

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 191 个，其中高危漏洞 72 个、中危漏洞 99 个、低危漏洞 20 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 123 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“多个 D-LINK 产品产品命令注入漏洞”、“AudioCoder '.m3u' 文件缓冲区溢出漏洞”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 家成员单位和多个合作伙伴及个人报送了本周收录的全部 191 个漏洞。各单位报送情况如表 1 所示。其中，启明星辰、安天实验室等单位报送数量较多。此外，奇虎 360 公司、知道创宇公司以及个人报送者向 CNVD 提交了 27 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	124	0
绿盟科技	41	0
安天实验室	112	0
天融信	56	0
恒安嘉新	57	0
奇虎 360	13	13
东软	3	0
知道创宇	2	2
个人	12	12

报送总计	420	27
录入总计	191（去重）	27

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Cisco、IBM、WordPress、D-Link 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	Cisco	24	13%
2	IBM	18	9%
3	WordPress	12	6%
4	D-Link	9	5%
5	EMC	6	3%
6	Microsoft	4	2%
7	Linux	4	2%
8	TYPO3	3	2%
9	NetApp	3	2%
10	HP	2	1%
11	其它	106	55%

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 191 个漏洞。其中应用程序漏洞 116 个，WEB 应用漏洞 40 个，操作系统漏洞 5 个，数据库漏洞 1 个，网络设备漏洞 28 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	116
WEB 应用漏洞	40
网络设备漏洞	28
操作系统漏洞	5
安全产品漏洞	1
数据库漏洞	1

表 3 漏洞按影响类型统计表

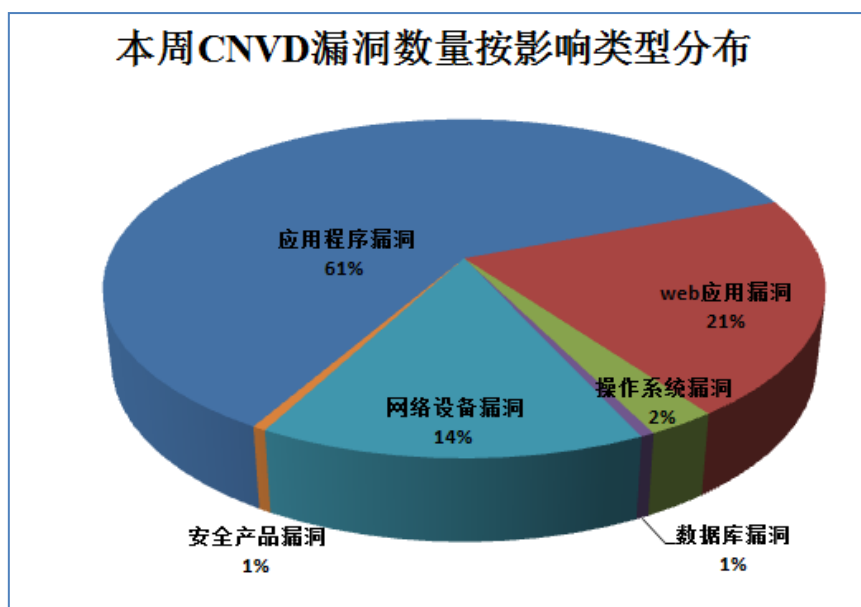


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 28 个网络设备漏洞：思科产品漏洞 13 个，D-LINK 产品漏洞 9 个，Huawei 产品漏洞 2 个，Vivotek 产品漏洞 4 个。

其中，“D-Link DNS-323 ShareCenter 远程命令执行漏洞、Huawei AR Series Routers SNMPv3 拒绝服务漏洞、Huawei AR 系列路由器 SNMPv3 远程栈缓冲区溢出漏洞、多个 Cisco 产品 root 权限命令执行漏洞、多个 D-LINK 产品产品内置账户安全绕过漏洞、多个 D-LINK 产品命令注入漏洞、多个 Vivotek IP Camera 产品命令注入漏洞、多个 Vivotek IP Camera 产品远程缓冲区溢出漏洞”的综合评级均为“高危”。

目前，互联网上已经出现了针对“Cisco Linksys E4200 Router 跨站脚本漏洞、Cisco Linksys E4200 Router 跨站脚本漏洞 (CNVD-2013-24102)、Cisco Linksys E4200 路由器本地文件包含漏洞、D-Link DSL-320B 存在多个漏洞、D-Link DSL-320B 存在多个验证绕过漏洞、多个 D-LINK 产品信息泄露漏洞(CNVD-2013-23650)、多个 Vivotek IP Camera 产品远程缓冲区溢出漏洞、多个 Vivotek IP Camera 产品远程验证绕过漏洞”的攻击代码，相关厂商已经发布了漏洞修补程序。

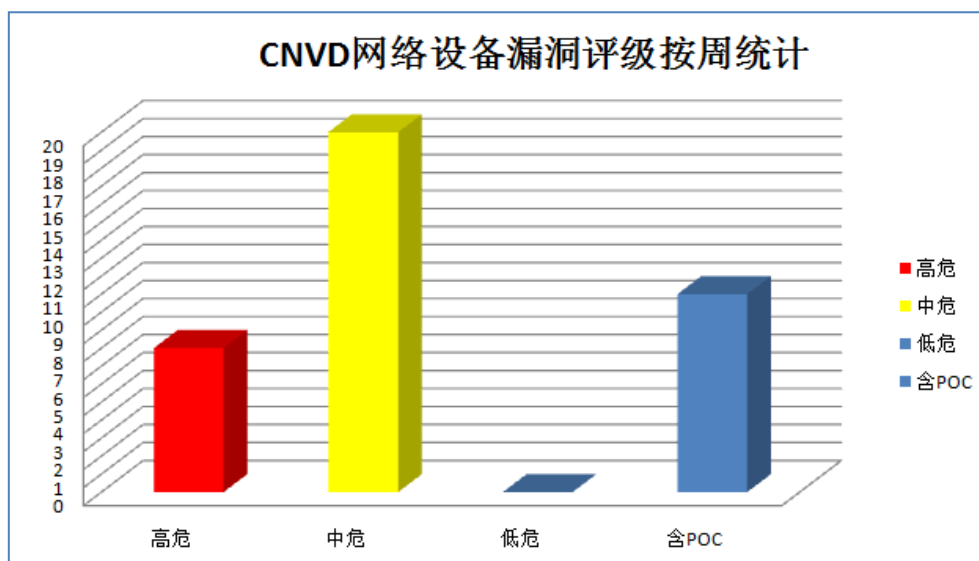


图 2 网络设备漏洞统计

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 Security Essential 是一款反恶意程序的软件；Microsoft Internet Explorer 是一款 WEB 浏览器。本周，上述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，诱使用户访问恶意网页执行挂马攻击，控制用户系统。

CNVD 收录的相关漏洞包括：Microsoft Security Essentials 本地权限提升漏洞、Microsoft IE 8 CGenericElement 对象内存释放重用、Microsoft Internet Explorer 内存错误引用漏洞（CNVD-2013-23860）、Microsoft Internet Explorer 'MSXML'错误文件枚举漏洞。其中，除“Microsoft Internet Explorer 'MSXML'错误文件枚举漏洞”之外，其余漏洞的综合评级均为“高危”。厂商已发布“Microsoft Security Essentials 本地权限提升漏洞、Microsoft Internet Explorer 内存错误引用漏洞（CNVD-2013-23860）”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-2013-24059>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23894>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23860>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-24057>

2、D-LINK 产品安全漏洞

D-Link DNS-323 是一款 NAS 网络存储设备；D-Link DSL-320B 是一款 ADSL 路由器设备。本周，上述 D-Link 产品被披露存在安全漏洞，攻击者利用漏洞可获得敏感信息，注入任意 OS 命令并以 WEB 权限执行。

CNVD 收录的相关漏洞包括：D-Link DNS-323 ShareCenter 远程命令执行漏洞、

D-Link DSL-320B 存在多个漏洞、D-Link DSL-320B 存在多个验证绕过漏洞、D-Link DNS-323 ShareCenter 远程目录遍历漏洞。其中，“D-Link DNS-323 ShareCenter 远程命令执行漏洞”的综合评级均为“高危”。厂商已发布“D-Link DSL-320B 存在多个验证绕过漏洞”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-2013-23856>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-24062>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-24061>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23855>

3、Huawei 产品安全漏洞

Huawei AR 系列路由器是基于华为 VRP 的下一代企业级路由器，集成了路由、交换、3G、WLAN、语音和安全功能。本周，Huawei AR 系列路由器被披露存在多个安全漏洞。远程攻击者利用漏洞提交特制 SNMPv3 消息，远程执行任意代码，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Huawei AR 系列路由器 SNMPv3 远程栈缓冲区溢出漏洞、Huawei AR Series Routers SNMPv3 拒绝服务漏洞。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-2013-23931>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23849>

4、IBM 产品安全漏洞

IBM Lotus Notes 是一款桌面客户端；IBM WebSphere DataPower XC10 Appliance 是结合 DataPower 硬件平台和 IBM 分布式缓存技术的解决方案；IBM Java SDK 是一款 Java SE 平台；IBM Sterling Order Management 支持用户与供应商协作并优化复杂的订单执行流程；IBM solidDB 是一款内存型数据库系统；Tivoli Federated Identity Manager 用于解决跨企业的联邦身份管理；IBM Sametime 是一套整合的企业级即时通讯软件。本周，上述 IBM 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，执行任意命令。

CNVD 收录的相关漏洞包括：IBM Lotus Notes 整数溢出漏洞、IBM WebSphere DataPower XC10 Appliance 存在未明漏洞、IBM Java 'Reflection API'存在多个安全绕过漏洞、IBM Sterling Order Management 信息泄露漏洞、IBM solidDB 存储过程调用拒绝服务漏洞、IBM Tivoli Federated Identity Manager 跨站脚本漏洞、IBM Sametime Classic Meeting Server 存在未明跨站脚本漏洞。其中，“IBM Lotus Notes 整数溢出漏洞”的综合评级为“高危”。厂商已发布了除“IBM Java 'Reflection API'存在多个安全绕过漏洞”之外，其余漏洞的修补程序。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-2013-24028>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-24048>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23964>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23853>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23851>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23836>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23834>

5、AudioCoder '.m3u' 文件缓冲区溢出漏洞

AudioCoder 是一款 MediaCoder 核心开发高性能音频转换工具。本周, 该产品被披露存在一个综合评级为“高危”的缓冲区溢出漏洞。由于 AudioCoder 处理播放列表时存在一个边界错误, 远程攻击者利用漏洞可构建特制的.m3u 文件, 诱使用户解析, 执行任意代码。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-2013-23843>

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-2013-24133	AlienVault OSSIM SQL 注入漏洞	高	暂无
CNVD-2013-24129	Cisco Unified Customer Voice Portal 远程拒绝服务漏洞	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://tools.cisco.com/security/center/viewAlert.x?alertId=28982
CNVD-2013-24132	Drupal Htmllarea 模块存在多个任意文件上传漏洞	高	暂无
CNVD-2013-24114	Invensys Wonderware Information Server 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: https://wdn.wonderware.com/sites/WDN/Pages/Downloads/Software.aspx
CNVD-2013-24131	Fujitsu Desktop Update 权限提升漏洞	高	暂无
CNVD-2013-24107	NetApp OnCommand System Manager OS 命令执行漏洞	高	NetApp OnCommand System Manager 2.2 已经修复此漏洞, 建议用户下载使用: http://www.netapp.com

CNVD-2013-24120	Joomla! DJ-Classifieds 组件 'se_regs[]' SQL 注入漏洞	高	暂无
CNVD-2013-24103	Craigslist Clone Gold 'catid'参数 SQL 注入漏洞	高	暂无
CNVD-2013-24046	Red Hat OpenShift Origin 远程命令执行漏洞	高	用户可参考如下厂商提供的安全公告获得补丁信息： https://bugzilla.redhat.com/show_bug.cgi?id=960363
CNVD-2013-24038	SAP ERP Central 组件 'CJDB_FILL_MEMORY_FROM_PP BQ'函数远程代码注入漏洞	高	用户可联系供应商获得补丁信息： https://service.sap.com/sap/support/notes

表 3 部分高危漏洞列表

小结：本周，Cisco 多款产品被披露存在多个拒绝服务漏洞，主要影响涉及基础电信企业和相关企业用户，而华为 AR 系列路由器被披露存在的多个拒绝服务或远程代码执行漏洞，也对企业级用户构成较大威胁。D-LINK 多款网络摄像头产品被披露存在多个权限绕过漏洞，个人用户需注意防范。此外，本周微软 IE 8 浏览器软件被披露存在高危漏洞，建议相关用户升级 IE 版本或下载微软公司提供的临时修复方案。

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、Apache 发布升级程序，修补 VCL 产品安全漏洞

Apache VCL 是一款自服务的系统，为最终用户提供专用计算环境的远程访问环境。本周，Apache 发布升级程序，修补了 VCL 存在的多个输入验证漏洞。攻击者可以利用漏洞进行跨站脚本或拒绝服务攻击。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/patchInfo/show/33829>

本周要闻速递

1. IE8 0day 漏洞临时修复工具已开放下载

微软公司在上周五证实 IE8 中存在一个 0day 漏洞，可导致远程代码执行。XP、Vista 和 Win7 中的 IE8 用户都有可能遭到攻击，微软建议 Vista 和 Win7 的用户将浏览器升级到 IE9 或 IE10 再使用。微软在昨天放出了一个 IE8 0day 漏洞的临时修复工具，这个工具名为“CVE-2013-1347 MSHTML Shim Workaround”，用户可以在微软网站下载到。

参考链接：<http://tech.sina.com.cn/s/2013-05-10/07428325498.shtml>

2. Adobe 发布公告称 ColdFusion 存在严重漏洞

Adobe 在本周三晚上发布了一个安全公告(APSA13-03)，在 Adobe ColdFusion 中存在一个严重漏洞，成功利用该漏洞可能允许攻击者远程访问存储在服务器上的文件。该漏洞影响版本为 Windows 10, 9.0.2, 9.0.1 和 9.0 版本，Macintosh 和 UNIX 版本的 ColdFusion。

参考链接：<http://it.msn.com.cn/127435/563588571194b.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