

信息安全漏洞周报

2011 年 10 月 17 日-2011 年 10 月 23 日

2011 年第 42 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 198 个，其中高危漏洞 73 个、中危漏洞 98 个、低危漏洞 27 个。上述漏洞中，可利用来实施远程攻击的漏洞有 174 个。网上已经出现针对“Opera 嵌入式 SVG 内容处理代码执行漏洞”、“GTA SA-MP server.cfg 本地缓冲区溢出漏洞”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 154 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 198 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、安天实验室的数量较多。

报送单位或个人	漏洞报送数量	私有漏洞数量
启明星辰	128	0
绿盟科技	63	0
安天实验室	31	0
恒安嘉新	30	0
安氏领信	2	0
总计	198（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 Oracle、Apple、WordPress、HP 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	Oracle	76	38.4%

2	Apple	17	8.6%
3	WordPress	14	7.1%
4	HP	8	4.0%
5	Novell	6	3.0%
6	Bugfree	4	2.0%
7	Joomla!	4	2.0%
8	Cisco	3	1.5%
9	Linux	3	1.5%
10	IBM	2	1.0%
11	其它	61	30.9%

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、心海软件学校心理管理系统安全漏洞

本周，CNVD 发布了北京心海导航科技有限公司的产品心海软件学校心理管理系统存在的多个安全漏洞。9月20日，CNVD 接到北京邮电大学安全研究员上报，称该系统存在 cookie 伪造漏洞和文件上传漏洞。攻击者可以利用上述漏洞伪造 cookie 和上传网页木马，以获得系统管理员权限或主机控制权。CNVD 收录的漏洞包括：心海软件学校心理管理系统文件上传漏洞、心海软件学校心理管理系统 cookie 伪造漏洞。其中，CNVD 对“心海软件学校心理管理系统 cookie 伪造漏洞”的综合评级为“高危”。目前，北京心海导航科技有限公司并未提供相关漏洞补丁。CNVD 将继续跟踪处置情况。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07380>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07376>

2、Oracle 产品安全漏洞

本周，Oracle 发布了 2011 年 10 月的安全更新，修复了其多款产品存在的 76 个安全漏洞。其中 56 个是针对 Oracle 的产品，其他 20 个补丁是修复 Java SE 产品，包括 Java FX 和 JRockit。利用上述漏洞，远程或本地攻击者可以进行拒绝服务攻击，获取敏感信息，劫持用户会话，操作系统数据，甚至访问或控制系统。CNVD 收录的相关漏洞包括：Oracle Java SE 远程 Java 实时环境漏洞（CNVD-2011-08014、CNVD-2011-08012、CNVD-2011-07924、CNVD-2011-07922）、Oracle Sun 产品 GlassFish Server 漏洞（CNVD-2011-08008）、Oracle Waveset 远程漏洞（CNVD-2011-07959）、Oracle Database Server 本地 Oracle Text 漏洞（CNVD-2011-07934）、Oracle OpenSSO 远程漏洞（CNVD-2011-079

30) 等。上述漏洞中的综合评级均为“高危”。CNVD 提醒 Oracle 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-2011-08014>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08012>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08008>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07959>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07934>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07930>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07924>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07922>

3、HP 产品安全漏洞

本周,HP 产品 MFP Digital Sending Software 和 Data Protector 存在多个安全漏洞。攻击者可以利用漏洞执行任意代码, 窃取敏感信息。CNVD 收录的相关漏洞包括: HP MFP Digital Sending Software 本地信息泄露漏洞 (CNVD-2011-08007)、HP Data Protector 存在未明远程代码执行漏洞 (CNVD-2011-07987、CNVD-2011-07986、CNVD-2011-07985、CNVD-2011-07984、CNVD-2011-07982、CNVD-2011-07981、CNVD-2011-07979)。除“HP MFP Digital Sending Software 本地信息泄露漏洞 (CNVD-2011-08007)”外, 其余漏洞的综合评级均为“高危”。目前, HP 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/vulnerability/CNVD-2011-08007>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07987>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07986>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07985>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07984>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07982>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07981>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07979>

4、Cisco 产品安全漏洞

本周, Cisco 多款产品存在多个安全漏洞。攻击者可以利用漏洞获得敏感信息, 上传恶意代码。CNVD 收录的相关漏洞包括: CiscoWorks Common Services 远程命令注入漏洞、Cisco Show/Share 匿名访问安全绕过漏洞、Cisco Show/Share 任意文件上传漏洞。其中“CiscoWorks Common Services 远程命令注入漏洞”、“Cisco Show/Share 匿名访问安全绕过漏洞”的综合评级均为“高危”。目前, Cisco 已经发布了这些漏洞的补丁程序, 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/vulnerability/CNVD-2011-07978>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07976>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07975>

5、Novell 产品安全漏洞

本周，Novell 的产品 ZENworks Handheld Management、ZENworks Configuration Management、Open Enterprise Server 等存在多个安全漏洞。远程攻击者可以利用漏洞执行任意代码或未授权修改信息。CNVD 收录的相关漏洞包括：Novell ZENworks Handheld Management 存在未明远程代码执行漏洞（CNVD-2011-08017、CNVD-2011-08016）、Novell help.Dall ActiveX 存在未明漏洞、Novell Antique ActiveX 存在未明漏洞、Novell l SGrid.Grid.1 ActiveX 存在未明漏洞、Novell Open Enterprise Server DSfW 域组策略对象安全绕过漏洞。Novell 已经发布了这些漏洞的补丁程序，CNVD 提醒 Novell 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-2011-08017>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08016>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07998>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07997>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07996>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07873>

6、Opera 嵌入式 SVG 内容处理代码执行漏洞

Opera 是一款开源的 WEB 浏览器。本周，Opera 被披露存在一个代码执行漏洞。由于 Opera 在处理嵌入到 Frameset 中的 SVG 内容存在错误，攻击者可以利用漏洞构建恶意 WEB 页，诱使用户解析，以应用程序上下文执行任意代码。目前，互联网上已经出现针对该漏洞的攻击代码，主要影响 Opera Software Opera 11.x 版本。该漏洞的综合评级为“高危”。厂商尚未发布该漏洞的补丁程序，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-2011-07837>

小结：本周，CNVD 发布了北京心海导航科技有限公司的产品心海软件学校心理管理系统存在的多个安全漏洞。攻击者可以利用漏洞伪造 cookie 和上传网页木马，以获得系统管理员权限或主机控制权。同时，Oracle 发布了 2011 年 10 月的安全更新，修复了其多款产品存在的 76 个安全漏洞。HP、Cisco 以及 Novell 产品也被披露存在多个安全漏洞。此外，Opera 零日漏洞也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、Linux 发布升级程序，修补 Kernel 安全漏洞

Linux 是一款开源的操作系统。本周，Linux 发布升级程序，修补了 Kernel 存在的多个漏洞。攻击者可以利用漏洞发起拒绝服务攻击或窃取敏感信息。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/5433>

<http://www.cnvd.org.cn/patch/5569>

<http://www.cnvd.org.cn/patch/5570>

本周要闻速递

1.我国需要加强信息安全漏洞分析与风险评估

据新华社电，工业和信息化部信息安全协调司副司长杨春艳日前表示，我国信息安全漏洞分析和风险评估工作需要突破一系列技术难关，不断探索方法创新，实施策略优化，并进一步增强国家在制度化上的工作安排。杨春艳在第四届信息安全漏洞分析与风险评估大会上说，当前我国信息安全环境越来越复杂多变。一方面，信息化发展速度很快，各类信息技术被广泛应用，国民经济和工业化对信息系统的依赖程度越来越高，社会发展与互联网的融合在不断加深，网民数量、网络规模、网络普及速度均居全球首位。但同时，各类信息安全事件层出不穷，漏洞后门普遍存在，安全风险不断增加，尤其是一些深层次、全局性的信息安全隐患开始显现，严重威胁国家经济发展和国家安全。

参考链接：http://hsb.hsw.cn/2011-10/23/content_8184278.htm

2.iPhone 4S 用户警惕 Siri 安全漏洞

安全技术公司发现，iPhone 4S 的 Siri 应用存在安全漏洞。在 iPhone 4S 的默认设置中，Siri 在手机锁屏的情况下也是可以运行的。这就意味着，即使别人无法打开你的手机，他们依然可以接入你手机里运行的 Siri 应用，并通过它来发短信和邮件，这样别人就很容易获取你手机里的大量信息，这样是很不安全的。iPhone 4S 默认设置中允许 Siri 运行是这一漏洞产生的原因。防止这个漏洞的方法也很简单，iPhone 4S 用户只需改变手机的设置，在选择密码保护情况下关闭 Siri 功能就可以了，这样一来，Siri 在 iPhone 4S 锁屏的情况下就不会运行了。

参考链接：<http://www.ctiforum.com/news/2011news/10/news10241.htm>

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