

信息安全漏洞周报

2011 年 12 月 5 日-2011 年 12 月 11 日

2011 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 77 个，其中高危漏洞 25 个、中危漏洞 48 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 66 个。本周收录的漏洞中，已有 45 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“HP Application Lifecycle Management 'GetInstalledPackages'本地特权提升漏洞”、“Adobe Acrobat/Reader U3D 内存破坏漏洞”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 3 家成员单位和一位个人上报者报送了本周收录的全部 77 个漏洞，其中包含 1 个原创漏洞，来自 NSS Labs 公司的研究员 Dillon Beresford 报送了 CNVD 成员单位 Baidu（百度）公司即时聊天软件 Hi 存在的文件解析错误漏洞。CNVD 工作委员会将对漏洞可利用的情况进行跟踪并验证，目前还尚未发现远程可利用情况。此外，CNVD 工作委员会将漏洞情况通报了百度公司。

各单位报送情况如表 1 所示。其中，启明星辰、绿盟科技、安天实验室报送数量均较多。

报送单位或个人	漏洞报送数量	原创漏洞数量
启明星辰	70	0
绿盟科技	37	0
安天实验室	33	0
Dillon Beresford	1	1
总计	77（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 Opera Software、Support Incident Tracker、ARC Informatique、Linux 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	Opera Software	5	6.5%
2	Support Incident Tracker	4	5.2%
3	ARC Informatique	4	5.2%
4	Linux	2	2.6%
5	HP	2	2.6%
6	D-Link	2	2.6%
7	Asterisk	2	2.6%
8	Apache Software Foundation	2	2.6%
9	Adobe	2	2.6%
10	Microsoft	1	1.3%
11	其它	51	66.2%

表 2 漏洞产品涉及厂商分布统计表

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、Arc Informatique 产品安全漏洞

Arc Informatique 是法国一家 SCADA/HMI 软件开发商，中文名为法国彩虹计算机公司。本周，Arc Informatique 的多款产品 FrontVue、PcVue 和 PlantVue 被披露存在多个安全漏洞。远程攻击者可以利用漏洞破坏内存、执行任意代码或通过目录遍历序列覆盖任意文件。CNVD 收录的相关漏洞包括：Arc Informatique 产品 ActiveX 控件漏洞（CNVD-2011-08925、CNVD-2011-08926、CNVD-2011-08927、CNVD-2011-08922）。上述漏洞的综合评级均为“高危”。目前，Arc Informatique 已经发布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=35361
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35362
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35363
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35357

2、Opera 浏览器安全漏洞

Opera 是一款开源的 WEB 浏览器。本周，Opera 被披露存在多个安全漏洞，攻击者

可以利用漏洞构建恶意 WEB 页，诱使用户解析，进而窃取用户的敏感信息。CNVD 收录的相关漏洞包括：Opera 缓存对象历史枚举漏洞、Opera 'visited'信息泄露漏洞、Opera Web Browser 存在漏洞、Opera Web Browser 'in'运算符跨域信息泄露漏洞、Opera Web Browser 顶级域名跨域信息泄露漏洞。目前，互联网上已经出现针对“Opera 'visited'信息泄露漏洞”的攻击代码，主要影响 Opera Web Browser 11.x 版本。厂商已经发布了“Opera Web Browser 存在漏洞、Opera Web Browser 'in'运算符跨域信息泄露漏洞、Opera Web Browser 顶级域名跨域信息泄露漏洞”的补丁，CNVD 提醒广大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=35359
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35311
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35312
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35314
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35315

3、Apache 产品安全漏洞

Apache 是一款互联网上应用较为广泛的 Web 服务软件。本周，Apache 的 Struts、ActiveMQ 和 MyFaces 等多款产品被披露存在安全漏洞。攻击者可以利用漏洞绕过安全限制、窃取敏感信息或使服务崩溃。CNVD 收录的相关漏洞包括：Apache Struts 会话篡改安全绕过漏洞、Apache MyFaces 信息泄露漏洞（CNVD-2011-08903）、Apache ActiveMQ Failover 机制远程拒绝服务漏洞。目前，厂商已经发布上述漏洞的修补程序，CNVD 提醒 Apache 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=35342
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35321
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35260

4、HP 产品安全漏洞

HP Application Lifestyle Management 是由 HP（惠普）公司提供的应用软件管理解决方案。本周，上述 HP 产品存在的一个本地特权提升漏洞。攻击者可以利用漏洞获得本地 root 特权。此外，HP 另一款产品 Device Access Manager 被披露存在一个内存破坏漏洞，攻击者可以利用漏洞以应用程序上下文执行任意代码。CNVD 收录的相关漏洞包括：HP Application Lifestyle Management 'GetInstalledPackages'本地特权提升漏洞、HP Device Access Manager for HP ProtectTools 堆内存破坏漏洞。其中，“HP Device Access Manager for HP ProtectTools 堆内存破坏漏洞”综合评级为“高危”。目前，互联网上已经出现了针对这两个漏洞的攻击代码。厂商尚未发布“HP Application Lifestyle Management 'GetInstalledPackages'本地特权提升漏洞”的补丁，CNVD 提醒广大用户随时关注厂商主页，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=35395

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35201

5、Adobe 产品安全漏洞

Adobe Flash Player 是一款 Flash 文件处理程序; Adobe Reader/Acrobat 是一款 PDF 文件处理程序。本周,上述 Adobe 产品被披露存在两个安全漏洞,远程攻击者可以利用漏洞破坏内存,以应用程序上下文执行任意代码,或控制目标用户系统。CNVD 收录的漏洞包括: Adobe Flash Player 存在未明代码执行漏洞、Adobe Acrobat/Reader U3D 内存破坏漏洞。其中,“Adobe Acrobat/Reader U3D 内存破坏漏洞”的综合评级为“高危”。目前,Adobe 尚未发布这两个漏洞的补丁程序,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=35282
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35389

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/sites/main/twaindex/advancedSearch.htm?columnid=52>

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2011-08940	Restorepoint 'remote_support.cgi'远程命令注入漏洞	高	TADASoft Restorepoint 3.3 Evaluation 已经修复此漏洞,建议用户下载使用: http://www.restorepoint.com/restorepoint/
CNVD-2011-08945	QContacts (Joomla component) SQL 注入漏洞	高	暂无
CNVD-2011-08929	SourceBans SQL/LF 注入漏洞	高	暂无
CNVD-2011-08912	Trend Micro Control Manager 'CmdProcessor.exe'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://downloadcenter.trendmicro.com/index.php?prodid=7
CNVD-2011-08911	Traq 'authenticate()'函数远程代码执行漏洞	高	Traq 2.3.1 已经修复此漏洞,建议用户下载使用: http://sourceforge.net/projects/qatraq/
CNVD-2011-08909	Novell ZENWorks Asset Management 'rtrlet'组件远程代码执行漏洞	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://download.novell.com/Download?buildid=hPvHtXeNmCU~

CNVD-2011-08889	GNU C Library '__tzfile_read()'缓冲区溢出漏洞	高	暂无
CNVD-2011-08901	Sielco Sistemi 多个产品缓冲区溢出漏洞	高	SIELCO SISTEMI Winlog Pro 2.7.9 和 SIELCO SISTEMI Winlog Lite 2.7.9 已经修复此漏洞，建议用户下载使用： www.sielcosistemi.com/download/WinlogLite_Setup.exe www.sielcosistemi.com/download/Winlog_Setup_SF.exe .
CNVD-2011-08908	Foxit Reader 存在未明内存破坏漏洞	高	暂无
CNVD-2011-08864	Blue Coat ProxyAV libpng 缓冲区溢出漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： https://kb.bluecoat.com/index?page=content

表 3 部分高危漏洞列表

小结：本周，法国彩虹计算机公司（Arc Informatique）的多款工业控制系统软件被披露存在多个综合评级为“高危”的安全漏洞，攻击者可以利用漏洞破坏内存、执行任意代码或通过目录遍历序列覆盖任意文件。建议国内采用该厂商产品的相关用户应及时下载补丁或更新文件进行加固。

此外，本周 Opera、Apache 以及 HP、Adobe、Foxit（福昕）等公司产品的被披露的零日漏洞和高危漏洞也对广大用户也构成较大威胁，请使用上述产品的网站服务器管理员、个人用户注意防范。

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、Novell 发布升级程序，修补 ZENworks Asset Management 漏洞

ZENworks Asset Management 是 Novell 公司提供的一款用于在组织内跨资源自动化 IT 管理和业务流程的工具。本周，Novell 发布升级程序，修补了 ZENworks Asset Management 存在的安全漏洞。远程攻击者可以利用漏洞以 SYSTEM 上下文执行任意代码。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=61](http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=6196)



本周要闻速递

1. Skype 存在漏洞 可泄露用户信息

据国外媒体报道，纽约大学理工学院在 Skype 中发现了一个安全漏洞，可能会向黑客泄露 Skype 用户的地理位置和 P2P 共享活动等信息。纽约大学的科学家们对 1 万个 Skype 用户和 20 位志愿者进行了为期 2 周的监控，最后发现了这个安全漏洞。黑客可以通过被跟踪的 Skype 用户从不同地点拨打电话的记录来追踪该用户的行动。科学家们在研究中成功地跟踪了一位 Skype 用户从纽约出发到芝加哥度假，然后返回法国家中的整个过程。科学家称：“要想跟踪某一位 Skype 用户，黑客首先要通过不显眼的一次通话来获得该用户的 IP 地址，然后才能展开跟踪。解决这个问题的方法非常简单，而且代价很低。” Skype 首席信息官称，公司将努力提高 Skype 软件的安全性能。

参考链接：<http://tech.qq.com/a/20111209/000228.htm>

2. 谷歌开始 Android 内部测试 将修复安全漏洞

据国外媒体报道，一些谷歌员工在 Google+ 上透露，Nexus S 的 Android 4.0 操作系统（Ice Cream Sandwich）已经在内部进行测试。但是随后大部分消息被删除了，预计谷歌将会很快推出正式的更新版本。此前北卡罗来纳州立大学研究发现，一些安卓设备存在主要的安全许可漏洞，这些漏洞允许非信任软件记录你的通话内容，发送短信，获得地理位置，做一些其他非经允许的事情。而谷歌和摩托罗拉都确认了漏洞的存在。业内人士表示，谷歌的这次内部测试主要是为了对 Android 4.0 更新进行性能测试和评估，从而发现一切日常使用中可能出现的 Bug，进行改善。谷歌在 10 月发布 Android 4.0 操作系统，但是发布之后一直没有迅速发布 Android 4.0 的更新，就是谷歌希望能够在 Android 4.0 中解决这一安全漏洞，从而延缓了其升级的速度。预计谷歌将在几个月之后发布正式版的 Android 4.0 更新。

参考链接：http://www.kejixun.com/a/2011-12-06/11264_1.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