

信息安全漏洞周报

2012 年 11 月 05 日-2012 年 11 月 11 日

2012 年第 44 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 181 个，其中高危漏洞 66 个、中危漏洞 110 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 179 个。本周收录的漏洞中，已有 95 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“**MyBB FollowerUser Plugin 'usid' SQL 注入漏洞**”、“**Microsoft Internet Explorer 9 内存破坏拒绝服务漏洞**”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 7 家成员单位和多个合作伙伴报送了本周收录的全部 181 个漏洞。各单位报送情况如表 1 所示。其中，启明星辰、绿盟科技等单位报送数量较多。此外，High-Tech Bridge Security Research 及一位个人报送者向 CNVD 提交了 5 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
启明星辰	163	0
绿盟科技	89	0
安天实验室	57	0
天融信	11	0
安氏领信	7	0
东软	1	0
知道创宇	4	0
High-Tech Bridge Security Research	1	1
个人报送者	4	4
报送总计	337	5
录入总计	181（去重）	5

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、Adobe、Apple 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	Google	16	9%
2	Adobe	13	7%
3	Apple	9	5%
4	Sophos	7	4%
5	Drupal	7	4%
6	Agile Access Control, Inc.	7	4%
7	Apache	6	3%
8	osCommerce	6	3%
9	Pattern Insight	5	3%
10	HP	2	1%
11	其它	103	57%

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 181 个漏洞。其中操作系统漏洞 4 个，应用程序漏洞 112 个，WEB 应用漏洞 63 个，安全产品漏洞 2 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	4
应用程序漏洞	112
WEB 应用漏洞	63
安全产品漏洞	2
网络设备漏洞	0
数据库漏洞	0

表 3 漏洞按影响类型统计表

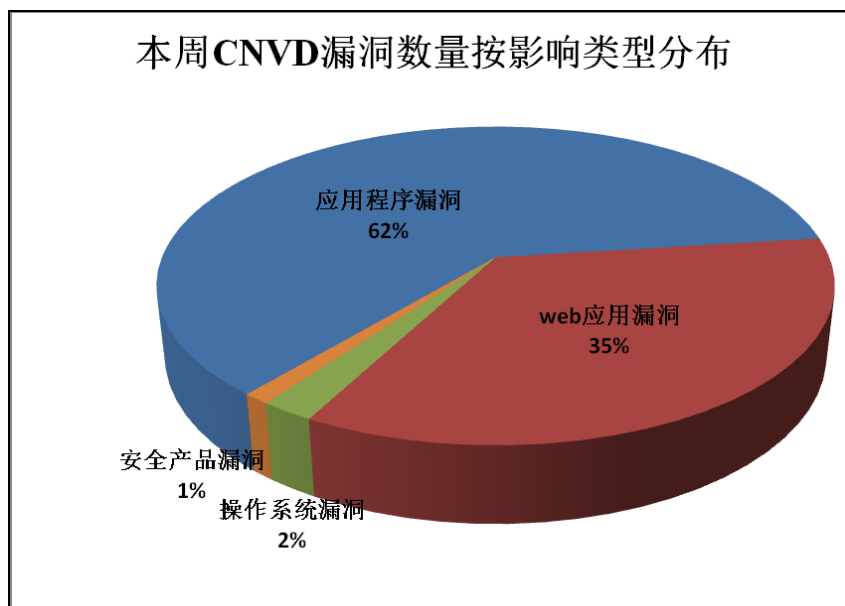


图 1 本周漏洞按影响类型分布

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、Google Chrome 安全漏洞

Google Chrome 是一款 WEB 浏览器。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可构建恶意 WEB 页，诱使用户解析，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 Buggy 图形驱动漏洞、Google Chrome GPU 整数检查漏洞、Google Chrome 纹理处理内存破坏漏洞、Google Chrome v8 越界访问漏洞、Google Chrome 输入类型转换漏洞、Google Chrome 视频布局漏洞、Google Chrome WebP 处理越界读漏洞、Google Chrome placeholder 内存错误引用漏洞等。上述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=60977
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60981
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60992
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60984
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60989
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60986
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60995
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60994

2、Adobe 产品安全漏洞

Adobe reader 是一款处理 PDF 文件的应用程序；Adobe Flash Player 是一款 Flash 文

件处理程序。本周，上述 Adobe 产品被披露存在多个安全漏洞，攻击者利用漏洞可执行任意代码或发起拒绝攻击。

CNVD 收录的相关漏洞包括：Adobe Reader 栈溢出漏洞、Adobe Reader 存在未明远程代码执行漏洞、Adobe Flash Player/AIR 存在未明安全绕过漏洞（CNVD-2012-15762）、Adobe Flash Player/AIR 存在未明缓冲区溢出漏洞（CNVD-2012-15758、CNVD-2012-15760、CNVD-2012-15759、CNVD-2012-15761）、Adobe Flash Player/AIR 存在未明内存破坏漏洞（CNVD-2012-15764）等。上述漏洞的综合评级均为“高危”。目前，厂商已经修复了上述漏洞，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=60783
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=61075
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=61058
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=61035
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=61056
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=61060
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=61055
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=61057

3、Apache 产品安全漏洞

Apache Tomcat 是一款开源的 JSP 应用服务器程序；Apache CXF 一个开源的 Service 框架；HttpClient 是 Apache Jakarta Common 下的子项目，用来提供支持 HTTP 协议的客户端编程工具包；Apache Axis2 是 Apache web services/SOAP/WDSL 引擎。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可通过任意合法证书进行中间人攻击，欺骗 SSL 服务器，或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Apache Tomcat 拒绝服务漏洞、Apache CXF 证书校验中间人攻击漏洞、Apache Commons HttpClient 证书校验中间人攻击漏洞、Apache Axis2 证书校验中间人攻击漏洞（CNVD-2012-15673、CNVD-2012-15674）、Apache Tomcat DIGEST 安全绕过漏洞。目前，厂商已经修复了“Apache Tomcat DIGEST 安全绕过漏洞”和“Apache Tomcat 拒绝服务漏洞”，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=60943
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60769
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60765
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60761
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60762
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60957

4、osCommerce 模块安全漏洞

osCommerce 是一款开源网上商城建站软件系统。本周，该产品的多个模块被披露存在多个安全漏洞，攻击者利用漏洞可通过任意合法证书进行中间人攻击，欺骗 SSL 服务器。

CNVD 收录的相关漏洞包括：osCommerce PayPal Express 模块证书校验中间人攻击漏洞、osCommerce Authorize.Net 模块证书校验中间人攻击漏洞、osCommerce Sage Pay Direct 模块证书校验中间人攻击漏洞、osCommerce PayPal Pro PayFlow 模块证书校验中间人攻击漏洞、osCommerce PayPal Pro PayFlow EC 模块证书校验中间人攻击漏洞、osCommerce MoneyBookers 模块证书校验中间人攻击漏洞、osCommerce PayPal Pro 模块证书校验中间人攻击漏洞。厂商尚未发布上述漏洞的修复程序，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=60940
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60938
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60937
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60955
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60975
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60939
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=60941

5、MyBB FollowerUser Plugin 'usid' SQL 注入漏洞

MyBB 是一款流行的论坛程序。本周，该被披露存在一个综合评级为“高危”的 SQL 注入漏洞。攻击者利用漏洞可获得数据库敏感信息。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/sites/main/preview/ldgg_preview.htm?tid=60679

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/publish/main/52/index.html>

CNVD 编号	漏洞名称	综合 评级	修复方式
CNVD-2012-15716	WordPress AJAX Post search 插件 SQL 注入漏洞	高	WordPress AJAX Post Search Plugin 1.3 已经修复此漏洞，建议用户下载使用： http://www.fingerfish.com/wp-plugin-ajax-search/
CNVD-2012-15714	Invision Power Board 'core.php' PHP 代码执行漏洞	高	用户可联系厂商获得相应的补丁程序： http://community.invisionpower.com/to

			pic/371625-ipboard-31x-32x-and-33x-security-update
CNVD-2012-15715	多个 Symantec 产品 CAB 文件处理内存破坏漏洞	高	Symantec Endpoint Protection 12.0 已经修复此漏洞，建议用户下载使用： http://www.symantec.com/
CNVD-2012-15751	Opera Web Browser 存在多个漏洞（CNVD-2012-15751）	高	Opera Web Browser 12.10 已经修复此漏洞，建议用户下载使用： http://www.opera.com
CNVD-2012-15669	Android SMS 伪造漏洞	高	暂无
CNVD-2012-15666	Amazon Elastic Load Balancing API Tools 证书校验中间人攻击漏洞	高	暂无
CNVD-2012-15682	AWAuctionScript CMS SQL 注入漏洞	高	暂无
CNVD-2012-15752	VeriCentre SQL 注入漏洞	高	VeriCentre Web Console 2.2 build 36 已经修复此漏洞，建议用户下载使用： http://global.verifone.com/products/software/estate-management/vericentre
CNVD-2012-15649	VBulletin ChangUonDyU - Advanced Statistics SQL 注入漏洞	高	暂无
CNVD-2012-15631	C3-ilex EOscada 资源管理错误漏洞	高	C3-ilex EOscada 11.0.19.2 已经修复此漏洞，建议用户下载使用： http://www.c3ilex.com/products/index.html

表 3 部分高危漏洞列表

本周，Google Chrome 以及 Adobe 的多款产品被披露存在多个安全漏洞，攻击者利用漏洞通过邮件发送恶意文件、网页挂载恶意程序的方式发起针对桌面终端用户的攻击。Apache 的多款产品以及 osCommerce 多个模块也被披露存在多个漏洞，这些漏洞的利用特点是存在中间人攻击方式，攻击者利用漏洞可通过任意合法证书进行中间人攻击，欺骗 SSL 服务器，从而窃取用户信息、劫持用户会话。此外，MyBB 论坛程序被披露存在零日漏洞，建议采用该软件的网站用户随时关注厂商主页，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、HP 布升级程序，修补 Performance Insight 漏洞

HP Performance Insight 是一款数据库第三方监控管理工具。本周，HP 修补了 Performance Insight 存在的多个漏洞。允许攻击者利用漏洞进行拒绝服务攻击。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=24582
http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=24583

本周要闻速递

1. 微软将发布 6 个安全补丁修复 Win8 漏洞

据国外媒体报道，微软称，将在 11 月 13 日星期二发布 6 个安全补丁，其中 4 个安全补丁将修复包括新发布的 Windows 8 在内的软件中的严重的安全漏洞。补丁将修复 Windows、IE、Office 和 .Net 框架中的安全漏洞。从 Windows XP 到 Windows 8，所有得到技术支持版本的 Windows 以及 Windows Server 和 IE 9 浏览器软件都将得到这些重要的补丁。微软称，所有 4 个严重等级的补丁都将修复远程执行代码的安全漏洞。此外，微软计划发布一个补丁修复 Office 软件中的远程执行代码安全漏洞。这个安全漏洞的风险等级是“重要”。微软还将发布一个修复 Windows 中的一个泄露信息安全漏洞的补丁。这个安全漏洞的风险等级是“中等”。微软称，Office 的安全补丁还将提供给使用 OS X 版 Office 软件的 Mac 机用户。

参考链接：http://news.xinhuanet.com/tech/2012-11/10/c_123938005.htm

2. 互联网最大规模帐号劫持漏洞即将引爆

目前有一项严重危害用户隐私的漏洞刚被发现，包括旅游、招聘、娱乐、SNS 交友、各大电商等各类网站均会被影响，国内使用第三方登录机制的网站中普遍存在此漏洞。由于此类攻击不受同源策略等浏览器的安全限制，且不易被目标发现，因此危害严重。一旦被利用，用户的帐号会被永久劫持，账户信息会被任意浏览和改动。由于之前出现过关联类漏洞，疑似已经有攻击者开始利用这个漏洞进行实际攻击，请广大网民确认自身账号信息是否已遭恶意劫持，及时采取措施保护自身账号。经确认，此漏洞是由于开发人员没有正确按照 OAuth2 授权机制的开发文档使用 OAuth2，导致攻击者能够实施跨站请求伪造(CSRF)通过第三方网站来劫持用户在目标网站的账户。

参考链接：<http://news.mydrivers.com/1/246/246374.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