

信息安全漏洞周报

2013 年 11 月 4 日-2013 年 11 月 10 日

2013 年第 45 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 136 个，其中高危漏洞 51 个、中危漏洞 74 个、低危漏洞 11 个。上述漏洞中，可利用来实施远程攻击的漏洞有 120 个。本周收录的漏洞中，已有 96 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“WordPress This Way Theme 'upload_settings_image.php'任意文件上传漏洞”、“多个 Microsoft 产品图形组件远程代码执行漏洞”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 7 家成员单位和及个人报送了本周收录的全部 136 个漏洞。报送情况如表 1 所示。其中，天融信、安天实验室、启明星辰、绿盟科技等单位报送数量较多。此外，知道创宇和个人报送者向 CNVD 提交了 11 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
天融信	165	0
安天实验室	138	0
启明星辰	98	0
绿盟科技	42	0
恒安嘉新	20	0
知道创宇	3	1
东软	1	0

个人	10	10
报送总计	477	11
录入总计	136（去重）	11

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Mozilla、Cisco、Linux、HP 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	Cisco	10	7%
2	Linux	10	7%
3	Mozilla	8	6%
4	HP	6	4%
5	Wireshark	5	4%
6	WordPress	4	3%
7	SaltStack	3	3%
8	Tiki Software Community Association	3	2%
9	Red Hat	2	1%
10	其它	85	63%

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 136 个漏洞。其中应用程序漏洞 78 个，WEB 应用漏洞 33 个，操作系统漏洞 14 个，网络设备漏洞 9 个，安全产品漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	78
WEB 应用漏洞	33
操作系统漏洞	14
网络设备漏洞	9
安全产品漏洞	2

表 3 漏洞按影响类型统计表

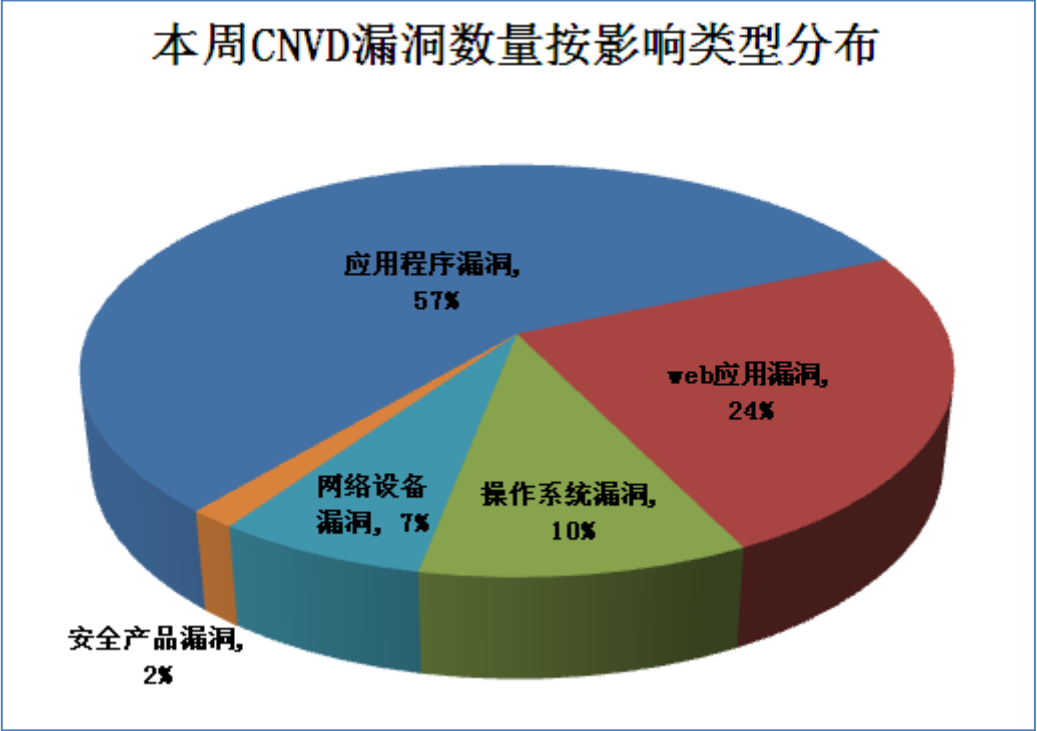


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 10 个电信行业漏洞（如下列表所示）。其中，“Cisco IOS XE Software 拒绝服务漏洞（CNVD-2013-14208）、Cisco IOS XE TCP 段重组拒绝服务漏洞、Cisco IOS XE TCP 分部重组存在多个拒绝服务漏洞、Cisco IOS XE Software 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。本周，CNVD 未收录移动互联网行业和工控系统行业漏洞。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2013-14324	MikroTik RouterOS 默认管理账户漏洞	中	否
电信	CNVD-2013-14283	ISC BIND Winsock API 存在漏洞	中	是
电信	CNVD-2013-14289	Cisco Prime Central for Hosted Collaboration Solution 拒绝服务漏洞	中	否
电信	CNVD-2013-14258	UNICORN WB-3300NR 路由器存在多个跨站请求伪造漏洞	低	否
电信	CNVD-2013-14254	Netgear WNDR3700 安全限制绕过漏洞	中	否
电信	CNVD-2013-14208	Cisco IOS XE Software 拒绝服	高	是

		务漏洞（CNVD-2013-14208）		
电信	CNVD-2013-14209	Cisco IOS Internet Key Exchange 重放安全绕过漏洞	中	是
电信	CNVD-2013-14210	Cisco IOS XE TCP 段重组拒绝服务漏洞	高	是
电信	CNVD-2013-14211	Cisco IOS XE TCP 分部重组存在多个拒绝服务漏洞	高	是
电信	CNVD-2013-14212	Cisco IOS XE Software 拒绝服务漏洞	高	是

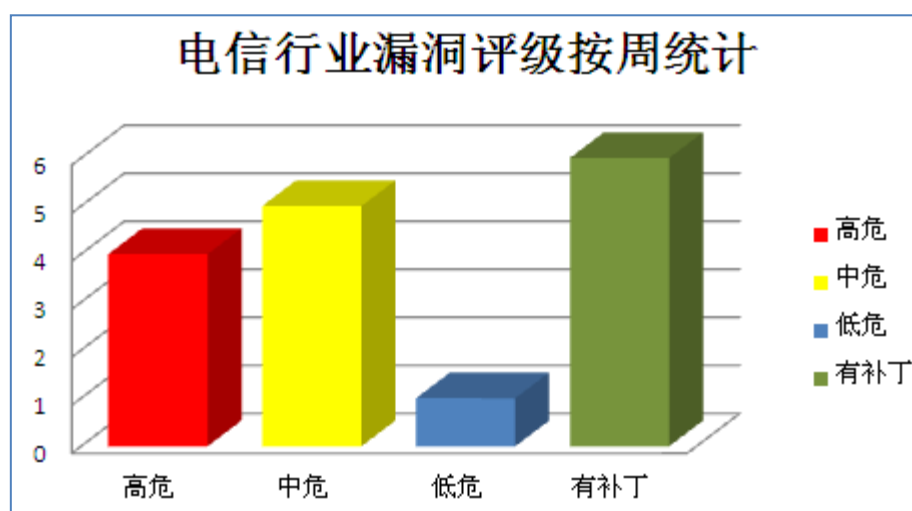


图 1 电信行业漏洞统计

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、Mozilla 产品安全漏洞

Mozilla Firefox/SeaMonkey/Thunderbird 是 Mozilla 所发布的 WEB 浏览器/新闻组客户端/邮件客户端。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞使应用程序崩溃或执行任意代码。

CNVD 收录的相关漏洞包括：Mozilla Firefox 存在未明内存破坏漏洞（CNVD-2013-14213、CNVD-2013-14220）、Mozilla 多个产品 nsContentUtils::ContentIsHostIncludingDescendantOf()函数 HTML 文档模版处理内存错误引用漏洞、Mozilla 多个产品 select 元素处理 URL 栏伪造漏洞、Mozilla 多个产品 nsEventListenerManager::SetEventHandler()内存错误引用漏洞、Mozilla 多个产品 Worker::SetEventListener()函数内存破坏漏洞、Mozilla 多个产品 nsIPresShell::GetPresContext()函数对象处理内存错误引用漏洞、Mozilla 多个产品 nsIOService::NewChannelFromURIWithProxyFlags()函数 BLOB URL 处理内存

错误引用漏洞。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-2013-14213>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14220>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14215>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14214>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14217>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14216>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14219>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14218>

2、HP 产品安全漏洞

HP SiteScope 是一种为确保分布式 IT 基础部件的可用性和性能的可代理的监视解决方案；HP LoadRunner 是一款惠普公司开发的性能测试工具；HP Application Lifecycle Management 是一款惠普公司发行的应用生命周期管理解决方案。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可以应用上下文执行任意代码。

CNVD 收录的相关漏洞包括：HP SiteScope 'issueSiebelCmd' SOAP 请求远程代码执行漏洞、HP LoadRunner Virtual User Generator 存在未明远程代码执行漏洞（CNVD-2013-14225、CNVD-2013-14226、CNVD-2013-14227）、HP Application LifeCycle Management 存在未明远程代码执行漏洞、HP Application Lifecycle Management Synchronizer 远程代码执行漏洞。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/flaw/show/CNVD-2013-14255>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14225>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14226>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14227>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14228>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14233>

3、Cisco 产品安全漏洞

Cisco Prime 是一款以服务为中心从终端、网络设备和应用整合管理有线与无线 LAN、WAN 与数据中心，并筛选信息的解决方案；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；Cisco AnyConnect Secure Mobility 是一个安全的企业移动解决方案；Cisco IOS 是多数思科系统路由器和网络交换机上使用的互联网络操作系统。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞进行未授权操作，使设备重启，导致拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco Prime Central for HCS Impact server Java process 远程拒绝服务漏洞、Cisco ASA CX 安全搜索策略绕过漏洞、Cisco AnyConnect Secure Mobility Client VPNAPI COM 模块存在未明溢出漏洞、Cisco IOS XE Software 拒绝服务漏洞（CNVD-2013-14208）、Cisco IOS Internet Key Exchange 重放安全绕过漏洞、Cisco IOS XE TCP 段重组拒绝服务漏洞、Cisco IOS XE TCP 分部重组存在多个拒绝服务漏洞、Cisco IOS XE Software 拒绝服务漏洞。其中，“Cisco IOS XE Software 拒绝服务漏洞（CNVD-2013-14208）”、“Cisco IOS XE TCP 段重组拒绝服务漏洞”、“Cisco IOS XE TCP 分部重组存在多个拒绝服务漏洞”、“Cisco IOS XE Software 拒绝服务漏洞”的综合评级为“高危”。厂商已经发布了上述漏洞的修补程序。CNVD 提醒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-2013-14230>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14231>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14232>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14208>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14209>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14210>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14211>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14212>

4、Linux 产品安全漏洞

Linux Kernel 是 Linux 操作系统的内核。本周，该产品被披露存在多个漏洞，攻击者利用漏洞可提升特权，使应用程序崩溃，执行任意代码。

CNVD 收录的相关漏洞包括：Linux Kernel 'oz_cdev_write()'函数本地缓冲区溢出漏洞、Linux Kernel 'mp_get_count()'本地信息泄露漏洞、Linux Kernel 'exitcode_proc_write()'函数本地缓冲区溢出漏洞、Linux Kernel 'drivers/staging/wlags49_h2/wl_priv.c'本地缓冲区溢出漏洞、Linux Kernel AACRAID 驱动 Compat IOCTL 安全绕过漏洞、Linux Kernel 'write_tag_3_packet()'函数本地堆缓冲区溢出漏洞、Linux Kernel skb_flow_dissect()函数特制 IP 报文 IHL 处理远程拒绝服务漏洞、Linux Kernel 'ipc_rcu_putref()'函数本地拒绝服务漏洞。除“Linux Kernel 'write_tag_3_packet()'函数本地堆缓冲区溢出漏洞”外，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-2013-14287>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14290>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14291>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14296>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14301>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14237>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14206>

5、OpenMediaVault /rpc.php 任意 cron 创建权限提升漏洞

OpenMediaVault 是一个开源的基于 Debian Linux 的下一代网络附加存储(NAS)解决方案。本周，OpenMediaVault 被披露存在一个综合评级为“高危”的任意 cron 创建权限提升漏洞。由于 OpenMediaVault/rpc.php 脚本不正确过滤用户提交的输入，远程攻击者利用漏洞提交特制的请求创建任意 cron 作业，提升权限。此外存在默认管理员账户，密码为'openmediavault'。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-2013-14241>

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-2013-14331	Juniper Junos J-Web 任意命令执行漏洞	高	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.juniper.net/us/en/
CNVD-2013-14334	SaltStack Salt 中间人攻击漏洞	高	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.saltstack.com/
CNVD-2013-14332	SaltStack Salt 存在多个远程代码执行漏洞	高	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.saltstack.com/
CNVD-2013-14300	SAP 产品 CRM Internet Sales / CRM Internet Service Web 应用存在未明 SQL 注入漏洞	高	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://service.sap.com/sap/support/notes/1592742
CNVD-2013-14304	McAfee Email Gateway 存在未明任意命令执行漏洞	高	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.mcafee.com/
CNVD-2013-14328	Attachmate Verastream Host Integrator 任意文件上传漏洞	高	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://support.attachmate.com/
CNVD-2013-14238	vTiger CRM '/browse.php'图像上传特制文件 PHP 代码执行漏洞	高	暂无
CNVD-2013-14330	PHPDISK 存在未明 SQL 注入漏洞	高	暂无

CNVD-2013-14205	Zabbix 任意命令执行漏洞	高	暂无
CNVD-2013-14288	GitLab 'SSH key upload'功能远程执行代码漏洞	高	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://gitlab.org/

表 3 部分高危漏洞列表

小结: 本周, Mozilla、Cisco、HP、Linux 的多款产品被披露存在多个漏洞, 攻击者利用漏洞可获得敏感信息, 导致拒绝服务攻击或执行任意代码。此外, OpenMediaVault 被披露存在一个高危零日漏洞, 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、FFmpeg 修补两个漏洞

FFmpeg 是一款用于录制、转换和流化音频和视频的完整解决方案。FFmpeg 修补了两个拒绝服务的漏洞, 避免攻击者利用此漏洞构建恶意文件, 诱使用户解析, 造成应用程序崩溃。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/40664>

<http://www.cnvd.org.cn/patchInfo/show/40692>

本周要闻速递

1. MS Office 曝出重大安全漏洞微软紧急修复

据国外媒体报道,《路透社》表示日前有黑客利用 Office 一项重大漏洞, 通过携带病毒的 Word 文档攻击消费者的电脑, 为此, 微软今天紧急发布了一个软件级补丁 “Fix It”, 作为临时补救措施。微软公司表示本次遭受攻击的用户主要集中在中东和南亚地区, 但是受影响的用户数量非常有限, 但是该公司并没有明确表示究竟有多少用户遭受到了攻击。微软表示, 本次遭受攻击的目前主要是装有 Office 2003、Office 2007 以及在 Windows XP 及 Server 2003 下运行 Office 2010 的计算机。此外, 本次攻击利用了一个之前未被发现的漏洞, 并且属于 “0day” 范畴, 而这也说明了本次出现的漏洞可能造成的危害并不小。Cylance 网络安全公司首席执行官 Stuart McClure 表示, 那些正在使用存在漏洞的 Office 企业应该尽早安装修复工具防止遭受到攻击。

参考链接: <http://cd.qq.com/a/20131107/008413.htm>

2. IE 曝 0day 漏洞影响 XP 及 Win7 系统

据科技博客 ZDNET 报道, 在 Windows XP 和 Windows 7 系统上的英文版本 IE 浏览器上, 发现了一处零日攻击漏洞。黑客利用该漏洞进行攻击, 主要针对目标为 Windows XP 系统上英文版 IE7、IE8 浏览器和 Windows 7 系统上的英文版 IE8 浏览器。该漏洞针对的是微软 IE 7、8、9 和 IE10 浏览器的易攻击性, 但是并没有指明 Windows 8 上的 IE10 或者任何系统上的 IE11 是否存在这一漏洞。据有关报道这一零日安全漏洞可带来两种形式的攻击: 一是隐私信息披露, 二是纵容黑客执行远程代码。该漏洞出现在 Windows XP 系统上并不令人意外, 但对于其能够在 Windows 7 系统上出现则似乎更不寻常。报道还称, 尽管目前微软尚未公布有关该漏洞的安全修复补丁, 但用户可以通过使用微软增强减灾体验工具 (EMET) 来暂时应对风险。但是用户要小心, 因为这样可能将多个版本的 DLL 复制到你的系统上。

参考链接: <http://news.mydrivers.com/1/282/282187.htm>

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