

信息安全漏洞周报

2012年9月10日-2012年9月16日

2012年第37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 179 个，其中高危漏洞 69 个、中危漏洞 100 个、低危漏洞 10 个。上述漏洞中，可利用来实施远程攻击的漏洞有 176 个。本周收录的漏洞中，已有 122 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“GNU glibc 'strcoll()'整数溢出漏洞”、“Ezylog photovoltaic management server 命令注入漏洞”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 179 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、天融信、安天实验室等单位报送数量较多。此外，来自 High-Tech Bridge Security Research Lab、亨达集团以及个人漏洞研究者向 CNVD 提交了 4 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
绿盟科技	152	0
启明星辰	186	0
安天实验室	34	0
恒安嘉新	16	0
天融信	23	0
安氏领信	10	0
东软	7	0
High-Tech Bridge Security Research Lab	2	2

亨达集团	1	1
个人报送者	1	1
报送总计	432	4
录入总计	179（去重）	4

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 FFmpeg、Apple、LimeSurvey、Siemens 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	FFmpeg	29	16%
2	Apple	25	14%
3	LimeSurvey	6	3%
4	Siemens	5	3%
5	McAfee	4	2%
6	Cisco	3	2%
7	Oracle	3	2%
8	Apache	3	2%
9	Microsoft	2	1%
10	Drupal	2	1%
11	其它	97	54%

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 179 个漏洞。其中操作系统漏洞 3 个，应用程序漏洞 134 个，WEB 应用漏洞 35 个，数据库漏洞 4 个，网络设备漏洞 1 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	3
应用程序漏洞	134
WEB 应用漏洞	35
网络设备漏洞	1
数据库漏洞	4
安全产品漏洞	2

表 3 漏洞按影响类型统计表

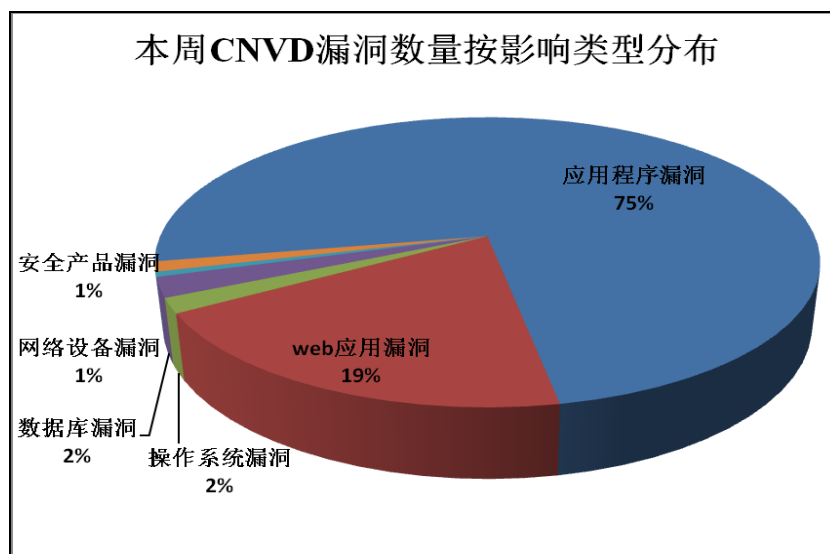


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 1 个网络设备漏洞：TP-LINK TL-WR340G 路由器拒绝服务漏洞。

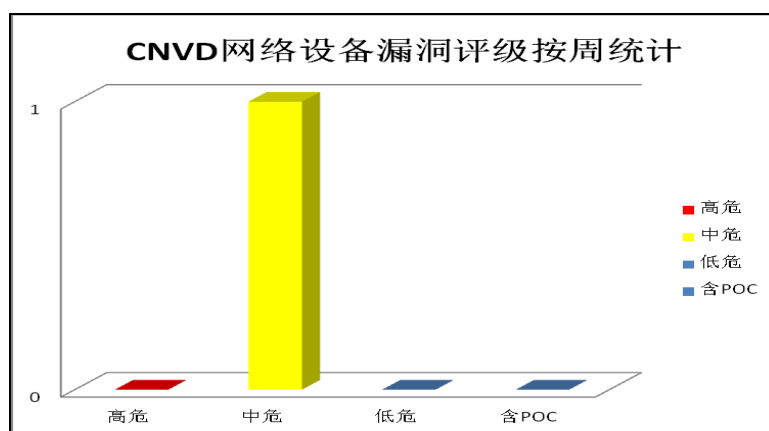


图 2 网络设备漏洞统计

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、Siemens 产品安全漏洞

Siemens SIMATIC 是一款采用工业控制领域自动化系统软件。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可读取系统文件；构建恶意 WEB 页，诱使用户解析，获得敏感信息或劫持用户会话；获得数据库信息或控制应用系统。

CNVD 收录的相关漏洞包括：Siemens SIMATIC WinCC 任意文件读取漏洞、Siemens

SIMATIC WinCC SOAP SQL 注入漏洞、Siemens SIMATIC WinCC 跨站请求伪造漏洞、Siemens SIMATIC WinCC ActiveX 控件账户信息泄露漏洞、Siemens SIMATIC WinCC 跨站脚本漏洞。其中，除“Siemens SIMATIC WinCC 任意文件读取漏洞”外，其余漏洞的综合评级均为“高危”。厂商已经修复了除“Siemens SIMATIC WinCC 跨站请求伪造漏洞”外的其余漏洞，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=56817
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56837
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56839
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56838
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56835

2、FFmpeg 安全漏洞

FFmpeg 是一款用于录制、转换和流化音视频的应用软件。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可使应用程序崩溃。

CNVD 收录的相关漏洞包括：FFmpeg ff_rv34_decode_frame 内存破坏漏洞（CNVD-2012-14412）、FFmpeg ff_MPV_frame_start 内存破坏漏洞（CNVD-2012-14410）、FFmpeg read_var_block_data 存在未明漏洞（CNVD-2012-14408）、FFmpeg ac3_decode_frame 存在未明漏洞（CNVD-2012-14375）、FFmpeg decode_frame 存在未明漏洞（CNVD-2012-14397）、FFmpeg decode_pic 存在未明漏洞（CNVD-2012-14405）、FFmpeg decode_slice_header 存在未明漏洞（CNVD-2012-14403）、FFmpeg decode_mb_info 存在未明漏洞（CNVD-2012-14385）等。其中，“FFmpeg ff_rv34_decode_frame 内存破坏漏洞（CNVD-2012-14412）”和“FFmpeg ff_MPV_frame_start 内存破坏漏洞（CNVD-2012-14410）”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=56644
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56642
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56640
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56598
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56629
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56637
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56635
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56617

3、LimeSurvey 安全漏洞

LimeSurvey 是一款开源的在线问卷调查软件。本周，该产品被披露存在多个安全漏

洞，攻击者利用漏洞可重定向用户信息，窃取敏感信息，执行任意 HTML 和脚本代码。

CNVD 收录的相关漏洞包括：LimeSurvey SQL 注入漏洞（CNVD-2012-14354、CNVD-2012-14353、CNVD-2012-14352、CNVD-2012-14356）、LimeSurvey 重定向漏洞（CNVD-2012-14355）、LimeSurvey 跨站脚本漏洞（CNVD-2012-14357）。其中，“LimeSurvey SQL 注入漏洞（CNVD-2012-14354、CNVD-2012-14353、CNVD-2012-14352、CNVD-2012-14356）”的综合评级均为“高危”。目前，厂商尚未发布修复程序。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=56537
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56538
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56536
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56535
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56539
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56540

4、Microsoft 产品安全漏洞

Microsoft System Center Configuration Manager 是一款可通过控制台来管理物理的、虚拟的和移动设备的客户端软件。本周，该产品被披露存在多个漏洞，攻击者利用漏洞，可构建恶意 WEB 页，诱使解析，获得敏感信息或劫持用户会话。

CNVD 收录的相关漏洞包括：Microsoft System Center Configuration Manager 跨站脚本漏洞、Microsoft Visual Studio Team Foundation Server 跨站脚本漏洞。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=56755
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=56775

5、Ezylog photovoltaic management server 命令注入漏洞

Ezylog photovoltaic management server 是一款 SCADA 产品，即数据采集与监视控制系统。本周，Ezylog photovoltaic management server 被披露存在一个综合评级为“高危”的命令注入漏洞。攻击者利用漏洞可以以管理员权限执行任意命令。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=56795

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-2012-14460	Citrix Receiver 和 Online 插件存在未明任意代码执行漏洞	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://support.citrix.com/article/CTX134681
CNVD-2012-14464	Knowledge Base Enterprise Edition 'category'参数 SQL 注入漏洞	高	暂无
CNVD-2012-14459	TCEexam SQL 注入漏洞	高	TCEexam 11.3.009 已经修复此漏洞，建议用户下载使用： http://freecode.com/projects/tcexam/releases/347588
CNVD-2012-14470	Openfiler 'NetworkCard'对象远程命令执行漏洞	高	暂无
CNVD-2012-14478	PHPList SQL 注入漏洞（CNVD-2012-14478）	高	厂商已经发布了升级补丁修复该漏洞： www.phplist.com/
CNVD-2012-14473	Joomla Kunena 'id'参数 SQL 注入漏洞	高	暂无
CNVD-2012-14476	Oreans Themida 缓冲区溢出漏洞	高	目前厂商已经发布了升级补丁以修复该漏洞，请到厂商的主页下载： http://www.oreans.com
CNVD-2012-14448	DeltaScripts PHP Links 存在多个 SQL 注入漏洞	高	暂无
CNVD-2012-14433	Open Source Competency Center (OSCC) MyMeeting/MyMesyuarat 任意代码执行漏洞	高	MyMesyuarat 09b-2 已经修复此漏洞，建议用户下载使用： http://sourceforge.net/projects/mymesyuarat/files/mymesyuarat/mymesyuarat-ver0.9b-2.zip/download
CNVD-2012-14444	libguac 远程缓冲区溢出漏洞	高	暂无
CNVD-2012-14438	IBM Java 存在多个未明漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，FFmpeg、LimeSurvey 及 Microsoft 产品被披露存在多个安全漏洞，攻击者利用漏洞可获得敏感信息或劫持用户会话，执行任意 HTML 和脚本代码，使应用程序崩溃。此外，Siemens SIMATIC 以及 Ezylog photovoltaic management server 等工业控制系统软件也被披露存在高危漏洞或零日漏洞，相关行业用户需加强防范。



CNVD 整理和发布以下重要安全修补信息。

1、Cisco 发布升级程序，修补多款产品漏洞

本周，Cisco 发布升级程序，修补了多款产品存在的漏洞。攻击者可以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=22211
http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=22213



本周要闻速递

1. 微软着手修复 IE10 浏览器中的 Flash 漏洞

此前报道过微软的 IE10 浏览器不支持 Flash 的最新版更新，而最新的 Flash 中包含了重要的漏洞修复补丁，这一度让用户不敢使用 IE10 浏览器。不过微软现在已经着手解决这个问题了，据悉 IE10 中的 Flash 漏洞修复工作已经开始，而且将很快发布，预计本周就能完成本次修复。据最新的消息，微软的工作人员正在对程序进行风险测试，相信不久就可以将升级补丁发放给用户下载。

参考链接：<http://tech.sina.com.cn/s/2012-09-12/12527609663.shtml>

2. Adobe 为 Flash Player 的漏洞提供补丁

Adobe 为使用广泛的 Adobe Reader 和 Acrobat 软件发布关键的安全更新，修复了一个危险的 Flash Player 漏洞、并且纠正在这些软件中的 20 个缺陷。该安全更新涉及到 Adobe 公司 11.3.300.270 版本的 Flash Player、以及更早的运行在 Windows、Macintosh 和 Linux 平台的版本。Adobe 公司正在督促 Windows 平台上使用 9.5.2 版本 Acrobat 和 Reader 的用户应用该安全更新。该更新文件纠正了各种各样的 Acrobat 和 Reader 编码错误，它们可能导致内存崩溃以及栈和缓冲区溢出状况。该安全更新还适用于在运行在 Mac 和 Windows 平台上其它版本的 Adobe Reader 和 Reader 用户。此外，Adobe 还发布了一个更新文件，纠正了在 Shockwave Player 中的 5 个漏洞。该更新文件影响到 11.6.5.635 和更早的版本。

参考链接：<http://security.ctocio.com.cn/375/12426875.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