

信息安全漏洞周报

2011 年 10 月 24 日-2011 年 10 月 30 日

2011 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**高**。

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 160 个，其中高危漏洞 56 个、中危漏洞 99 个、低危漏洞 5 个。上述漏洞中，可利用来实施远程攻击的漏洞有 146 个。网上已经出现针对“Oracle AutoVue 'AutoVueX.ocx' ActiveX 控件'SaveViewStateToFile()'不安全方法漏洞”、“Opera Web 浏览器树遍历内存错误引用漏洞”等的零日攻击代码，请使用相关产品的用户注意做好防护措施。本周收录的漏洞中，已有 112 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。

成员单位报送漏洞统计

本周，共 5 家成员单位报送了本周收录的全部 160 个漏洞，各单位报送情况如表 1 所示。其中，绿盟科技、启明星辰、恒安嘉新的数量较多。

报送单位或个人	漏洞报送数量	私有漏洞数量
绿盟科技	104	0
启明星辰	91	0
恒安嘉新	78	0
安天实验室	38	0
安氏领信	2	0
总计	160（去重）	0

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Google、Cisco、Apple、WordPress 等多家厂商的产品，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	Google	18	11.3%

2	Moodle	14	8.8%
3	Cisco	11	6.9%
4	Apple	10	6.3%
5	eFront	7	4.4%
6	Linux	5	3.1%
7	Wordpress	5	3.1%
8	Winamp	3	1.8%
9	Oracle	3	1.8%
10	Novell	3	1.8%
11	其它	81	50.7%

表 2 漏洞产品涉及厂商分类统计

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、Apple QuickTime 安全漏洞

Apple QuickTime 是一款多媒体播放器。本周，Apple 发布安全更新，修复 QuickTime 产品存在的多个安全漏洞。攻击者可以利用漏洞使应用程序崩溃或执行任意代码。CNVD 收录的相关漏洞包括：Apple QuickTime 脚本注入漏洞、Apple Quicktime 关联文件解析漏洞（CNVD-2011-08179、CNVD-2011-08177、CNVD-2011-08175、CNVD-2011-08174、CNVD-2011-08173、CNVD-2011-08172、CNVD-2011-08171）等。上述漏洞中，除“Apple QuickTime 脚本注入漏洞”、“Apple Quicktime 关联文件解析漏洞（CNVD-2011-08177、CNVD-2011-08175）”外，其余漏洞的综合评级均为“高危”。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/vulnerability/CNVD-2011-08180>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08179>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08177>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08175>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08174>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08173>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08172>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08171>

2、Google Chrome 安全漏洞

本周，Google 发布安全更新，修复 Chrome 浏览器存在多个安全漏洞。远程攻击者

可以利用漏洞进行拒绝服务攻击或产生其他未明影响。CNVD 收录的相关漏洞包括：Google Chrome 函数泄露漏洞（CNVD-2011-08117）、Google Chrome 内存错误引用漏洞（CNVD-2011-08116、CNVD-2011-08113、CNVD-2011-08106、CNVD-2011-08103）、Google Chrome 堆溢出漏洞（CNVD-2011-08114）、Google Chrome 越界写漏洞（CNVD-2011-08110）、Google Chrome 时序处理漏洞（CNVD-2011-08104）等。上述漏洞中，除“Google Chrome 内存错误引用漏洞（CNVD-2011-08113）”、“Google Chrome 越界写漏洞（CNVD-2011-08110）”和“Google Chrome 时序处理漏洞（CNVD-2011-08104）”外，其余漏洞的综合评级均为“高危”。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/vulnerability/CNVD-2011-08117>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08116>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08113>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08106>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08103>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08114>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08110>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08104>

3、Cisco 产品安全漏洞

本周，Cisco 发布安全更新，修复了其多款产品 WebEx、IOS、Adaptive Security Appliance 等存在的多个漏洞。攻击者可以利用漏洞以应用程序上下文执行任意代码、获得敏感信息或发起拒绝服务攻击。CNVD 收录的相关漏洞包括：Cisco IOS dot1x 端口处理拒绝服务漏洞（CNVD-2011-08151、CNVD-2011-08150）、Cisco WebEx WRF/ATAS32 文件格式远程缓冲区溢出漏洞（CNVD-2011-08149、CNVD-2011-08148）、Cisco IOS 'ethernet-ldp'组件远程拒绝服务漏洞、Cisco Video Surveillance 2421,2500 和 2600 系列 IP 摄像头拒绝服务漏洞、Cisco CiscoWorksCommon Services 信息泄露漏洞、Cisco IOS ICMPv6 Echo 请求信息泄露漏洞等。除“Cisco Video Surveillance 2421, 2500 和 2600 系列 IP 摄像头拒绝服务漏洞”、“Cisco CiscoWorks Common Services 信息泄露漏洞”、“Cisco IOS ICMPv6 Echo 请求信息泄露漏洞”外，其余漏洞的综合评级均为“高危”。CNVD 提醒 Cisco 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/vulnerability/CNVD-2011-08151>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08150>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08149>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08148>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08145>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08141>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08140>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08134>

4、Winamp 产品安全漏洞

Winamp 是一款多媒体播放器。本周，Winamp 被披露存在多个综合评级为“高危”的安全漏洞。远程攻击者可以利用漏洞构建畸形 Winamp 媒体关联文件，触发堆缓冲区溢出。CNVD 收录的相关漏洞包括：Winamp 'toc_alloc'缓冲区溢出漏洞、Winamp 'channels'缓冲区溢出漏洞、Winamp 'iOffsetMusic'缓冲区溢出漏洞。CNVD 提醒 Winamp 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/vulnerability/CNVD-2011-08185>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08184>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08183>

5、Oracle AutoVue 安全漏洞

Oracle AutoVue 是一款图文浏览、标注、协同作业的应用软件。本周，上述 Oracle 产品被披露存在多个安全漏洞，远程攻击者可利用漏洞在任意位置创建或覆盖任意扩展文件。CNVD 收录的相关漏洞包括：Oracle AutoVue 'AutoVueX.ocx' ActiveX 控件'Export3DBom()'不安全方法漏洞、Oracle AutoVue 'AutoVueX.ocx' ActiveX 控件'ExportEdaBom()'不安全方法漏洞、Oracle AutoVue 'AutoVueX.ocx' ActiveX 控件'SaveViewStateToFile()'不安全方法漏洞。目前，互联网上已经出现针对这些漏洞的攻击代码，主要影响 Oracle AutoVue 20.0.1 版本。其中，“Oracle AutoVue 'AutoVueX.ocx' ActiveX 控件'SaveViewStateToFile()'不安全方法漏洞”的综合评级为“高危”。目前，厂商尚未发布上述漏洞的补丁程序，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/vulnerability/CNVD-2011-08039>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08056>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08057>

小结：本周，Apple、Google 和 Cisco 均发布安全公告，修复了 Apple QuickTime、Google Chrome 和 Cisco 多款产品存在的多个安全漏洞，远程和本地攻击者可以利用这些漏洞引发多种威胁。同时，Winamp 产品也被披露存在多个安全漏洞，Oracle AutoVue ActiveX 控件零日漏洞对使用该产品的用户构成较大威胁。请使用上述软件的相关机构和个人及时采取安全防范措施。

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，修补多款产品安全漏洞

本周, Novell 发布升级程序, 修补了 XTier Framework、ZENworks Handheld Management 和 iPrint Client 产品的多个安全漏洞。远程攻击者可以利用漏洞执行任意代码、创建文件或导致应用程序拒绝服务。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/patch/5653>
<http://www.cnvd.org.cn/patch/5652>
<http://www.cnvd.org.cn/patch/5651>



本周要闻速递

1. 国内知名反病毒软件被曝“蓝屏漏洞” 可致蓝屏死机

有技术博客爆料称, 国内某知名反病毒软件存在一个极易导致电脑死机的“蓝屏漏洞”, 影响该产品当前所有版本(2012 SP2 及以下版本)。“只要运行 9 行代码的小程序, 就可以让安装该产品的电脑立刻蓝屏崩溃。”据分析, 该产品的“蓝屏漏洞”实际上是一个拒绝服务漏洞。目前, 厂商尚未对此次蓝屏漏洞曝光事件做出回应, 也没有宣布何时修复漏洞。

参考链接: <http://www.2cto.com/News/201110/109285.html>

2. 各种云架构存在“大量”安全漏洞

德国研究人员称, 他们在亚马逊 Web 服务(AWS)中发现了一些错误, 由此他们认为, 在很多云架构中也存在着类似的错误, 可能导致攻击者获取管理权限, 从而盗取所有用户的数据。虽然研究人员称他们已将这些安全漏洞告知了 AWS, 而且 AWS 也已经修复了这些漏洞, 但他们认为同样类型的攻击针对其他的云服务同样有效。德国波鸿鲁尔大学的一个研究团队利用多种 XML 签名封装攻击获取了不少客户账号的管理员权限, 然后可以创建客户云的新实例, 可以添加镜像或删除镜像。研究人员还利用跨站脚本漏洞攻击了开源的私有云软件框架 Eucalyptus。他们还发现亚马逊的服务也容易受到跨站脚本攻击。这说明公有云并不像表面看上去那么安全。这些问题在其他云架构中也能够发现。

参考链接: http://security.zdnet.com.cn/security_zone/2011/1031/2063488.shtml

3. 安全专家发现 Facebook 安全缺陷

安全渗透测试者在 Facebook 上发现了一个重大缺陷, 即允许任何人向他人发送社交网站的恶意应用程序。一名高级安全技术顾问发现了该漏洞, 并在博客中公开披露。该人士表示, Facebook 此漏洞最危险的是, 黑客可以利用社会工程技术让人推送附件, 有可能造成计算机感染恶意软件。Facebook 官方并没有立即对此事作出回应。

参考链接: <http://www.2cto.com/News/201110/109423.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