

信息安全漏洞周报

2011 年 11 月 14 日-2011 年 11 月 20 日

2011 年第 46 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 133 个，其中高危漏洞 46 个、中危漏洞 81 个、低危漏洞 6 个。上述漏洞中，可利用来实施远程攻击的漏洞有 121 个。本周收录的漏洞中，已有 91 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“ISC BIND 递归查询远程拒绝服务漏洞”、“Mozilla Firefox 'OnStartRequest()'空指针拒绝服务漏洞”等影响较大的零日漏洞，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 5 家成员单位报送了本周收录的全部 133 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、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	88	0
绿盟科技	82	0
恒安嘉新	51	0
安天实验室	31	0
安氏领信	2	0
总计	133（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 Adobe、Google、SAP、Apple、Joomla!、IBM 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	Adobe	12	9.0%
2	Google	8	6.0%

3	SAP	7	5.3%
4	Apple	5	3.8%
5	Joomla!	5	3.8%
6	IBM	4	3.0%
7	Drupal	4	3.0%
8	HP	3	2.3%
9	Dell	3	2.3%
10	ZTE Corporation	2	1.5%
11	其它	80	60.0%

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、ISC BIND 9 递归查询远程拒绝服务漏洞

ISC BIND 9 是互联网上应用较为广泛的 DNS 服务软件。本周，ISC BIND 9 被披露存在安全漏洞，使用 BIND 9 软件的递归服务器会缓存一个无效记录，随后收到客户端对这一记录的查询时会在缓存中查找到这一记录并应答，造成该情况的原因目前尚未查明。远程攻击者可利用此漏洞使服务程序崩溃。受该漏洞影响的 BIND 9 版本包括当前支持的所有版本，以及 9.4-ESV、9.6-ESV、9.7.x、9.8.x，CNVD 对该漏洞的技术评级为“中危”，但由于互联网上应用 BIND 9 的 DNS 服务器较多，对域名系统及域名解析服务安全构成较大威胁。目前，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，同时用户可升级到 BIND 9.8.1-P1、9.7.4-P1、9.6-ESV-R5-P1、9.4-ESV-R5-P1 版本，以减轻该漏洞威胁。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08571>

2、Google Chrome 安全漏洞

本周，Google 发布安全更新，修复 Chrome 浏览器存在的多个安全漏洞。远程攻击者可以利用漏洞构建恶意 WEB 页，诱使用户解析，导致应用程序崩溃或者执行任意代码。CNVD 收录的相关漏洞包括：Google Chrome 越界远程代码执行漏洞（CNVD-2011-08589）、Google Chrome Apple 运行权限要求漏洞、Google Chrome editing 内存错误引用漏洞、Google Chrome shader 变量映射缓冲区溢出漏洞、Google Chrome Vorbis 解码器堆溢出漏洞、Google Chrome VP8 编码内存破坏漏洞、Google Chrome MKV 和 Vorbis 媒体处理漏洞、Google Chrome Theora 解码器两次释放漏洞。其中，除“Google Chrome editing 内存错误引用漏洞、Google Chrome MKV 和 Vorbis 媒体处理漏洞”外，

其余漏洞的综合评级均为“高危”。Google 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-2011-08589>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08497>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08495>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08494>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08493>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08491>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08490>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08488>

3、Apple 产品安全漏洞

本周，Apple 的产品 iTunes 和 iOS 存在多个安全漏洞。攻击者可以利用漏洞绕过安全限制或检查，导致任意代码执行。CNVD 收录的相关漏洞包括：Apple iTunes 软件更新伪造漏洞、Apple iOS 代码签名检查漏洞（CNVD-2011-08479、CNVD-2011-08478）、Apple iOS libinfo 信息泄露漏洞（CNVD-2011-08473）、Apple iOS FreeType 处理内存破坏漏洞（CNVD-2011-08471）。其中，除“Apple iOS 代码签名检查漏洞（CNVD-2011-08479、CNVD-2011-08478）、Apple iOS libinfo 信息泄露漏洞（CNVD-2011-08473）”外，上述漏洞的综合评级均为“高危”。目前，Apple 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-2011-08536>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08479>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08478>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08473>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08471>

4、Adobe Flash Player 安全漏洞

Adobe Flash Player 是一款 Flash 文件处理程序。本周，Adobe Flash Player 被披露存在多个安全漏洞。攻击者可以利用漏洞导致代码执行。CNVD 收录的相关漏洞包括：Adobe Flash Player 内存破坏漏洞（CNVD-2011-08487、CNVD-2011-08486、CNVD-2011-08481、CNVD-2011-08477、CNVD-2011-08476、CNVD-2011-08475、CNVD-2011-08474、CNVD-2011-08470）。上述漏洞的综合评级均为“高危”。目前，Adobe 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-2011-08487>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08486>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08481>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08477>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08476>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08475>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08474>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08470>

5、Mozilla Firefox 'OnStartRequest()' 空指针拒绝服务漏洞

Mozilla Firefox 是一款 Mozilla 公司生产的 WEB 浏览器。本周, Mozilla Firefox 存在空指针引用拒绝服务漏洞。远程攻击者可以利用漏洞执行任意代码, 导致系统拒绝服务。目前, 互联网上已经出现针对该漏洞的攻击代码, 并且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-2011-08556>

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/vulnerability/advancedSearch>

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2011-08596	V-CMS SQL 注入漏洞	高	暂无
CNVD-2011-08594	webERP SQL 注入漏洞	高	webERP 4.06RC2 已修复此漏洞, 建议用户下载使用: http://www.weberp.org/HomePage
CNVD-2011-08553	Drupal Webform CiviCRM 集成模块存在未明 SQL 注入漏洞	高	Webform CiviCRM Integration 7.x-2.2 和 6.X-2.2 已修复此漏洞, 建议用户下载使用: http://drupal.org/project/webform_civicrm
CNVD-2011-08523	PBCS Technology 'articlenav.php' SQL 注入漏洞	高	暂无
CNVD-2011-08514	Mini-Stream RM-MP3 Converter 栈缓冲区溢出漏洞	高	暂无
CNVD-2011-08498	Hancom Office 文档处理远程代码执行漏洞	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.hancom.co.kr/notice.noticeView.do?targetRow=1-ice_seqno=100
CNVD-2011-08489	Joomla! 'com_biiatemplateshop' 组件'groups' 参数 SQL 注入漏洞	高	暂无
CNVD-2011-08501	OneCMS 存在多个 SQL 注入漏洞	高	暂无

CNVD-2011-08506	Wordpress 插件 Zingiri 远程代码执行漏洞	高	暂无
CNVD-2011-08492	openEngine 'id' 参数 SQL 注入漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，ISC BIND 9 被披露存在安全漏洞，影响到互联网上众多采用 BIND 9 的域名服务器，攻击者可直接发起针对 DNS 系统的拒绝服务攻击。Apple、Google、Adobe 等公司的个人桌面应用产品被披露存在多个漏洞，Mozilla Firefox 被披露存在零日漏洞，对广大用户操作系统桌面应用安全构成较大威胁。

此外，CNVD 本周收录了多个在国内外网站信息系统中应用广泛的网站内容管理系统（CMS）存在的 SQL 注入、远程代码执行等漏洞，利用这些漏洞有可能获得网站数据库后台敏感信息甚至是操作系统管理权限。

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、SAP 发布升级程序，修补 NetWeaver 安全漏洞

本周，SAP 发布升级程序，修补了 NetWeaver 的安全漏洞。SAP NetWeaver 是 SAP 提供面向服务的应用和集成平台套件。攻击者可以利用该产品漏洞执行任意命令或代码。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/patch/5913>

<http://www.cnvd.org.cn/patch/5912>

<http://www.cnvd.org.cn/patch/5911>

<http://www.cnvd.org.cn/patch/5910>

<http://www.cnvd.org.cn/patch/5909>

<http://www.cnvd.org.cn/patch/5908>

<http://www.cnvd.org.cn/patch/5922>

本周要闻速递

1. 政府网站普遍存在三大安全漏洞

目前，政府网站重视硬件投入，也采取了一定的防护措施，但在检测中发现，安全漏洞在各级政府网站中仍然普遍存在，SQL 注入、信息泄露、弱密码三大安全漏洞尤其突出。相比常见的电脑黑客篡改网页，危害性更大的是政府网站的数据遭到窃取。随着办公数字化、网络化，那些公众可以上网办理业务的行业，如工商、税务、交通等部门的安全要求进一步提高。网上曾曝出某市交通一卡通的搭乘信息可以输入卡号随意查询的案例，而税务报表等数据隐含更多的个人信息。

参考链接: <http://roll.sohu.com/20111119/n326196552.shtml>

2. 当当网被曝安全漏洞致用户资料泄露

据第三方安全问题反馈平台乌云漏洞报告平台 11 月 10 日曝光，当当网存在设计缺陷或逻辑错误，大量用户资料因此泄露。乌云平台 10 日在微博发布消息称，当当网存在设计缺陷，登录后可通过漏洞获得所有用户的姓名、联系方式、地址等信息。报告者称“某处设计不当，过于详细，太容易发现了”。据乌云平台透露，所发布的安全漏洞将以认领及邮件方式通知厂商，目前其页面漏洞回应一项显示“未能联系到厂商或者厂商积极拒绝”。当当网随后发布声明称，当当网已修复相关漏洞，经过检查，不存在大量用户信息泄露的情况。

参考链接: <http://roll.sohu.com/20111111/n325247727.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