

信息安全漏洞周报

2013 年 12 月 09 日-2013 年 12 月 15 日

2013 年第 50 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 122 个，其中高危漏洞 57 个、中危漏洞 61 个、低危漏洞 4 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 87 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“Hex Workshop 'mfc100trk.dll' DLL 加载任意代码执行漏洞”、“Enorth Webpublisher CMS 'this day'参数 SQL 注入漏洞”等零日攻击代码，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、合作伙伴、国家互联网应急中心及个人报送了本周收录的全部 122 个漏洞。报送情况如表 1 所示。其中，天融信、安天实验室、启明星辰等单位报送数量较多。此外，国家互联网应急中心、High-Tech Bridge Security Research Lab 及个人报送者向 CNVD 提交了 13 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
天融信	149	0
安天实验室	142	0
启明星辰	127	0
绿盟	64	0
奇虎 360	57	0
恒安嘉新	8	0
东软	1	0

上海交大	1	0
国家互联网应急中心	2	2
High-Tech Bridge Security Research Lab	2	2
个人	9	9
报送总计	562	13
录入总计	122（去重）	13

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、Mozilla、Google 等多家厂商的产品，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	21	17%
2	Mozilla	13	11%
3	Google	7	6%
4	Linux	5	4%
5	OpenJPEG	5	4%
6	Sharetronix LLC	5	4%
7	Adobe	4	3%
8	wordpress	3	2%
9	Zimbra	1	1%
10	其它	58	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 122 个漏洞。其中应用程序漏洞 81 个，WEB 应用漏洞 18 个，操作系统漏洞 15 个，网络设备漏洞 7 个，安全产品漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	81
WEB 应用漏洞	18
网络设备漏洞	7
操作系统漏洞	15
安全产品漏洞	1

表 3 漏洞按影响类型统计表

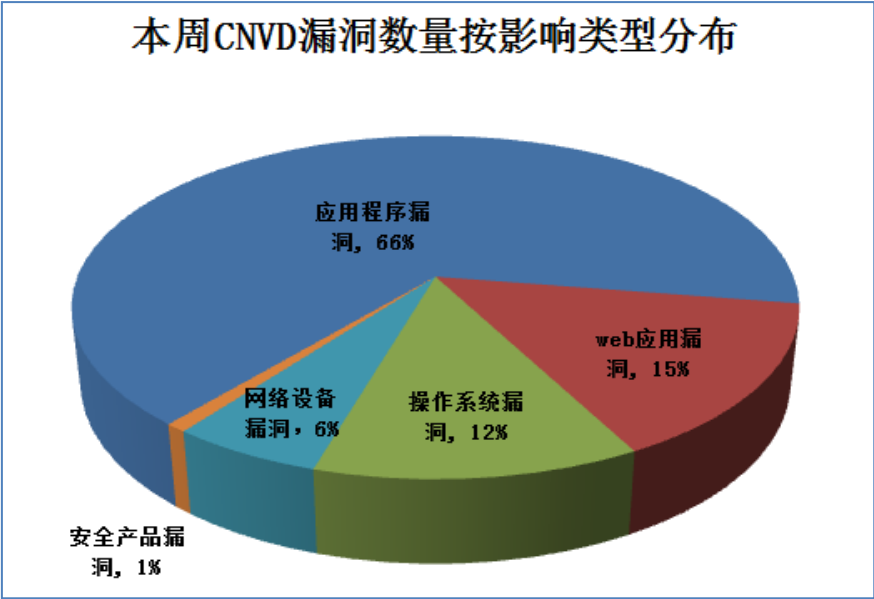


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 5 个电信行业漏洞和 4 个工控系统漏洞（如下列表所示）。其中，“D-Link DSR 路由器系列产品 SQL 注入漏洞、Siemens SINAMICS S/G 安全绕过漏洞、RuggedCom Rugged Operating System 验证绕过漏洞、RuggedCom Rugged Operating System 会话劫持漏洞”的综合评级均为“高危”。相关厂商已经发布了漏洞修复程序。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2013-14981	Alvarion BreezeACCESS VL 默认账户漏洞	中	否
电信	CNVD-2013-14982	ASUS WL520gu Wireless Router WPA 密钥泄露漏洞	中	否
电信	CNVD-2013-14983	ASUS WL520gu Wireless Router WPA-PSK 密文泄露漏洞	中	否
电信	CNVD-2013-14984	ASUS WL520gu Wireless Router 默认账户漏洞	中	否
电信	CNVD-2013-15014	D-Link DSR 路由器系列产品 SQL 注入漏洞	高	是
工控系统	CNVD-2013-14924	Siemens SINAMICS S/G 安全绕过漏洞	高	是
工控系统	CNVD-2013-14994	RuggedCom Rugged Operating System 验证绕过漏洞	高	是
工控系统	CNVD-2013-14993	RuggedCom Rugged Operating System 会话劫持漏洞	高	是
工控	CNVD-2013-14992	Schneider Electric Modicon M340 多个	中	否

系统		默认账户漏洞		
----	--	--------	--	--

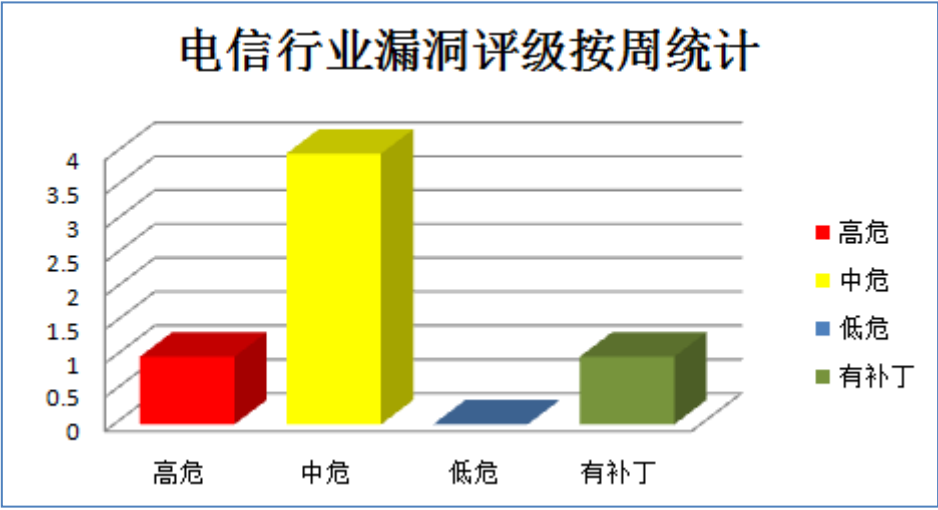


图 1 电信行业漏洞统计

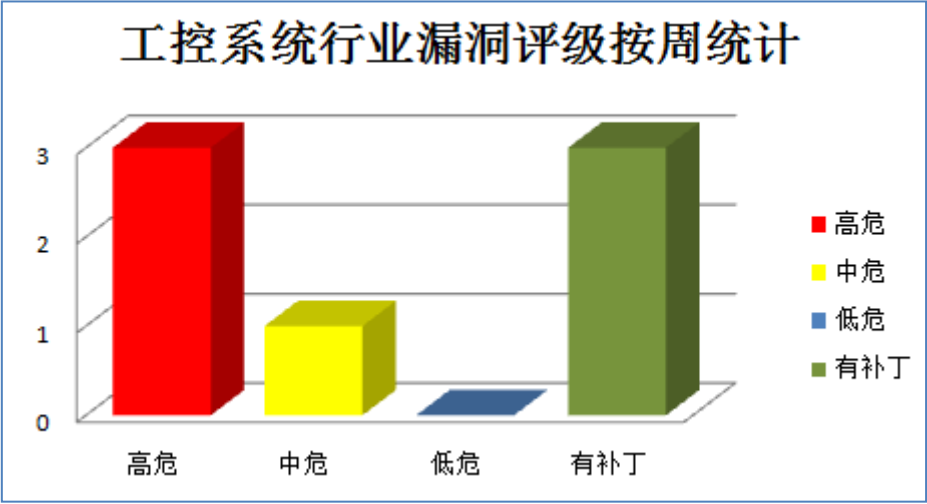


图 2 工控系统行业漏洞统计

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

12 月 11 日，微软发布了 2013 年 12 月份的月度例行安全公告，共含 11 项更新，修复了 Microsoft Windows、Internet Explorer、Office、SharePoint Server、Office Web Apps、Lync 和 ASP.NET 软件中存在的 24 个安全漏洞。其中，MS13-096、MS13-097、MS13-098、MS13-099、MS13-100 和 MS13-105 项更新综合评级均为最高级“严重”级别，剩余 5 项更新综合评级均为“重要”级别。利用上述漏洞，攻击者可以执行任意代码，提升权限，安全功能绕过或泄露敏感信息。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer 存在未明内存破坏漏洞（CNVD-2013-15020、CNVD-2013-15021、CNVD-2013-15022、CNVD-2013-15012）、Microsoft Internet Explorer 内存破坏漏洞（CNVD-2013-14998）、Microsoft Windows WinVerifyTrust 签名验证漏洞、Microsoft Windows 脚本运行对象库存在未明内存错误引用漏洞、Microsoft Windows 'Win32k.sys'地址值处理本地内存破坏漏洞等。上述漏洞综合评级为“高危”。厂商已经发布了上述漏洞的修补程序，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/flaw/show/CNVD-2013-15020>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15021>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15022>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14998>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15012>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15008>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15007>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15006>

2、Google Chrome 产品安全漏洞

Google Chrome 是一款 Web 浏览工具。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可劫持用户会话，发起网络钓鱼攻击，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 音轨处理任意代码执行漏洞、Google Chrome v8 'runtime.cc'缓冲区溢出漏洞、Google Chrome V8 Dehoistable Array Indices 处理越界写漏洞、Google Chrome 'ReplaceSelectionCommand::doApply'内存错误引用漏洞、Google Chrome 302 重定向一键登录流处理会话固定漏洞、Google Chrome 模态对话框地址栏伪造漏洞、Google Chrome V8 Dehoistable Array Indices 处理越界读漏洞。其中，“Google Chrome 音轨处理任意代码执行漏洞、Google Chrome v8 'runtime.cc'缓冲区溢出漏洞、Google Chrome V8 Dehoistable Array Indices 处理越界写漏洞、Google Chrome 'ReplaceSelectionCommand::doApply'内存错误引用漏洞”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 提醒用户及时下载补丁更新，避免引发漏洞相关的安全事件。

参考链接：<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14942>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14941>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14940>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14938>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14939>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14937>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14936>

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，攻击者利用漏洞可使应用程序崩溃，执行任意代码。

CNVD 收录的相关漏洞包括：Mozilla 多个产品存在未明内存破坏漏洞（CNVD-2013-15034）、Mozilla 多个产品有序列表元素替换任意代码执行漏洞、Mozilla 多个产品表单编辑内存错误引用漏洞、Mozilla 多个产品 event listeners 内存错误引用漏洞、Mozilla 多个产品 GetElementIC 类型数组生成未明漏洞、Mozilla 多个产品 'GetHoverGeneration()' synthetic 鼠标移动内存错误引用漏洞、Mozilla 多个产品存在未明内存破坏漏洞、Mozilla Firefox WEB 应用安装持久 Doorhanger 通知漏洞等。其中，除“Mozilla Firefox WEB 应用安装持久 Doorhanger 通知漏洞”外，其余漏洞的综合评级均为“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/flaw/show/CNVD-2013-15034>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15037>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15039>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15040>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15041>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15043>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15046>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15045>

4、Adobe 产品安全漏洞

Adobe Shockwave Player 是播放使用 Macromedia 和 Adobe Director 制作的网页内容的软件。Adobe Flash Player 是一个集成的多媒体播放器。本周，上述产品被披露存在多个漏洞，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：Adobe Shockwave Player 存在未明内存破坏漏洞（CNVD-2013-15025、CNVD-2013-15026）、Adobe Flash Player 和 AIR 类型混淆远程代码执行漏洞、Adobe Flash Player 和 AIR 远程代码执行漏洞。其中，“Adobe Shockwave Player 存在未明内存破坏漏洞（CNVD-2013-15025、CNVD-2013-15026）”的综合评级均为“高危”。厂商已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/flaw/show/CNVD-2013-15025>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15026>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14999>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15000>

5、Enorth Webpublisher CMS 'thisday'参数 SQL 注入漏洞

Enorth Webpublisher 是一款内容管理系统。本周，Enorth Webpublisher 被披露存在一个综合评级为“高危”的 SQL 注入漏洞，由于 Enorth Webpublisher log_searchday.jsp 脚本未能正确过滤用户提交给'thisday'参数的数据，远程攻击者利用漏洞可提交特制的 SQL 查询，操作或获取数据库信息。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/flaw/show/CNVD-2013-14960>

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/flaw/list.htm>

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2013-15048	MIUI 系统存在多个漏洞	高	暂无
CNVD-2013-15014	D-Link DSR 路由器系列产品 SQL 注入漏洞	高	厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： http://www.dlink.com/
CNVD-2013-15047	EMC Data Protection Advisor Illuminator EJBInvokerServlet 远程代码执行漏洞	高	暂无
CNVD-2013-15018	Samba DCE-RPC 帧长度字段处理远程缓冲区溢出漏洞	高	厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： http://www.samba.org/
CNVD-2013-15027	ack 存在多个代码执行漏洞	高	厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： http://openwall.com/lists/oss-security/2013/12/05/2
CNVD-2013-15013	NetGear 多款路由器存在后门漏洞	高	暂无
CNVD-2013-15011	OpenJPEG 存在多个越界内存破坏漏洞	高	暂无
CNVD-2013-14966	phpcms v9 会员注册头像文件上传漏洞	高	PHPCMS V9.5.2 Release 已经修复该漏洞，建议用户下载更新： http://download.phpcms.cn/v9/9.5/
CNVD-2013-14993	RuggedCom Rugged Operating System 会话劫持漏洞	高	RuggedCom ROS V3.12.2 已经修复该漏洞，建议用户下载更新： http://www.ruggedcom.com/

CNVD-2013-14973	OpenCart 存在多个漏洞	高	暂无
-----------------	-----------------	---	----

表 3 部分高危漏洞列表

小结：本周，微软发布了 2013 年 12 月份的月度例行安全公告，共含 11 项更新，修复了 Microsoft Windows、Internet Explorer、Office、SharePoint Server、Office Web Apps、Lync 和 ASP.NET 软件中存在的 24 个安全漏洞。攻击者可以执行任意代码，提升权限，安全功能绕过或泄露敏感信息。Google Chrome 和 Adobe、Mozilla 的多款产品被披露存在多个漏洞，攻击者利用漏洞可使应用程序崩溃，执行任意代码，漏洞可能会导致大规模的网页篡改和网络钓鱼攻击。此外，Enorth Webpublisher 内容管理系统被披露存在一个高危零日漏洞，建议相关用户应随时关注厂商主页，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、Zimbra 修补 Zimbra 产品漏洞

Zimbra 是一款专业的企业级邮件系统。本周，Zimbra 修补了 Zimbra 7.2.2 Patch 2、7.2.3、8.0.2 Patch 1、8.0.3 版本存在的文件包含漏洞，避免攻击者利用漏洞查看本地配置文件 localconfig.xml 信息，包括 LDAP 协议授权的根目录，通过窃取的 LDAP 信任请求/service/admin/soap API，创建具有管理员权限的用户，获得管理控制权。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/patchInfo/show/41543>

本周要闻速递

1. 警惕 Android 框架层注入漏洞

Android 系统频频惊现漏洞，并随之产生各种系统安全问题。近日，有国外媒体报道称 Android 系统再现框架层的注入漏洞，通过该漏洞攻击者可以执行某些特定代码或绕过某些安全检查，从而让 Android 手机面临危险。目前 Google 在最新的 Android 4.4 KitKat 系统已经修复了该漏洞问题，但是该漏洞还普遍存在于 Android 3.x-4.3 的系统版本中，当有 Activity 继承 Preference Activity 类并且被声明成 export=true 的时候就具备了被攻击的条件，这很可能会遭到黑客的恶意利用。

参考链接：<http://finance.21cn.com/stock/wmkzg/a/2013/1213/13/25510957.shtml>

2. 微软 NDPProxy 内核漏洞仍未修复

微软发布 12 月安全补丁，但并未修复已经公开曝光的 WindowsNDProxy 内核提权漏洞 ((CVE-2013-5065)。据了解，该漏洞影响 WindowsXP 及 Server2003 系统，目前一些安全软件已对此漏洞推出“热补丁”防护措施，预防木马病毒破坏系统。据微软发布

的安全公告称，已有黑客利用 NDProxy 内核提权漏洞发动攻击，如果用户不慎打开植入攻击代码的 PDF 文件，恶意代码就会自动运行，查看、更改或删除隐私数据，甚至创建具有管理员权限的系统帐户，使木马病毒获得系统最高控制权。此前，微软提供了手工禁用 NDProxy.sys 的临时解决方案，但该方案会导致系统某些服务无法正常工作，影响虚拟专用网络（VPN）、远程访问服务（RAS）和拨号网络。鉴于该漏洞威胁较大，国内多家安全厂商陆续对漏洞作出响应，开发出热补丁防护措施，在不影响系统正常功能的前提下防御漏洞攻击。

参考链接：<http://finance.21cn.com/stock/cfgd/a/2013/1211/14/25475721.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是国家计算机网络应急技术处理协调中心的简称（英文简称为 CNCERT 或 CNCERT/CC），成立于 1999 年 9 月，是一个非政府非盈利的网络安全技术协调组织，主要任务是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展中国互联网上网络安全事件的预防、发现、预警和协调处置等工作，以维护中国公共互联网环境的安全、保障基础信息网络和网上重要信息系统的安全运行。目前，CNCERT 在我国大陆 31 个省、自治区、直辖市设有分中心。

同时，CNCERT 积极开展国际合作，是中国处理网络安全事件的对外窗口。CNCERT 是国际著名网络安全合作组织 FIRST 正式成员，也是 APCERT 的发起人之一，致力于构建跨境网络安全事件的快速响应和协调处置机制。截止 2012 年，CNCERT 与 51 个国家和地区的 91 个组织建立了“CNCERT 国际合作伙伴”关系。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82990999