

信息安全漏洞周报

2013 年 10 月 21 日-2013 年 10 月 27 日

2013 年 第43 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 264 个，其中高危漏洞 53 个、中危漏洞 178 个、低危漏洞 33 个。上述漏洞中，可利用来实施远程攻击的漏洞有 232 个。本周收录的漏洞中，已有 212 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“Elite CMS Pro 'page'参数 SQL 注入漏洞”、“D-Link DIR-100 'RuntimeDiagnosticPing'缓冲区溢出漏洞”等零日攻击代码，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 家成员单位及个人报送了本周收录的全部 264 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、天融信等单位报送数量较多。此外，安天实验室和个人报送者向 CNVD 提交了 48 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
安天实验室	160	1
启明星辰	132	0
天融信	60	0
绿盟科技	21	0
恒安嘉新	10	0
个人	47	47
报送总计	430	48
录入总计	264（去重）	48

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、Apple、Cisco 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	Oracle	92	35%
2	Apple	34	13%
3	Cisco	18	7%
4	IBM	11	4%
5	wordpress	7	3%
6	HP	5	2%
7	ReviewBoard	3	1%
8	VMware	2	1%
9	Linux	1	1%
10	其它	91	33%

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 264 个漏洞。其中应用程序漏洞 167 个，操作系统漏洞 42 个，WEB 应用漏洞 31 个，网络设备漏洞 15 个，数据库漏洞 6 个，安全产品漏洞 3 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	167
操作系统漏洞	42
WEB 应用漏洞	31
网络设备漏洞	15
数据库漏洞	6
安全产品漏洞	3

表 3 漏洞按影响类型统计表

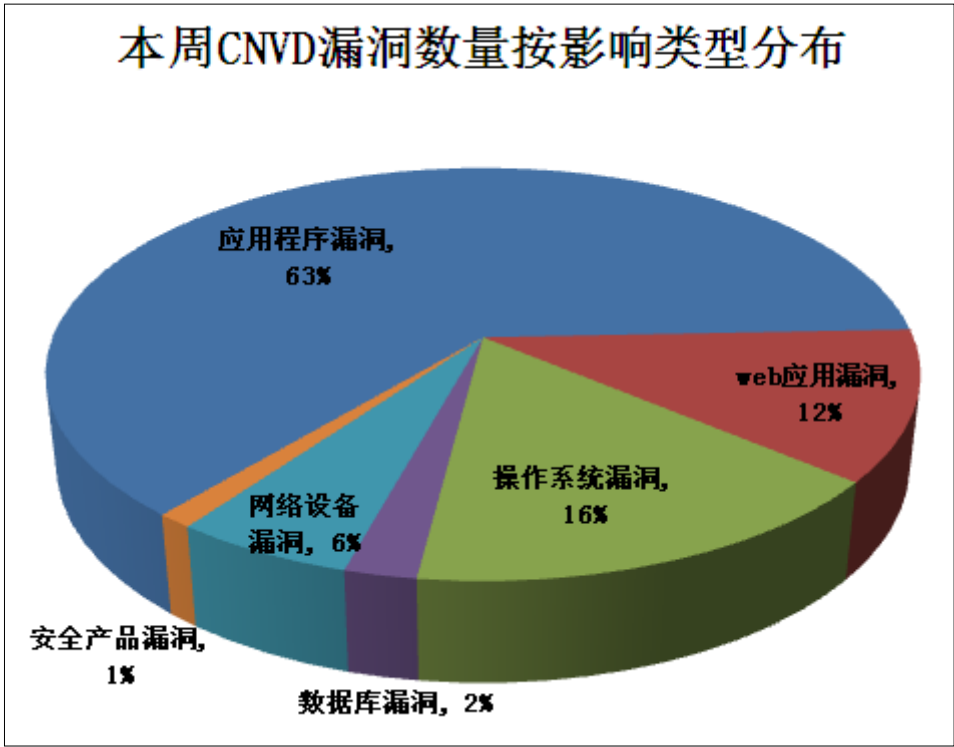


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 22 个电信行业漏洞、5 个移动互联网行业漏洞和 1 个工控系统行业漏洞（如下列表所示）。其中，“D-Link DIR-605L CAPTCHA Data 栈缓冲区溢出漏洞”、“D-Link DIR-100 'RuntimeDiagnosticPing'缓冲区溢出漏洞”、“Tenda 无线路由器远程命令执行后门漏洞”、“Nano-10 PLC 远程拒绝服务漏洞”的综合评级均为“高危”。相关厂商已经发布了漏洞修复程序。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2013-14072	Cisco Secure Access Control System 远程拒绝服务漏洞（CNVD-2013-14072）	中	是
电信	CNVD-2013-14064	D-Link DIR-605L CAPTCHA Data 栈缓冲区溢出漏洞	高	否
电信	CNVD-2013-14029	TRENDnet N300 Routers 存在多个未明漏洞	中	是
电信	CNVD-2013-13992	IBM Tivoli Endpoint Manager LDAP/AD 验证控制台用户伪造漏洞	中	是
电信	CNVD-2013-14082	DrayTek Vigor 2700 ADSL 路由器命令注入漏洞	中	否
电信	CNVD-2013-13967	IBM WebSphere DataPower	中	是

		XC10 Appliance 存在未明漏洞 (CNVD-2013-13967)		
电信	CNVD-2013-13966	IBM WebSphere DataPower XC10 Appliance 未授权访问漏 洞 (CNVD-2013-13966)	中	是
电信	CNVD-2013-13957	D-Link DIR-100 'RuntimeDiagnosticPing'缓冲区 溢出漏洞	高	否
电信	CNVD-2013-14023	IBM Integration Bus XML4J 解 析器实体扩展拒绝服务漏洞	中	是
电信	CNVD-2013-14016	ARRIS DG860A 'router.data' NVRAM 备份文件远程信息泄 露漏洞	中	否
电信	CNVD-2013-13947	Cisco Unity Connection 目录遍 历漏洞	中	是
电信	CNVD-2013-13873	HP LaserJet Pro 打印机远程管 理员密码泄露漏洞	中	是
电信	CNVD-2013-13948	Tenda 无线路由器远程命令执 行后门漏洞	高	否
电信	CNVD-2013-13807	IBM WebSphere eXtreme Scale 监测控制台跨站脚本漏洞	低	是
电信	CNVD-2013-13808	IBM WebSphere eXtreme Scale 监测控制台存在未明信息泄 露漏洞	中	是
电信	CNVD-2013-13809	Cisco WebEx Meetings Server 部署口令校验安全绕过漏洞	中	是
电信	CNVD-2013-13817	Oracle 多个产品多个子件远程 存在未明信息泄露漏洞	中	是
电信	CNVD-2013-13824	Oracle MySQL Server Optimizer 存在未明远程拒绝服务漏洞 (CNVD-2013-13824)	中	是
电信	CNVD-2013-13833	Oracle MySQL Server Optimizer 存在未明远程拒绝服务漏洞	中	是
电信	CNVD-2013-13836	Oracle MySQL Server Locking 存 在未明远程拒绝服务漏洞	低	是
电信	CNVD-2013-13847	Oracle MySQL Server InnoDB 存 在未明远程拒绝服务漏洞	中	是
电信	CNVD-2013-13933	Oracle MySQL Server Replication 存在未明远程漏洞	中	是
工控系统	CNVD-2013-13985	Nano-10 PLC 远程拒绝服务漏 洞	高	否
移动互联 网	CNVD-2013-14060	Apple iOS 7 for iPhone 锁屏本 地安全绕过漏洞	低	是
移动互联	CNVD-2013-14061	Apple iOS 7 for iPhone 不正确	低	是

网		密码尝试时间延迟绕过漏洞		
移动互联网	CNVD-2013-14062	Apple iOS 7 for iPhone 任意号码呼叫漏洞	中	是
移动互联网	CNVD-2013-14024	多个 I-O DATA 产品存在未明会话劫持漏洞	中	是
移动互联网	CNVD-2013-13878	Bluetooth U 'New Folder - Index' 模块存在多个目录遍历漏洞	中	否

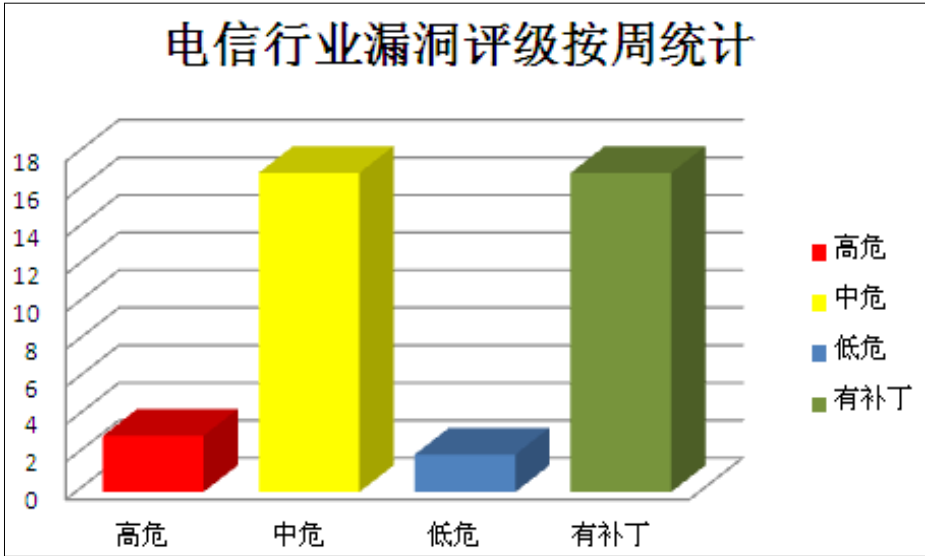


图 1 电信行业漏洞统计

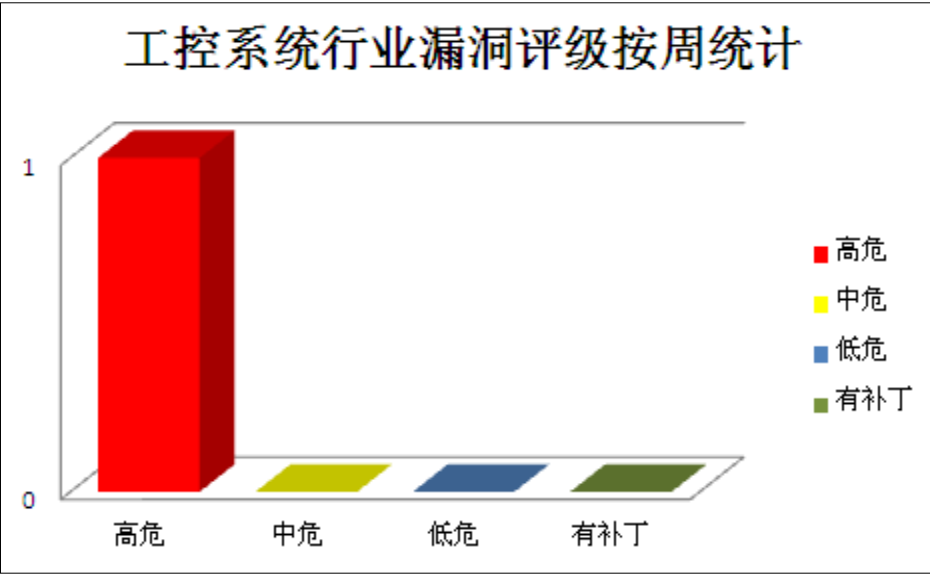


图 2 工控系统行业漏洞统计

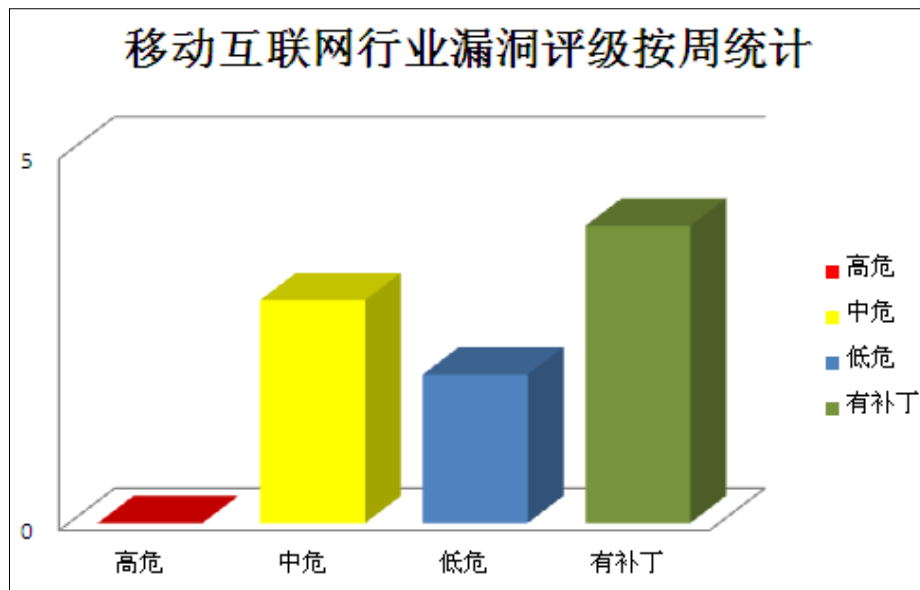


图 3 移动互联网行业漏洞统计

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、Oracle 产品安全漏洞

Oracle 发布了 2013 年 10 月的安全更新，修复了其多款产品存在的 127 个安全漏洞。利用上述漏洞，攻击者发起恶意攻击。

CNVD 收录的相关漏洞包括：Oracle Java JDK / JRE / JavaFX JavaFX 子件存在未明漏洞、Oracle Java SE 远程漏洞（CNVD-2013-13842）、Oracle Java JDK / JRE Deployment 子件存在未明任意代码执行漏洞（CNVD-2013-13848）、Oracle Java JDK / JRE / JRockit JAXP 子件存在未明漏洞、Oracle Java JDK / JRE Swing 子件存在未明任意代码执行漏洞、Oracle Java JDK / JRE Swing 子件任意代码执行漏洞、Oracle Java JDK / JRE / JavaFX JavaFX 子件任意代码执行漏洞、Oracle Identity Analytics / Sun Role Manager Security 子件存在未明漏洞等。上述漏洞的综合评级均为“高危”。厂商已经发布了上述漏洞的修补程序。CNVD 提醒广大 Oracle 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/patchInfo/show/40347>

<http://www.cnvd.org.cn/patchInfo/show/40350>

<http://www.cnvd.org.cn/patchInfo/show/40357>

<http://www.cnvd.org.cn/patchInfo/show/40372>

<http://www.cnvd.org.cn/patchInfo/show/40393>

<http://www.cnvd.org.cn/patchInfo/show/40395>

<http://www.cnvd.org.cn/patchInfo/show/40409>

<http://www.cnvd.org.cn/patchInfo/show/40414>

2、Apple 安全漏洞

Apple Mac OS X 是一款苹果公司开发的操作系统。本周，Apple Mac OS X 被披露存在多个安全漏洞，攻击者利用漏洞可导致应用程序崩溃或执行任意代码。

CNVD 收录的相关漏洞包括：Apple Mac OS X Kernel SHA-2 摘要处理拒绝服务漏洞、Apple Keynote 演示模式锁屏绕过漏洞、Apple Mac OS X 屏幕共享服务器 VNC 用户名格式串漏洞、Apple Mac OS X USB Hub 控制器畸形请求处理本地拒绝服务漏洞、Apple Mac OS X hibernation 自动登录锁屏绕过漏洞、Apple Mac OS X 智能卡服务证书吊销检查漏洞、Apple Mac OS X Kernel 组播报文处理远程拒绝服务漏洞、Apple Mac OS X OpenLDAP ldapsearch minssf 配置加密漏洞等。其中，“Apple Mac OS X Kernel SHA-2 摘要处理拒绝服务漏洞”、“Apple Keynote 演示模式锁屏绕过漏洞”、“Apple Mac OS X 屏幕共享服务器 VNC 用户名格式串漏洞”的综合评级均为“高危”。厂商已经发布了上述漏洞的修补程序。CNVD 提醒 用户及时下载补丁更新，避免引发漏洞相关的安全事件。

参考链接：<http://www.cnvd.org.cn/patchInfo/show/40503>

<http://www.cnvd.org.cn/patchInfo/show/40493>

<http://www.cnvd.org.cn/patchInfo/show/40491>

<http://www.cnvd.org.cn/patchInfo/show/40513>

<http://www.cnvd.org.cn/patchInfo/show/40516>

<http://www.cnvd.org.cn/patchInfo/show/40515>

<http://www.cnvd.org.cn/patchInfo/show/40520>

<http://www.cnvd.org.cn/patchInfo/show/40519>

3、Cisco 产品安全漏洞

Cisco Unified Computing System 是一个集计算、虚拟化和网络于一体的平台；Cisco Identity Services Engine 是一款用于 Cisco TrustSec 解决方案的中央策略引擎。Cisco Adaptive Security Appliance 是一款自适应安全设备，可提供安全和 VPN 服务的模块。本周，上述产品被披露存在多个漏洞，攻击者利用漏洞可获取敏感信息、发起拒绝服务攻击，执行任意代码，获取 root 权限。

CNVD 收录的相关漏洞包括：Cisco Unified Computing System 权限提升漏洞、Cisco Unified Computing System 信息泄露漏洞（CNVD-2013-14067）、多个 Cisco Appliances 拒绝服务漏洞、Cisco Identity Services Engine 远程任意命令执行漏洞、Cisco Secure Access Control System 远程拒绝服务漏洞（CNVD-2013-14072）、Cisco ASA VPN 拒绝服务漏洞、Cisco Unified Computing System 本地拒绝服务漏洞、Cisco Unified Computing System 信息泄露漏洞（CNVD-2013-14019）、其中“Cisco Identity Services Engine 远程任意命令执行漏洞”的综合评级为“高危”。除了“Cisco Unified Computing System 信息泄露漏洞

（CNVD-2013-14067）”外，厂商均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/patchInfo/show/40532>
<http://www.cnvd.org.cn/patchInfo/show/40533>
<http://www.cnvd.org.cn/patchInfo/show/40530>
<http://www.cnvd.org.cn/patchInfo/show/40528>
<http://www.cnvd.org.cn/patchInfo/show/40512>
<http://www.cnvd.org.cn/patchInfo/show/40453>
<http://www.cnvd.org.cn/patchInfo/show/40467>

4、IBM 产品安全漏洞

IBM Tivoli Endpoint Manager 提供了统一、实时的可视化和实施方法来向所有端点部署和管理补丁；IBM Lotus Domino 服务器是一款基于 WEB 合作的应用程序架构；IBM WebSphere DataPower XC10 Appliance 是一款结合强大的 DataPower 硬件平台和 IBM 分布式缓存技术的解决方案。IBM Integration Bus(之前称作 WebSphere Message Broker)是一款企业服务总线产品,为面向服务架构(SOA)环境和非 SOA 环境提供连通性和通用数据转换；IBM Java 是一款 JRE 运行时环境。本周，上述产品被披露存在多个漏洞，攻击者利用漏洞可获取敏感信息、发起拒绝服务攻击，执行任意代码。

CNVD 收录的相关漏洞包括：IBM Tivoli Endpoint Manager LDAP/AD 验证控制台用户伪造漏洞、IBM iNotes HTML 注入漏洞（CNVD-2013-14079）、IBM iNotes HTML 注入漏洞、IBM WebSphere DataPower XC10 Appliance 存在未明漏洞（CNVD-2013-13967）、IBM WebSphere DataPower XC10 Appliance 未授权访问漏洞（CNVD-2013-13966）、IBM Integration Bus XML4J 解析器实体扩展拒绝服务漏洞、IBM Java 存在多个未明安全绕过漏洞、IBM WebSphere eXtreme Scale 监测控制台跨站脚本漏洞等。除了“IBM Java 存在多个未明安全绕过漏洞”外，厂商均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/patchInfo/show/40482>
<http://www.cnvd.org.cn/patchInfo/show/40509>
<http://www.cnvd.org.cn/patchInfo/show/40499>
<http://www.cnvd.org.cn/patchInfo/show/40447>
<http://www.cnvd.org.cn/patchInfo/show/40448>
<http://www.cnvd.org.cn/patchInfo/show/40478>
<http://www.cnvd.org.cn/patchInfo/show/40304>

5、Tenda 无线路由器远程命令执行后门漏洞

Tenda 是深圳的一家网络设备提供商。本周，该厂商生产的无线路由器被披露存在一个综合评级为“高危”的远程命令执行后门漏洞。Tenda 的 W330R、W302R 无线路

由器固件最新版本及 Medialink MWN-WAPR150N 中存在后门。该漏洞通过一个 UDP 数据包即可利用，如果设备收到以字符串 “w302r_mfg” 为开头的数据包，即可触发此漏洞执行各类命令，甚至以 root 权限执行任何命令。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/flaw/show/CNVD-2013-13948>

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-2013-14078	SAP NetWeaver Web Dynpro Live Update XML 外部实体信息泄露漏洞	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://scn.sap.com/community/netweaver
CNVD-2013-14076	SAP Sybase Adaptive Server Enterprise 存在未明远程代码执行漏洞	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://www.sap.com/
CNVD-2013-14074	Joomla! Maian15 组件'name'参数任意 shell 上传漏洞	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://www.joomla.org/
CNVD-2013-14073	Cisco Identity Services Engine 远程任意命令执行漏洞	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://www.cisco.com/
CNVD-2013-14069	FFmpeg/Libav 存在多个拒绝服务漏洞	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://ffmpeg.org/security.html
CNVD-2013-14064	D-Link DIR-605L CAPTCHA Data 栈缓冲区溢出漏洞	高	暂无
CNVD-2013-13985	Nano-10 PLC 远程拒绝服务漏洞	高	暂无
CNVD-2013-13984	ocaine Gem for Ruby 哈希对象处理任意命令执行漏洞	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://rubygems.org/gems/cocaine
CNVD-2013-13581	GestiOL ip_checkhost.cgi 'ip'命令注入漏洞	高	暂无
CNVD-2013-13586	WHMCompleteSolution (WHMCS) /includes/dbfunctions.php SQL 注入漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，Oracle 发布了 2013 年 10 月份的月度例行安全公告，修复了 Oracle 多款产品存在的 127 个安全漏洞。Apple Mac OS X 产品及 IBM 和 Cisco 的多款产品均被披露存在多个漏洞，攻击者利用漏洞可获取敏感信息或发起拒绝服务攻击。此外，本周 D-link、Tenda 等多款无线路由器被披露存在后门漏洞，对企业和个人用户构成较为严重的威胁，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、Linux Kernel 'dm-snapshot'信息泄露漏洞

Linux Kernel 是一款开源的操作系统，Linux Kernel 的 device-mapper 子系统存在信息泄露问题，在某些条件下，解释的数据会写入快照块设备，攻击者可利用该漏洞读取不可访问的释放空间中磁盘块的数据。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/40433>

本周要闻速递

1. 甲骨文：修补安全漏洞远离劫持风险

本周二，甲骨文公司修复了 Java、数据库及其它产品当中存在的 127 项安全问题，同时搞定了某些可能允许攻击者接管系统的严重漏洞。其中发布的最新 Java SE 7 Update 45（7u45）版本当中包含 51 项修复内容，在本次重要补丁更新的全部 127 项内容中占据很大比例。在此次被修正的安全漏洞中，有 50 种能够被以远程方式用于绕过难机制、其中的 12 种更属于最高严重等级——这意味着它们的存在很可能导致底层操作系统被完全控制。在此次 Java 安全更新中被修复的 51 项漏洞当中，有 40 项只影响客户端部署，其中包括经常成为攻击目标的 Java 网络浏览器插件以及 8 项既影响客户端又影响服务器部署的漏洞。最后一项漏洞影响到的是 jhat，一款能够被用于执行 Java 堆分析的开发工具。在本次重要补丁更新中，其它 76 项与 Java 漏洞无关的安全修复涵盖了甲骨文旗下的众多产品线，其中包括：甲骨文数据库、甲骨文 Fusion 中间件、甲骨文企业管理器网格控制、甲骨文电子商务套件、甲骨文供应链产品套件、甲骨文 PeopleSoft 企业版、甲骨文 Siebel CRM、甲骨文 iLearning、甲骨文行业应用程序、甲骨文 FLEXCUBE、甲骨文 Primavera、甲骨文与 Sun Systems 产品套件、甲骨文 Linux、虚拟化以及甲骨文 MySQL。

参考链接：<http://article.pchome.net/content-1664475.html>

2. 思科修复网络和通信产品中的严重安全漏洞

思科公司近日发布了软件安全更新来解决几款关键产品中的 DDoS 和任意命令执行漏洞，包括 Apache Struts 开发框架中的一个已知漏洞。此外，还发布了思科身份服务引擎(ISE)的安全更新，该引擎是针对有线、无线和 VPN 连接的安全政策管理平台。该公司表示，在思科 ISE 和 Cisco Unified SIP Proxy 上执行攻击并不需要任何身份验证，但对 Cisco Business Edition 3000 执行攻击则需要攻击者提供有效的登录凭证或者诱使具有登录凭证的用户执行恶意 URL。利用 Struts 漏洞的地下攻击工具的存在提高了使用受感染思科产品的企业的风险。

参考链接：http://www.cnw.com.cn/news-international/htm2013/20131025_285016.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是国家计算机网络应急技术处理协调中心的简称（英文简称为 CNCERT 或 CNCERT/CC），成立于 1999 年 9 月，是一个非政府非盈利的网络安全技术协调组织，主要任务是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展中国互联网上网络安全事件的预防、发现、预警和协调处置等工作，以维护中国公共互联网环境的安全、保障基础信息网络和网上重要信息系统的安全运行。目前，CNCERT 在我国大陆 31 个省、自治区、直辖市设有分中心。

同时，CNCERT 积极开展国际合作，是中国处理网络安全事件的对外窗口。CNCERT 是国际著名网络安全合作组织 FIRST 正式成员，也是 APCERT 的发起人之一，致力于构建跨境网络安全事件的快速响应和协调处置机制。截止 2012 年，CNCERT 与 51 个国家和地区的 91 个组织建立了“CNCERT 国际合作伙伴”关系。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82990999