft Word RTF 文件'listoverridecount'远程代码执行漏洞等。上述漏洞的综合评级均为“高危”。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。

参考链接：

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16811

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16784

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16786

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16788

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16790

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16792

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16793

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16795

3、Google 产品安全漏洞

Google Chrome 是一款流行的 WEB 浏览器。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可使应用程序崩溃，执行任意代码。

CNVD 收录的相关漏洞包括：Google Chrome 历史浏览拒绝服务漏洞、Google Chrome AAC 解码栈破坏漏洞、Google Chrome visibility events 内存错误引用漏洞、Google Chrome URL 加载器内存错误引用漏洞、Google Chrome PPAPI 缓冲区溢出漏洞、Google Chrome Chromoting client 插件存在未明漏洞。除“Google Chrome Chromoting client 插件存在未明漏洞”外，其余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-2012-16799

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16803

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16794

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16796

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16801

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16798

4、IBM 产品安全漏洞

IBM Server Firmware Power 5 是一款基于 IBM POWER5 处理器的中端服务器；IBM Flex System 是 IBM 发布的“专家集成系统”的核心组件；IBM eDiscovery Manager 是一款电子存储信息的软件；IBM Informix Dynamic Server 是一款数据库服务程序。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敏感信息，执行任意代码。

CNVD 收录的相关漏洞包括：IBM Flex System CMM/IMM2 信息泄露漏洞、IBM eDiscovery Manager 跨站脚本漏洞、IBM Server Firmware Power 5 远程权限提升漏洞、IBM Informix Dynamic Server 缓冲区溢出漏洞（CNVD-2012-16733）。其中，“IBM Server Firmware Power 5 远程权限提升漏洞”和“IBM Informix Dynamic Server 缓冲区溢出漏洞（CNVD-2012-16733）”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=CNVD-2012-16732

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16783

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16828

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2012-16733

5、VLC Media Player 'swf'文件栈缓冲区溢出漏洞

VLC media player 是一款流行的媒体播放程序。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。攻击者利用漏洞可构建恶意文件，诱使用户解析，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-2012-16735

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-2012-16832	Samsung Smart Tv 附带存储设备读取漏洞	高	暂无
CNVD-2012-16839	Joomla! Joomsport 组件 SQL 注入漏洞	高	暂无
CNVD-2012-16827	OpenDocMan SQL 注入漏洞	高	OpenDocMan 1.2.6.2a 已经修复此漏洞，建议用户下载使用： http://sourceforge.net/projects/opendocman/files/opendocman/1.2.6.2a/

CNVD-2012-16836	Freeside SQL 注入漏洞	高	暂无
CNVD-2012-16821	MyBB Tips Of The Day 插件 SQL 注入漏洞	高	暂无
CNVD-2012-16822	Citrix XenApp XML 服务接口远程代码执行漏洞	高	供应商已经修复此漏洞，建议用户升级更新： http://support.citrix.com/article/CTX135025
CNVD-2012-16825	gksu-polkit 本地权限提升漏洞	高	暂无
CNVD-2012-16776	Agora-Project SQL 注入漏洞	高	暂无
CNVD-2012-16775	Symantec Endpoint Protection Manager 远程代码执行漏洞	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.symantec.com/index.jsp
CNVD-2012-16761	Sumatra PDF/MuPDF 'lex_number()' 函数远程整数溢出漏洞	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://blog.kowalczyk.info/software/sumatrapdf/free-pdf-reader.html http://www.mupdf.com/

表 3 部分高危漏洞列表

小结： 本周，微软公司均发布了月度安全更新，用于修复微软 Windows、Internet Explorer、Office、Server 软件的多个安全漏洞。攻击者可以利用上述漏洞绕过安全限制或以应用程序上下文执行任意代码。本周，Adobe ColdFusion、Flash Player、AIR 产品以及 Google Chrome 和 IBM 的多款产品被披露存在多个漏洞，攻击者利用漏洞可获得敏感信息或执行任意代码，攻击者有可能利用发起大规模挂马攻击或基于互联网设备的探测攻击。本周，VLC Media Player 以及 MyBB DyMy User Agent 插件被披露存在零日漏洞，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、HP 布升级程序，修补 OpenVMS 产品漏洞

HP OpenVMS 是一款 HP Integrity 或 AlphaServer 服务器中使用的操作系统。本周，HP 修补了 OpenVMS 存在的拒绝服务漏洞。攻击者利用漏洞可对系统进发起拒绝服务攻击。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=26493

本周要闻速递

1. 三星 5 款手机爆安全漏洞

据国外媒体报道报道，一位名为 alephzain 的开发者宣称，自己发现了三星设备上的一个重大漏洞，黑客可以通过恶意软件进入设备的物理内存，更改、盗取用户数据。此漏洞出现的手机包括 Galaxy S2、Galaxy S3、Galaxy Note、Galaxy Note 2 和 Galaxy Note 10.1 在内 5 款手机，这些手机都采用三星猎户座 4 系处理器，也包括了魅族 MX2。利用此漏洞，XDA 开发者论坛上的一位版主已经做出 APK 文件，可以取得用户设备的根权限。此漏洞只针对于使用猎户座 4 系处理器的设备，Nexus 10 因为采用的是猎户座 5 系处理器而不受影响。暂时尚未出现利用该漏洞的恶意软件，三星暂未对此做出反应。参考链接：<http://it.sohu.com/20121217/n360631500.shtml>

2. 微软回应 IE 鼠标监控漏洞

有消息显示，IE 6 -10 中普遍存在一个重要漏洞，使黑客能够轻松地跟踪用户的鼠标移动轨迹，即便 IE 窗口已经最小化。消息来源 Spider.io 表示，他们在 10 月 1 日就将此漏洞报告给微软安全研发中心，但微软表示短时间内不可能完成修复工作。他们透露，目前至少有两家在线广告分析公司在利用此漏洞监视 IE 用户的鼠标轨迹。微软近日对此消息作出了公开表态：网站方可以跟踪用户的鼠标移动轨迹，即便 IE 窗口已经最小化，但他们只能获取鼠标的移动轨迹，并不知道用户具体在操作什么功能。我们已经和业内的安全研究员进行了沟通，认为这个漏洞对用户基本不会产生安全威胁。正如我们之前所述，尚未出现消息显示，这个漏洞导致了用户信息被盗。Spider.io 认为，将鼠标轨迹转化为数据并非难事，监视方可以通过广告定位的方式确认用户访问的网站性质及网页布局，看来微软并不认同这个观点。

参考链接：<http://it.sohu.com/20121215/n360535306.shtml>

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