

信息安全漏洞周报

2011 年 11 月 7 日-2011 年 11 月 11 日

2011 年第 45 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 132 个，其中高危漏洞 45 个、中危漏洞 84 个、低危漏洞 3 个。上述漏洞中，可利用来实施远程攻击的漏洞有 124 个。本周收录的漏洞中，已有 67 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。本周互联网上出现了针对“HP Data Protector Media Operations 缓冲区溢出漏洞”等高危漏洞的零日攻击代码，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 5 家成员单位和多个合作伙伴/个人报送了本周收录的全部 132 个漏洞，各单位报送情况如表 1 所示。其中，恒安嘉新、启明星辰、绿盟科技的数量较多。

报送单位或个人	漏洞报送数量	私有漏洞数量
恒安嘉新	92	0
启明星辰	60	0
绿盟科技	44	0
安天实验室	31	0
东软	3	0
广西信息网络安全协会	3	1
总计	132（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 Mozilla、Joomla!、HP、Microsoft 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	Mozilla	9	6.8%
2	Joomla!	8	6.0%
3	HP	6	4.5%
4	Support Incident	5	3.8%
5	Microsoft	5	3.8%
6	Adobe	4	3.0%
7	Drupal	4	3.0%
8	Mahara	4	3.0%
9	IBM	3	2.3%
10	TRS	3	2.3%
11	其它	81	61.5%

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、Microsoft 产品安全漏洞

本周，微软发布了 2011 年 11 月份的月度例行安全公告，更新修复了影响 Windows 操作系统和组件（包含 Windows Vista、Windows 7、Windows Server 2008 和 Windows Server 2008 R2）的安全漏洞。另外，Microsoft Excel 也发现存在漏洞，并且厂商尚未发布该漏洞的补丁程序。利用上述漏洞，攻击者可以远程执行任意代码、提升特权，或导致系统拒绝服务。CNVD 收录的相关漏洞包括：Microsoft Windows 活动目录 LDAPS 身份验证绕过漏洞、Microsoft Windows Mail/Meeting Space 不安全库加载漏洞、Microsoft Windows TrueType 字体解析拒绝服务漏洞、Microsoft Windows TCP/IP 引用计数溢出漏洞、Microsoft Excel 内存错误引用远程代码执行漏洞。上述漏洞中“Microsoft Windows TrueType 字体解析拒绝服务漏洞”、“Microsoft Excel 内存错误引用远程代码执行漏洞”的综合评级为“高危”。CNVD 提醒广大 Microsoft 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-2011-08402>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08401>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08399>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08398>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08348>

2、TRS WCM 安全漏洞

TRS 内容协作平台（TRS Web Content Management，简称：TRS WCM）涵盖网

站建立、内容服务、内容传递等内容价值链的各个方面，将结构化和非结构化信息提供给所有用户。本周，CNVD 接到广西信息安全协会研究人员报送的 TRS 产品存在的多个漏洞。攻击者可以利用漏洞添加、篡改帮助文件的内容，上传文件，或获取敏感信息。CNVD 收录的相关漏洞包括：TRS WCM 敏感信息泄露漏洞、TRS WCM 文件上传漏洞、TRS WCM SQL 注入漏洞。上述漏洞中“TRS WCM 文件上传漏洞”、“TRS WCM 文件上传漏洞”的综合评级为“高危”。拓尔思公司称之前已针对上述漏洞提供过补丁，但没有在官方网站发布。CNVD 抽样检测结果发现部分使用该软件的省级政府网站仍存在没有修复漏洞的情况。CNVD 提醒广大使用该软件的用户直接联系厂商以获取补丁信息。

参考链接：暂无

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08437>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08436>

3、Adobe Shockwave Player 安全漏洞

Adobe Shockwave Player 是一款使用 Director Shockwave Studio 制作的网页外挂播放软件。本周，Adobe 发布安全更新，修复 Adobe Shockwave Player 存在的多个漏洞。远程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 Shockwave Player 内存破坏漏洞（CNVD-2011-08408、CNVD-2011-08407、CNVD-2011-08405、CNVD-2011-08404）。上述漏洞的综合评级均为“高危”。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-2011-08408>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08407>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08405>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08404>

4、Mozilla 产品安全漏洞

Mozilla Firefox/Thunderbird 是 Mozilla 所发布的 WEB 浏览器和邮件客户端软件。本周，Mozilla 存在多个安全漏洞。攻击者可以利用漏洞获得特权、注入或执行任意代码，导致系统拒绝服务（内存损坏和应用程序崩溃）或信息泄露。CNVD 收录的相关漏洞包括：Mozilla Firefox/Thunderbird 权限提升漏洞、Mozilla Firefox/Thunderbird 跨站脚本漏洞、Mozilla Firefox/Thunderbird 拒绝服务漏洞（CNVD-2011-08427、CNVD-2011-08425、CNVD-2011-08423）、Mozilla Firefox/Thunderbird 任意代码执行漏洞、Mozilla Firefox/Thunderbird 信息泄露漏洞、Mozilla Firefox/Thunderbird 代码执行漏洞。除“Mozilla Firefox/Thunderbird 跨站脚本漏洞”、“Mozilla Firefox/Thunderbird 信息泄露漏洞”外，其余漏洞的综合评级均为“高危”。CNVD 提醒 Mozilla 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-2011-08430>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08428>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08427>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08425>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08423>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08419>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08414>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08412>

5、HP Data Protector Media Operations 安全漏洞

本周，HP Data Protector Media Operations 被披露存在缓冲区溢出和目录遍历漏洞。攻击者可以利用漏洞以应用程序上下文执行任意代码或进行目录遍历攻击，下载安装程序分区中的任意文件。CNVD 收录的相关漏洞包括：HP Data Protector Media Operations 缓冲区溢出漏洞、HP Data Protector Media Operations 参数目录遍历漏洞。上述漏洞中，“HP Data Protector Media Operations 缓冲区溢出漏洞”的综合评级为“高危”。目前，互联网上已经出现针对该漏洞的攻击代码，主要影响 HP Data Protector Media Operations 6.20 及之前版本。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-2011-08369>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08339>

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-2011-08466	Oracle Hyperion Strategic Finance Formula One ActiveX 控件 'SetDevNames()'缓冲区溢出漏洞	高	暂无
CNVD-2011-08459	Support Incident Tracker SQL 注入漏洞	高	暂无
CNVD-2011-08443	DTV Player 播放列表解析缓冲区溢出漏洞	高	暂无
CNVD-2011-08392	zenphoto Ajax 文件管理器代码注入漏洞	高	ZenPhoto 1.4.1.5 及之后版本已修复此漏洞，建议用户下载使用： http://www.zenphoto.org/
CNVD-2011-08332	Advantech ADAM OPC Server ActiveX 控件缓冲区溢出漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： http://support.advantech.com.tw/support/DownloadSRDetail.aspx?SR_ID=1-2NMHLB

CNVD-2011-08344	Mahara MNet 远程特权提升漏洞	高	Mahara 1.4.1 已经修复此漏洞，建议用户下载使用： http://mahara.org/
CNVD-2011-08385	Joomla! BF Quiz 组件 'catid' 参数 SQL 注入漏洞	高	暂无
CNVD-2011-08442	AbsoluteFTP 远程缓冲区溢出漏洞	高	暂无
CNVD-2011-08416	11in1 CMS CRLF 注入漏洞	高	暂无
CNVD-2011-08352	Site@School 'index.php' SQL 注入漏洞	高	用户可联系供应商获得补丁信息： http://siteatschool.sourceforge.net/

表 3 部分高危漏洞列表

小结：本周，微软发布了 2011 年 11 月份的月度例行安全公告，更新修复了影响 Windows 操作系统和组件（包含 Windows Vista、Windows 7、Windows Server 2008 和 Windows Server 2008 R2）的安全漏洞。同时，TRS、Mozilla、Adobe 也被披露存在多个漏洞，HP Data Protector Media Operations 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、IBM 发布升级程序，修补多款产品安全漏洞

本周，IBM 发布升级程序，修补了 IBM 存在的多个安全漏洞。攻击者可以利用漏洞修改其他用户的偏好、获得敏感目录和文件名信息、在受影响站点上下文的用户浏览器会话中执行任意 HTML 或脚本代码。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/5801>
<http://www.cnvd.org.cn/patch/5800>
<http://www.cnvd.org.cn/patch/5793>

本周要闻速递

1. 微软发布 11 月安全公告

本周，微软发布了 11 月安全公告及补丁以应对至少 4 个 Windows 的漏洞。此次更

新针对所有 Windows 版本中的远程代码执行和拒绝服务问题，微软敦促其用户群特别注意 MS11-083 公告，其针对 Windows TCP/IP 协议中一个较严重的漏洞。微软还修补了一个 Windows Mail 中的一个漏洞（MS11-085），该漏洞可能使用户遭受黑客通过浏览器的攻击。微软有望在接下来 30 天内完成应对其的功能漏洞检测代码。11 月的更新还包括动态目录（Active Directory）权限升级缺陷的补丁（MS11-086）以及针对 Windows 内核驱动的补丁（MS11-084），其允许拒绝服务攻击。

参考链接：http://news.ccidnet.com/art/946/20111110/3115449_1.html

2. Skype 和 MSN 被曝存漏洞

据国外媒体报道，Skype、MSN 存在安全隐患，攻击者可通过 IP 地址窃取用户信息，窥视用户聊天记录，为网络犯罪留下隐患。据科技网站 TrendMicro 报道，有报告称在 Skype 和 MSN 上发现了监听用户网络活动并记录呼叫记录的后门程序 BKDR_R2D2.A。黑客可以利用基于 R2D2 的字符串对 Skype、Yahoo! Messenger、MSN Messenger 和 SioGate x-lite 等软件完成监听聊天对话、记录 Skype 上的视频通话、监控浏览器的网络流量及截图功能。

参考链接：http://news.ccidnet.com/art/11099/20111111/3118559_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