

信息安全漏洞周报

2013 年 06 月 17 日-2013 年 06 月 23 日

2013 年第 25 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 195 个，其中高危漏洞 64 个、中危漏洞 114 个、低危漏洞 17 个。上述漏洞中，可利用来实施远程攻击的漏洞有 178 个。本周收录的漏洞中，已有 150 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“Fobuc Guestbook 'index.php' SQL 注入漏洞”、“Syslog Server 远程拒绝服务漏洞”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 8 家成员单位及个人报送了本周收录的全部 195 个漏洞。各单位报送情况如表 1 所示。其中，启明星辰、安天实验室、天融信、绿盟科技等单位报送数量较多。此外，知道创宇公司和个人报送者向 CNVD 提交了 10 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	115	0
绿盟科技	53	0
安天实验室	102	0
天融信	95	0
恒安嘉新	16	0
东软	1	0
知道创宇	4	4
个人	6	6
报送总计	392	10

录入总计	195（去重）	10
------	---------	----

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Oracle、Microsoft、FFmpeg、IBM 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	Oracle	38	19%
2	Microsoft	24	12%
3	FFmpeg	13	7%
4	IBM	11	6%
5	Siemens	8	4%
6	WordPress	6	3%
7	Apache	5	3%
8	Airlive	5	3%
9	Cisco	4	2%
10	Red Hat	3	2%
11	其它	78	39%

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 195 个漏洞。其中应用程序漏洞 155 个，WEB 应用漏洞 16 个，网络设备漏洞 17 个，操作系统漏洞 6 个，安全产品漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	155
WEB 应用漏洞	16
网络设备漏洞	17
操作系统漏洞	6
安全产品漏洞	1
数据库漏洞	0

表 3 漏洞按影响类型统计表

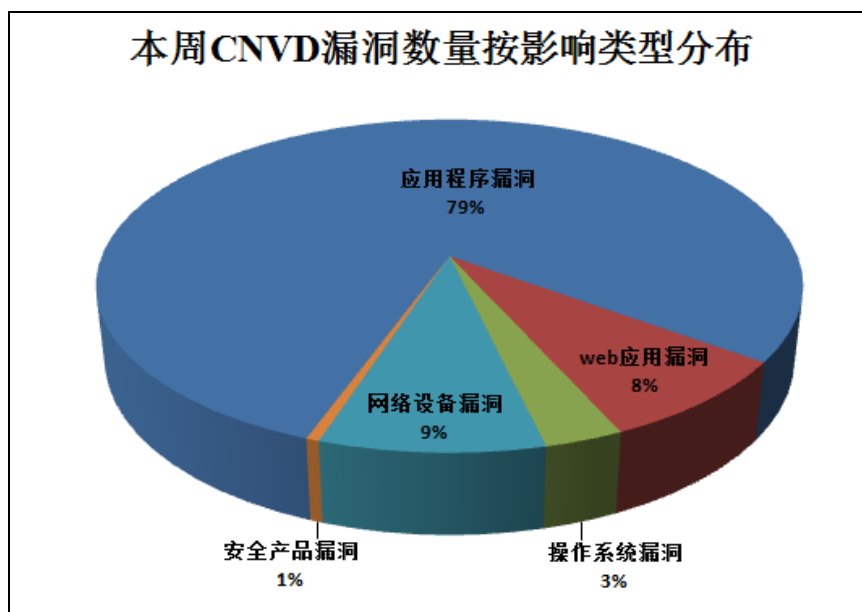


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 17 个网络设备漏洞：Cisco Secure Access Control System (ACS) 报告查看信息泄漏漏洞、多个 Ubiquiti airCam 产品远程缓冲区溢出漏洞、TP-LINK TL-SC3171 IP Camera 身份验证绕过漏洞、D-Link DIR-615 存在多个远程漏洞、Airlive IP Cameras 跨站请求伪造漏洞、Samsung SHR-5162 和 SHR-5082 存在未明跨站脚本漏洞、Sony CH/DH Series IP Cameras 跨站请求伪造漏洞、Linksys N300 Router 'submit_button' 跨站脚本漏洞、Airlive IP Cameras 目录遍历漏洞、Airlive IP Cameras 备份文件信息泄漏漏洞、Airlive IP Cameras 拒绝服务漏洞、Brickcom Multiple IP Cameras 信息泄漏漏洞、Brickcom Multiple IP Cameras 跨站请求伪造漏洞、Buffalo WZR-HP-G300NH2 跨站请求伪造漏洞、多个佳能打印机验证检查安全绕过漏洞、多个佳能打印机信息泄漏漏洞、多个佳能打印机拒绝服务漏洞。

其中，“D-Link DIR-615 存在多个远程漏洞”的综合评级为“高危”。目前，互联网上已经出现了针对“多个 Ubiquiti airCam 产品远程缓冲区溢出漏洞、D-Link DIR-615 存在多个远程漏洞、Airlive IP Cameras 跨站请求伪造漏洞、Sony CH/DH Series IP Cameras 跨站请求伪造漏洞、Airlive IP Cameras 目录遍历漏洞、Airlive IP Cameras 拒绝服务漏洞、Brickcom Multiple IP Cameras 跨站请求伪造漏洞、Buffalo WZR-HP-G300NH2 跨站请求伪造漏洞、多个佳能打印机拒绝服务漏洞”的攻击代码。相关厂商已经发布了漏洞修复程序。

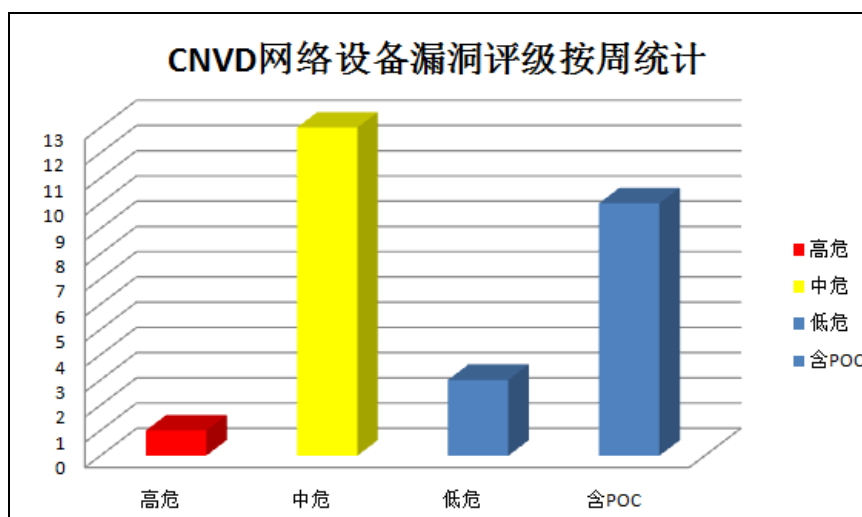


图 2 网络设备漏洞统计

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、Microsoft 产品安全漏洞

Microsoft Internet Explorer 是一款流行的 WEB 浏览器; Microsoft Windows 是一款流行的操作系统; Microsoft Office 是基于 Windows 操作系统的办公软件套装。本周，上述微软产品被披露存在多个安全漏洞，远程攻击者利用漏洞可导致应用程序崩溃，执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer 内存破坏漏洞（CNVD-2013-26677）、Microsoft Windows TCP/IP Driver 畸形报文处理远程拒绝服务漏洞、Microsoft Office PNG File 缓冲区溢出漏洞、Microsoft Internet Explorer 存在未明内存破坏漏洞（CNVD-2013-26553、CNVD-2013-26552、CNVD-2013-26549）、Microsoft Internet Explorer WEB 页脚本调试内存破坏漏洞、Microsoft Internet Explorer 存在未明内存破坏漏洞（CNVD-2013-26550）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-2013-26677>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26557>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26554>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26553>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26552>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26551>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26550>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26549>

2、Oracle 产品安全漏洞

Oracle Java Runtime Environment 是一款为 JAVA 应用程序提供运行环境的解决方案。本周，该产品被披露存在安全漏洞，攻击者利用漏洞可执行任意代码。

CNVD 收录的相关漏洞包括：Oracle Java JDK / JRE 2D 子件存在未明任意代码执行漏洞（CNVD-2013-26943、CNVD-2013-26942）、Oracle Java JDK / JRE Deployment 子件存在未明任意代码执行漏洞（CNVD-2013-26941）、Oracle Java JDK / JRE Libraries 子件存在未明漏洞（CNVD-2013-26940）、Oracle Java JDK / JRE Serviceability 子件存在未明任意代码执行漏洞、Oracle Java JDK / JRE AWT 子件存在未明任意代码执行漏洞（CNVD-2013-26938）、Oracle Java JDK / JRE Sound 子件存在未明任意代码执行漏洞、Oracle Java JDK / JRE HotSpot 子件存在未明拒绝服务漏洞等。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-2013-26943>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26942>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26941>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26940>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26939>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26938>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26927>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26924>

3、Siemens 产品安全漏洞

Siemens SIMATIC WinCC 是工业控制领域监测控制和数据采集及人机界面 HMI 系统；Siemens SIMATIC PCS 是工业控制领域过程控制系统；Siemens OpenScape 是一款统一通信软件平台；Siemens COMOS 是一体化软件解决方案，用于工厂及机械设备资产的整个生命周期内对其进行全盘设计和管理。本周，上述产品被披露存在多个安全漏洞。攻击者利用漏洞或绕过安全限制，获得未授权的访问获取敏感信息，或执行 SQL 查询或 OS 命令。

CNVD 收录的相关漏洞包括：Siemens SIMATIC WinCC/PCS 7 硬编码凭证安全绕过漏洞、Siemens SIMATIC WinCC/PCS 7 SQL 注入漏洞、Siemens OpenScape 产品 OS 命令注入漏洞、Siemens COMOS 本地安全绕过漏洞、Siemens OpenScape 产品敏感信息泄漏漏洞、Siemens OpenScape 产品文件泄漏漏洞、Siemens OpenScape 产品跨站脚本漏洞、Siemens SIMATIC WinCC/PCS 7 用户名枚举漏洞等。其中，“Siemens SIMATIC WinCC/PCS 7 硬编码凭证安全绕过漏洞、Siemens SIMATIC WinCC/PCS 7 SQL 注入漏洞、Siemens OpenScape 产品 OS 命令注入漏洞”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-2013-26800>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26803>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26890>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26957>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26891>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26889>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26888>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26802>

4、Apache 产品安全漏洞

Apache Santuario 是实现 XML 的安全标准组件；OpenJPA 是 Apache 组织提供的开源项目，实现了 EJB 3.0 中的 JPA 标准，提供数据管理框架。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可导致应用程序崩溃，执行任意代码。

CNVD 收录的相关漏洞包括：Apache Santuario XML Security for C++远程堆缓冲区溢出漏洞、Apache Santuario XML Security for C++远程栈缓冲区溢出漏洞、Apache Santuario XML Security for C++远程拒绝服务漏洞、Apache Santuario XML Security for C++签名绕过漏洞、Apache OpenJPA 对象反序列化任意文件创建或覆盖漏洞。其中，“Apache Santuario XML Security for C++远程堆缓冲区溢出漏洞、Apache Santuario XML Security for C++远程栈缓冲区溢出漏洞”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-2013-26956>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26954>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26955>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26953>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26898>

5、Fobuc Guestbook 'index.php' SQL 注入漏洞

Fobuc Guestbook 是一款基于 WEB 的留言本系统。本周，该产品被披露存在一个综合评级为“高危”的 SQL 注入漏洞。通过"category" GET 参数传递给 index.php 的输入在用于 SQL 查询之前缺少过滤，远程攻击者利用漏洞可注执行恶意 SQL 查询，获取数据库信息或控制应用系统。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-2013-26581>

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-2013-26908	JustSystems 多个产品存在未明任意代码执行漏洞	高	用户可参考如下厂商提供的安全公告获得补丁信息： http://www.justsystems.com/jp/info/js13002.html
CNVD-2013-26959	ZamFoo 'zamfoo_do_restore_zamfoo_backup.cgi'任意命令执行漏洞	高	暂无
CNVD-2013-26958	Symantec Endpoint Protection Manager 远程缓冲区溢出漏洞	高	Symantec Endpoint Protection Management Console 12.1 RU3 已经修复此漏洞，建议用户下载更新： http://www.symantec.com/business/endpoint-protection
CNVD-2013-26843	REDCap 存在多个未明漏洞	高	REDCap 5.1.1 已经修复此漏洞，建议用户下载更新： http://www.project-redcap.org/
CNVD-2013-26849	WordPress Leaflet Maps Marker 插件 SQL 注入漏洞	高	WordPress Leaflet Maps Marker Plugin 3.5.3 已经修复此漏洞，建议用户下载更新： http://www.mapsmarker.com/
CNVD-2013-26829	IBM Tivoli Monitoring 拒绝服务漏洞（CNVD-2013-26829）	高	用户可参考如下厂商提供的安全公告获得补丁信息： http://www-01.ibm.com/support/docview.wss?uid=swg21635080
CNVD-2013-26825	Havalite CMS 'upload.php'任意文件上传漏洞	高	暂无
CNVD-2013-26563	Simple PHP Agenda 'edit_event.php' SQL 注入漏洞	高	php-agenda 2.2.9 已经修复此漏洞，建议用户下载更新： http://sourceforge.net/projects/php-agenda/
CNVD-2013-26728	D-Link DIR-615 存在多个远程漏洞	高	暂无
CNVD-2013-26821	Fly-High CMS 'upload.php'任意文件上传漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，Microsoft、Oracle、Apache 的多款产品被披露存在多个漏洞，个人和

企业用户应注意加强防范上述漏洞威胁。本周 Siemens 多款工控产品被披露存在漏洞，攻击者利用漏洞绕过安全限制，严重的可获得相关生产系统控制权。此外，Fobuc Guestbook 留言本系统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 Enterprise Virtualization Manager 是一款虚拟化解决方案应用。Red Hat Enterprise Virtualization Hypervisor 是专用的 KVM 管理程序。本周，Red Hat 发布升级程序，修补了多款产品存在的拒绝服务和权限提升漏洞。攻击者可以利用漏洞使主机崩溃或以 SYSTEM 权限执行任意恶意程序。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/34646>
<http://www.cnvd.org.cn/patchInfo/show/34645>
<http://www.cnvd.org.cn/patchInfo/show/34644>

本周要闻速递

1. 微软悬赏 10 万美元寻找 Win8 安全漏洞

周二，微软宣布愿意对关于 Windows 安全漏洞的信息支付最高 10 万美元的奖金，就从本月末即将发布的 Windows 8.1 预览版开始。对于能为阻止类似漏洞日后被利用而提供新防御技术的研究者们，微软将为每份方案提供价值 5 万美元的额外“防御奖金”。除了这些 10 万和 5 万美元的大奖之外，微软还将为影响 IE 11 预览版的漏洞支付 1.1 万美元，这项策略是为了在该软件向消费者广泛发布前修复漏洞。

参考链接：<http://news.163.com/13/0621/18/91TPI6A600014JB5.html>

2. Facebook 安全漏洞导致 600 万个用户信息泄露

6 月 24 日消息，据国外媒体报道，上周末，Facebook 安全团队称发现一项安全漏洞，这个漏洞是 Download Your Information(DYI)将导致用户的 email 或手机号码泄露给其他用户。目前，有 600 万个用户账号恐遭遇泄露。Facebook 安全团队称，发生泄露的原因，是当用户从联络人名单或地址簿上传到 Facebook 时，Facebook 便会从其他用户的联络人信息进行对比，从而找出用户之间的关联、并进行推荐。但因为漏洞的存在，部分信息包含交友建议、以及减少 Facebook 邀请数量的信息，会在无意中被记录下来，如果用户帐户下载了 Download Your Information(DYI)工具，下载了他们的 Facebook 用

户帐户信息，便可看到其他联络人、或曾经联络过的人的 email 或手机电话号码。

参考链接：<http://site.qudong.com/2013/0624/147058.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