

信息安全漏洞周报

2013 年 05 月 27 日-2013 年 06 月 02 日

2013 年第 22 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 154 个，其中高危漏洞 57 个、中危漏洞 88 个、低危漏洞 9 个。上述漏洞中，可利用来实施远程攻击的漏洞有 144 个。本周收录的漏洞中，已有 109 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“YeaLink IP Phone SIP-T20P/SIP-T26P 安全绕过漏洞”、“Weyal CMS 存在多个 SQL 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 6 家成员单位及个人报送了本周收录的全部 154 个漏洞。各单位报送情况如表 1 所示。其中，安天实验室、启明星辰、天融信、绿盟科技等单位报送数量较多。此外，奇虎 360 和个人报送者向 CNVD 提交了 25 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	77	0
绿盟科技	40	0
安天实验室	98	0
天融信	61	0
恒安嘉新	24	0
奇虎 360	4	4
个人	22	21
报送总计	325	25
录入总计	154（去重）	25

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 WordPress、Apple、X.Org、Cisco 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	WordPress	18	12%
2	Apple	12	8%
3	X.Org	10	6%
4	Cisco	8	5%
5	Apache	4	3%
6	Red Hat	4	3%
7	IBM	4	3%
8	Siemens	3	2%
9	Novell	2	1%
10	TP-LINK	1	1%
11	其它	88	56%

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 154 个漏洞。其中应用程序漏洞 91 个，WEB 应用漏洞 40 个，网络设备漏洞 14 个，操作系统漏洞 4 个，安全产品漏洞 5 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	91
WEB 应用漏洞	40
网络设备漏洞	14
操作系统漏洞	4
安全产品漏洞	5
数据库漏洞	0

表 3 漏洞按影响类型统计表

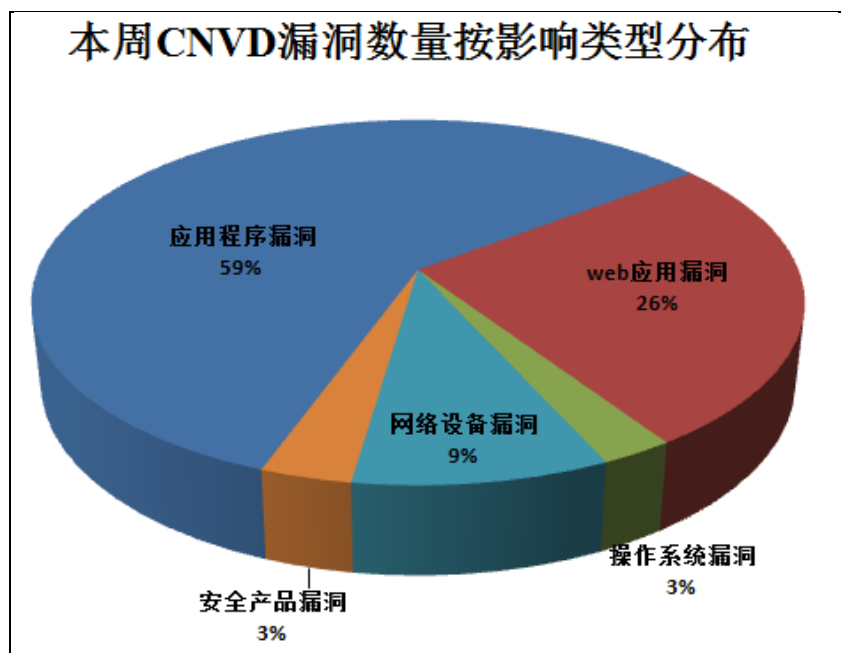


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 14 个网络设备漏洞：Zavio IP Cameras 验证绕过漏洞、Zavio IP Cameras OS 命令注入漏洞、Zavio IP Cameras RTSP 认证预设漏洞、Zavio IP Cameras 授权 OS 命令注入漏洞、Sony Playstation 3 文件处理本地命令执行漏洞、Siemens Scalance X200 系列交换机 SNMPv3 远程安全绕过漏洞、TP-LINK TL-WR842ND 目录遍历漏洞、YeaLink IP Phone SIP-T20P/SIP-T26P 安全绕过漏洞、Cisco Nexus 1000V VSM/VEM Heartbeat 远程拒绝服务漏洞、Cisco Nexus 1000V VSM 到 vCenter 通信中间人攻击漏洞、Cisco Nexus 1000V 不充分 VSM/VEM 验证漏洞、Cisco Nexus 1000V ESXi Hypervisor 拒绝服务漏洞、Cisco Nexus 1000V VSM/VEM 通信加密绕过漏洞、Cisco Nexus 1000V VSM/VEM 通信加密存在漏洞。其中，“Siemens Scalance X200 系列交换机 SNMPv3 远程安全绕过漏洞”和“YeaLink IP Phone SIP-T20P/SIP-T26P 安全绕过漏洞”的综合评级为“高危”。

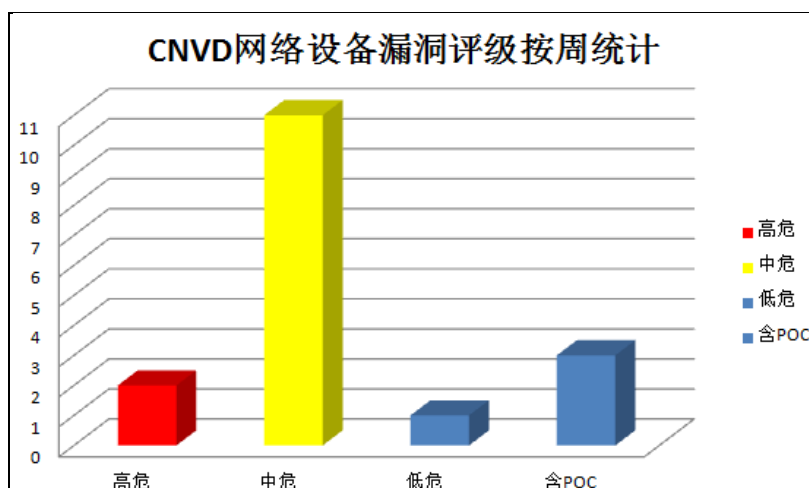


图 2 网络设备漏洞统计

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、Apple QuickTime 安全漏洞

Apple QuickTime 是一款内置多媒体播放器。本周，该产品被披露存在多个安全漏洞，远程攻击者利用漏洞构建恶意文件，诱使用户解析，可使应用程序崩溃或执行任意代码。

CNVD 收录的相关漏洞包括：Apple QuickTime JPEG 编码数据处理缓冲区溢出漏洞、Apple QuickTime 'mvhd' atoms 处理缓冲区溢出漏洞、Apple QuickTime 'enof' atoms 处理缓冲区溢出漏洞、Apple QuickTime QTIF 文件处理内存破坏漏洞、Apple QuickTime FPX 文件处理缓冲区溢出漏洞、Apple QuickTime MP3 文件处理缓冲区溢出漏洞、Apple QuickTime TeXML 文件处理内存破坏漏洞、Apple QuickTime H.263 编码电影文件处理缓冲区溢出漏洞等。上述漏洞的综合评级均为“高危”。厂商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/flaw/show/CNVD-2013-25617>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25198>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25187>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25188>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25189>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25190>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25191>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25192>

2、Cisco 产品安全漏洞

Cisco Nexus 系列交换机是数据中心级交换机；Cisco WebEx Social 是企业协作平台；

Cisco IOS 是思科系统路由器和网络交换机上使用的互连网络操作系统。本周，上述产品被披露存在安全漏洞，攻击者利用漏洞欺骗服务器，获取敏感信息，进行拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco Nexus 1000V VSM/VEM 通信加密存在漏洞、Cisco Nexus 1000V VSM/VEM 通信加密绕过漏洞、Cisco Nexus 1000V ESXi Hypervisor 拒绝服务漏洞、Cisco Nexus 1000V 不充分 VSM/VEM 验证漏洞、Cisco Nexus 1000V VSM 到 vCenter 通信中间人攻击漏洞、Cisco Nexus 1000V VSM/VEM Heartbeat 远程拒绝服务漏洞、Cisco WebEx for iOS 证书验证安全绕过漏洞、Cisco IOS XR Software SNMP 拒绝服务漏洞。厂商已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/flaw/show/CNVD-2013-25633>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25631>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25630>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25626>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25623>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25622>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25385>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25337>

3、IBM 产品安全漏洞

IBM WebSphere Portal 是一款基于 SOA 的解决方案；IBM WebSphere DataPower SOA Appliances 是 IBM 针对面向服务架构(SOA)这一整体方案中的重要组件；IBM Tivoli Monitoring 用于提供基本系统资源的监控特性，以检测系统瓶颈和潜在的问题；IBM Rational Directory Server 是为兼容的 Rational 工具提供集中通用基础架构服务或用户验证、用户管理、组定义、用户数据存储和应用数据存储的解决方案。本周，上述产品被披露存在多个安全漏洞。远程攻击者利用漏洞发送恶意应答给用户，进行欺骗等攻击，获取用户敏感信息或劫持用户会话。

CNVD 收录的相关漏洞包括：IBM WebSphere Portal HTTP 应答分片漏洞、IBM WebSphere DataPower SOA Appliances 跨站脚本漏洞、IBM Tivoli Monitoring Portal Browser 客户端跨站脚本漏洞、IBM Rational Directory Server 帮助文件系统调试信息泄漏洞。厂商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/flaw/show/CNVD-2013-25606>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25419>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25407>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25406>

4、Apache 产品安全漏洞

Apache Tomcat 是一款开源 JSP 应用服务器程序; Apache Struts 框架是一个基于 Java Servlets, JavaBeans 和 JavaServer Pages (JSP) 的 Web 应用框架的开源项目。本周, 上述产品被披露存在多个安全漏洞, 远程攻击者利用漏洞绕过某些安全限制, 执行未授权操作, 造成拒绝服务并执行任意代码。

CNVD 收录的相关漏洞包括: Apache Tomcat DIGEST Authentication 重放攻击漏洞、Apache Tomcat 不安全临时文件处理漏洞、Apache Struts 'includeParams' 不完整修复安全绕过漏洞、Apache Struts2 Showcase 应用远程命令执行漏洞。其中, “Apache Struts2 Showcase 应用远程命令执行漏洞”、Apache Struts 'includeParams' 不完整修复安全绕过漏洞的综合评级均为“高危”。目前, 互联网上已经出现了“Apache Struts2 Showcase 应用远程命令执行漏洞”的攻击代码。厂商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/flaw/show/CNVD-2013-25530>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25529>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25473>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25257>

5、YeaLink IP Phone SIP-T20P/SIP-T26P 安全绕过漏洞

YeaLink IP Phone SIP-T20P/SIP-T26P 是 IP 电话设备。本周, 该产品被披露存在一个综合评级为“高危”的安全绕过漏洞。攻击者利用漏洞使用第一个可用 SIP 账户, 无需用户确认即可打电话, 并且呼叫者也可以通过话筒监听。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/flaw/show/CNVD-2013-25617>

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/flaw/list.htm>

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2013-25481	LibRaw 'exposure correction'缓冲区溢出漏洞	高	LibRaw 0.15.1 已修复此漏洞, 建议用户下载使用: http://www.libraw.org/download
CNVD-2013-25485	Siemens Solid Edge SEListCtrlX ActiveX 内存破坏漏洞	高	暂无
CNVD-2013-25410	Mesa libGLX 远程代码执行漏洞	高	用户可参考如下厂商提供的安全公告获得补丁信息: http://lists.freedesktop.org/archives/mesa-dev/2013-May/039720.html

			http://lists.freedesktop.org/archives/mesa-dev/2013-May/039722.html
CNVD-2013-25486	Siemens Solid Edge WebPartHelper ActiveX 远程代码执行漏洞	高	暂无
CNVD-2013-25541	Red Hat Certificate System 格式串漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://rhn.redhat.com/errata/RHSA-2013-0856.html
CNVD-2013-25561	AVE.CMS 'index.php' SQL 注入漏洞	高	暂无
CNVD-2013-25585	Siemens Scalance X200 系列交换机 SNMPv3 远程安全绕过漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： http://www.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens_se
CNVD-2013-25420	Weyal CMS 存在多个 SQL 注入漏洞	高	暂无
CNVD-2013-25422	X.Org libFS 'FSOpenServer()' 内存破坏漏洞	高	用户可参考如下厂商提供的安全公告获得补丁信息： http://cgit.freedesktop.org/xorg/lib/libFS/commit/?id=26dc23446c2e7818fdebfb46e101bac4883df07e
CNVD-2013-25479	ERDAS ER Viewer 'rf_report_error()' 函数栈缓冲区溢出漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，Apple Quicktime 播放器被披露存在多个安全漏洞，攻击者利用漏洞欺骗服务器，获取敏感信息，或造成拒绝服务攻击。Apache 被披露存在多个安全漏洞，远程攻击者利用漏洞绕过某些安全限制，执行未授权操作，造成拒绝服务或取得系统管理权限。而 Cisco 和 IBM 多款产品也被披露存在多个漏洞，相关企业用户应重点加强防范。此外，YeaLink 被披露存在高危零日漏洞，建议相关用户应随时关注厂商主页，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、Red Hat 发布升级程序，修补多款产品安全漏洞

Red Hat Certificate System 是一款认证系统。Red Hat Network Satellite 是一款基于

Linux 架构的系统管理工具。Red Hat 'livecd-tools'提供对 Kickstart 文件的读/执行支持以用于创建系统映像。本周，Red Hat 发布升级程序，修补了多款产品存在的漏洞。远程攻击者可利用漏洞执行任意代码，绕过安全限制，获取敏感信息。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/patchInfo/show/34371>

<http://www.cnvd.org.cn/patchInfo/show/34372>

<http://www.cnvd.org.cn/patchInfo/show/34373>

<http://www.cnvd.org.cn/patchInfo/show/34326>

本周要闻速递

1. “超级网银”被曝存安全漏洞

“超级网银”作为央行 2009 年开发的一套跨行财务管理产品，并且于 2010 年 8 月升级为第二代的“超级网银”，在技术上是安全成熟的。但根据网友反馈，很少用户意识到，自己的银行账户可以授权给别人任意转账。通俗地说，就是可以用一个网银账户，实现多张银行卡的跨行查询和转账，国内绝大多数银行均默认支持该项功能。然而一旦有不法分子恶意利用“超级网银”，通过欺诈手段获取他人银行账户的授权，就可以将对方账户余额全部偷走。鉴于“超级网银”授权链接都是银行官网地址，此前没有任何安全软件会对其报警拦截。业界专家建议用户警惕陌生人发来的此类链接。

参考链接：<http://tech.sina.com.cn/i/2013-06-01/12388401865.shtml>

2. 甲骨文将解决多个 Java 安全漏洞

近日甲骨文宣布将解决 Java 安全漏洞问题，包括添加集中策略管理与企业环境白名单功能。随着主要科技公司的高质量科技研发和软件违规使用，包括苹果和 Facebook 在内都存在 Web 插件的安全问题。“甲骨文此举意在有助于减少潜在危险利用性和 Java 漏洞在桌面环境中的严重性,为 Java 操作在服务器环境中提供额外的安全保护,”甲骨文 Java 平台的软件开发团队领导拉马尼透露。同时，早些时候由于黑客成功攻击苹果、Facebook、微软和其他公司引发了关于 Java 安全价值的争议，原因在于在系统运行 Web 插件时没有修补漏洞而遭受了零日攻击。甲骨文向 Java 的前持有者 Sun 微系统公司表示，他们不得不采用 Oracle 的修复计划以解决“优先顺序”和“特定时间”等问题。

参考链接：<http://www.zuitech.com/26958.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