

信息安全漏洞周报

2011 年 11 月 28 日-2011 年 12 月 4 日

2011 年第 48 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低。

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 76 个，其中高危漏洞 22 个、中危漏洞 53 个、低危漏洞 1 个。上述漏洞中，可利用来实施远程攻击的漏洞有 72 个。本周收录的漏洞中，已有 32 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“Siemens SIMATIC WinCC Flexible Runtime 'HmiLoad.exe'缓冲区溢出漏洞”和“Gretech GOM Player '.asx'文件远程栈缓冲区溢出漏洞”等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报送了本周收录的全部 76 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、安天实验室报送数量较多。此外，CNVD 还收录了国网电力科学研究院信息安全网络安全实验室以及北京网御星云信息技术有限公司报送的 2 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	52	0
绿盟科技	41	0
安天实验室	40	0
恒安嘉新	19	0
安氏领信	2	0
北京网御星云信息技术有限公司	1	1
广西信息网络安全协会	1	1

总计	76（去重）	2
----	--------	---

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Siemens、Schneider Electric、WikkaWiki、MyBB 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	Siemens	11	14.5%
2	WikkaWiki	5	6.6%
3	Schneider Electric	4	5.3%
4	MyBB	3	3.9%
5	WordPress	2	2.6%
6	Mediawiki	2	2.6%
7	FFmpeg	2	2.6%
8	IBM	1	1.3%
9	HP	1	1.3%
10	Adobe	1	1.3%
11	其它	44	58.0%

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、Schneider Electric 产品安全漏洞

本周，Schneider Electric（施耐德电气）多个产品被披露存在多个漏洞。攻击者可以利用这些漏洞进行拒绝服务攻击、窃取敏感数据或远程执行代码等。CNVD 收录的相关漏洞包括：Schneider Electric 缓冲区溢出漏洞、Schneider Electric Vijeo Historian Web Server 存在未明目录遍历漏洞、Schneider Electric Vijeo Historian Web Server 跨站脚本漏洞、TeeChart ActiveX 控件缓冲区溢出拒绝服务漏洞。其中，“Schneider Electric 缓冲区溢出漏洞”和“TeeChart ActiveX 控件缓冲区溢出拒绝服务漏洞”的综合评级为“高危”。目前，Schneider Electric 官方已对存在漏洞的产品发布了补丁，CNVD 建议相关用户立即进行修复，避免引发漏洞相关的网络安全事件。更多相关信息可参考 CNVD 官网的安全公告（http://www.cnvd.org.cn/publish/main/19/2011/20111202141327218758445/20111202141327218758445_.html）。

参考链接：http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35092
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=34965

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=34966

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=34968

2、Siemens 产品安全漏洞

本周，Siemens（西门子）公司的产品 SIMATIC WinCC Flexible（2008 SP2 版本）和 Automation License Manager（500.0.122 1 版本）被披露存在目录遍历、缓冲区溢出、拒绝服务等 9 个安全漏洞。攻击者可以利用漏洞进行拒绝服务攻击、窃取敏感数据或远程执行代码等。CNVD 收录的相关漏洞包括：Siemens Automation License Manager 缓冲区溢出漏洞、Siemens Automation License Manager 'wcscpy_s'缓冲区溢出漏洞、Siemens Automation License Manager 'almaxcx.dll' ActiveX 任意文件覆盖漏洞、Siemens Automation License Manager 拒绝服务漏洞、Siemens SIMATIC WinCC Flexible Runtime 'HmiLoad.exe'缓冲区溢出漏洞、Siemens SIMATIC WinCC Flexible Runtime 'HmiLoad.exe'目录遍历漏洞、Siemens SIMATIC WinCC Flexible Runtime 'HmiLoad.exe'服务崩溃漏洞、Siemens SIMATIC WinCC Flexible Runtime 'HmiLoad.exe'文件下载漏洞等。其中，“Siemens Automation License Manager 缓冲区溢出漏洞、Siemens Automation License Manager 'wcscpy_s'缓冲区溢出漏洞、Siemens SIMATIC WinCC Flexible Runtime 'HmiLoad.exe'缓冲区溢出漏洞、Siemens SIMATIC WinCC Flexible Runtime 'HmiLoad.exe'服务崩溃漏洞”的综合评级为“高危”。目前，厂商尚未发布上述漏洞的修补程序，CNVD 提醒相关用户关注厂商主页以获取最新版本，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=34967

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=34969

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=34970

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=34971

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=34973

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=34975

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=34977

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=34978

3、WikkaWiki 安全漏洞

WikkaWiki 是一个用 PHP 语言编写的轻量级 Wiki 引擎，后台数据使用 MySQL 数据库存储。本周，WikkaWiki 被披露存在多个安全漏洞，远程攻击者可以利用漏洞获得数据库管理权限或以 WEB 权限执行任意代码，删除用户账户。CNVD 收录的相关漏洞包括：WikkaWiki 未限制文件上传漏洞（CNVD-2011-08811）、WikkaWiki 跨站请求伪造漏洞（CNVD-2011-08813）、WikkaWiki 下载任意文件（CNVD-2011-08817）、WikkaWiki 代码存在漏洞（CNVD-2011-08810）。上述漏洞中，“WikkaWiki 下载任意文件（CNVD-2011-08817）”和“WikkaWiki 代码存在漏洞（CNVD-2011-08810）”的综合评级均为“高危”。目前，WikkaWiki 尚未发布上述漏洞的修补程序，CNVD 提醒相关用户关注

厂商主页以获取最新版本，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=35146
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35148
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35152
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35145

4、Ubuntu 安全漏洞

Ubuntu 是一款基于 linux 内核的发行版本。本周，Ubuntu 被披露存在两个安全漏洞。远程或本地的攻击者可以利用漏洞绕过安全限制、执行任意文件。CNVD 收录的相关漏洞包括：Ubuntu 升级管理器不安全临时目录创建漏洞、Ubuntu 升级管理器 GPG 签名校验安全绕过漏洞。目前，Ubuntu 已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/sites/main/preview/ldgg_preview.htm?tid=34972
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=34974

5、Gretech GOM Player '.asx'文件远程栈缓冲区溢出漏洞

Gretech GOM Player 是一款多媒体播放软件。Gretech GOM Player 在处理特制的 ASX 文件时存在栈缓冲区溢出，攻击者可以利用漏洞构建恶意文件，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 GRETECH CORP. GOM Player 2.1.33.5071 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/sites/main/preview/ldgg_preview.htm?tid=35121

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/index.html>

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2011-08740	A2CMS 'index.php'本地文件泄露漏洞	高	暂无
CNVD-2011-08728	PHP Video Script 'index.php'SQL 注入漏洞	高	暂无
CNVD-2011-08734	TYPO3 Hut-Manager 存在未明 SQL 注入漏洞	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://typo3.org/fileadmin/ter/m/mm/mm_hutinfo_1.0.1.t3x
CNVD-2011-08777	CoDeSys 整数溢出漏洞	高	暂无
CNVD-2011-08770	Avid Media Composer 'AvidPhoneticIndexer.exe'远程栈缓冲区溢出漏洞	高	暂无

CNVD-2011-08799	StoryBoard Quick XML 文件缓冲区溢出漏洞	高	暂无
CNVD-2011-08802	ClearSilver 'neo_cgi'模块存在多个格式串漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： https://bugzilla.redhat.com/show_bug.cgi?id=757542
CNVD-2011-08803	Ctek SkyRouter 4200 和 4300 系列路由器远程任意命令执行漏洞	高	暂无
CNVD-2011-08772	Final Draft 存在多个远程栈缓冲区溢出漏洞	高	Final Draft 8.02 已经修复此漏洞，建议用户下载使用： http://www.finaldraft.com/index.php
CNVD-2011-08784	CCMPlayer '.m3u'文件远程栈缓冲区溢出漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，Schneider Electric（施耐德电气）、Siemens（西门子）等公司的工业控制系统产品被披露存在多个漏洞。这些漏洞影响了 Schneider Electric 和 Siemens 的多款产品的多个版本。攻击者利用漏洞可对使用 Schneider Electric 和 Siemens 的用户构成严重的威胁。同时 Ubuntu、WikkaWiki 产品也被披露存在多个漏洞。Gretech GOM Player 零日漏洞也构成较大威胁，请使用上述产品的网站服务器管理员、个人用户注意防范。

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、Apache 发布升级程序，修补 MyFaces 漏洞

本周，Apache 发布升级程序，修补了 MyFaces 存在的安全漏洞。远程攻击者可利用漏洞绕过部分安全限制。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=6097

本周要闻速递

1. Ubuntu 11.04 内核升级

Canonical 于 11 月 29 日发布了公告 USN-1285-1，发布 Ubuntu 11.04 的一个内核升级补丁，修补近期发现的七个安全漏洞。专家建议 Ubuntu 11.04 用户在第一时间通过 Update Manager 进行升级更新，之后系统内核版本将会变为 linux-image-2.6.38-13 (2.6.38-13.52)。由于不可避免地涉及 ABI 变动，内核封装有了新版本，所有的第三方内核模块都不得不重新安装、重新编译。如果用户使用了 linux-restricted-modules，也必须同时更新。

参考链接: <http://security.ctocio.com.cn/95/12213095.shtml>

2.网络现 JAVA 高危漏洞

近日，一则披露 Oracle 公司 Java Applet Rhino 脚本引擎存在远程执行代码高危漏洞的消息遭披露，该漏洞的代码细节被完全公开。目前，该漏洞的演示程序已在国内多个安全论坛、主流论坛广泛传播，并有进一步扩大的趋势。专家指出，黑客利用该漏洞可以轻松制作含有恶意木马病毒的网页。由于 JAVA 组件被广泛安装在桌面电脑和服务器的上，浏览攻击者设计的网页会轻易被木马病毒所感染，可能导致计算机被完全控制，从而遭受虚拟帐号财产被盗、个人信息泄漏等损失。而大多数安全软件的网页防护功能，均无法抵御黑客基于此漏洞特制的挂马网页。据了解，微软在最新一期信息安全研究报告中称，最近一年内，微软信息安全团队总共侦测到 2750 万次瞄准 Java 漏洞的攻击，平均每季度 690 万次，JAVA 已经成为了继 Adobe 之后黑客的主要攻击目标。

参考链接: <http://www.enet.com.cn/article/2011/1202/A20111202943952.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