

信息安全漏洞周报

2013 年 09 月 02 日-2013 年 09 月 08 日

2013 年第 36 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 158 个，其中高危漏洞 57 个、中危漏洞 92 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 139 个。本周收录的漏洞中，已有 99 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“dBlog CMS 'm'参数 SQL 注入漏洞”、“TP-LINK TD-W8951ND Router 存在多个输入验证漏洞”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 158 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、天融信等单位报送数量较多。此外，个人报送者向 CNVD 提交了 4 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	125	0
安天实验室	80	0
天融信	67	0
恒安嘉新	41	0
绿盟科技	41	0
东软	1	0
工业和信息化部电子 工业标准化研究院	5	0
个人	4	4
报送总计	364	4

录入总计	158（去重）	4
------	---------	---

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Palo Alto Networks、Cisco、Linux 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	Palo Alto Networks	19	12%
2	Cisco	18	11%
3	Linux	13	8%
4	Citrix Systems, Inc.	8	5%
5	Trivantis	7	4%
6	WordPress	7	4%
7	Dragon Design Services Network Pty. Ltd.	6	4%
8	Super Micro Computer	3	2%
9	IBM	2	1%
10	Adobe	1	1%
11	其它	74	48%

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 158 个漏洞。其中应用程序漏洞 91 个，WEB 应用漏洞 24 个，操作系统漏洞 14 个，数据库漏洞 1 个，网络设备漏洞 9 个，安全产品漏洞 19 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	24
网络设备漏洞	9
操作系统漏洞	14
安全产品漏洞	19
数据库漏洞	1

表 3 漏洞按影响类型统计表

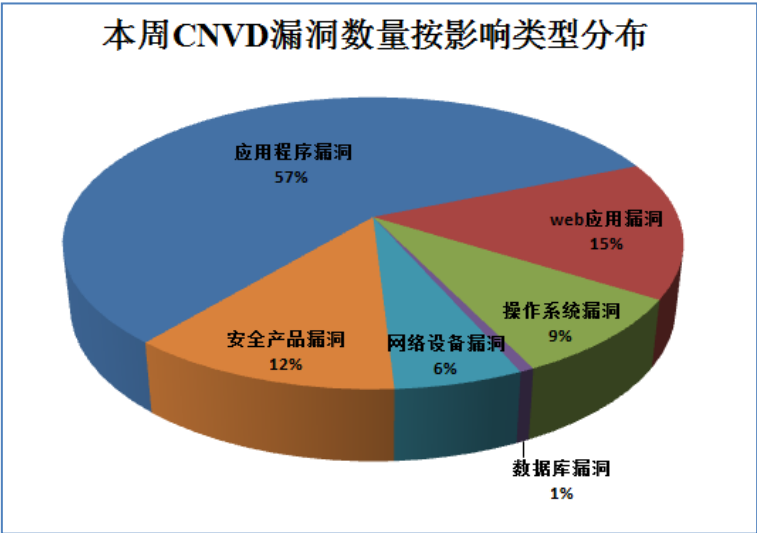


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 16 个电信行业漏洞和 3 个移动互联网行业漏洞（如下列表所示）。其中，“Cisco WebEx WRF Player JPEG DHT 索引内存破坏漏洞、Cisco WebEx WRF Player 栈缓冲区溢出漏洞、Cisco WebEx WRF Player 堆内存破坏漏洞、Cisco WebEx WRF Player 异常处理器内存破坏漏洞、Cisco WebEx WRF Player 内存破坏漏洞、MikroTik RouterOS 'sshd'组件存在多个堆内存破坏漏洞、Android 系统 WebView 控件任意命令执行漏洞、Android 平台 Bitcoin 不充分 RNG 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 未收录工控系统漏洞。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2013-12860	Cisco WebEx WRF Player JPEG DHT 索引内存破坏漏洞	高危	有补丁
电信	CNVD-2013-12861	Cisco WebEx WRF Player 栈缓冲区溢出漏洞	高危	有补丁
电信	CNVD-2013-12831	Cisco WebEx WRF Player 堆内存破坏漏洞	高危	有补丁
电信	CNVD-2013-12830	Cisco WebEx WRF Player 异常处理器内存破坏漏洞	高危	有补丁
电信	CNVD-2013-12832	Cisco WebEx WRF Player 内存破坏漏洞	高危	有补丁
电信	CNVD-2013-12838	Cisco Secure Access Control System 畸形报文拒绝服务漏洞	中危	有补丁
电信	CNVD-2013-12803	多个 Cisco 产品跨站脚本漏洞	中危	无补丁
电信	CNVD-2013-12811	TP-LINK TD-W8951ND Router 存在多个输入验证漏洞	中危	无补丁

电信	CNVD-2013-12816	MikroTik RouterOS 'sshd'组件存在多个堆内存破坏漏洞	高危	无补丁
电信	CNVD-2013-12759	IBM WebSphere Commerce 'search'拒绝服务漏洞	中危	有补丁
电信	CNVD-2013-12787	DISCUZ 存在未明跨站脚本漏洞	中危	无补丁
电信	CNVD-2013-12739	Cisco Wireless LAN Controller 存在多个拒绝服务漏洞	中危	有补丁
电信	CNVD-2013-12741	Cisco IOS 'ESTABLISHED'远程拒绝服务漏洞	中危	有补丁
电信	CNVD-2013-12743	Cisco ISE Captive Portal Application 纯文本凭证信息泄露漏洞	中危	有补丁
电信	CNVD-2013-12746	Cisco Unified Communications Manager 跨站请求伪造漏洞 (CNVD-2013-12746)	中危	无补丁
电信	CNVD-2013-12719	Cisco IOS XR RIP 特制报文拒绝服务漏洞	中危	有补丁
移动互联网	CNVD-2013-12829	Android 系统 WebView 控件任意命令执行漏洞	高危	无补丁
移动互联网	CNVD-2013-12742	Apple iOS6 特殊阿拉伯字符拒绝服务漏洞	中危	无补丁
移动互联网	CNVD-2013-12800	Android 平台 Bitcoin 不充分 RNG 漏洞	高危	有补丁

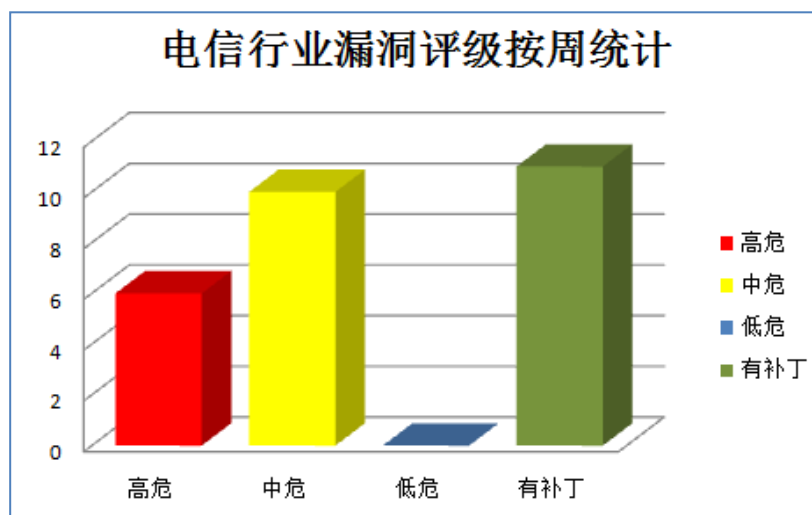


图 2 电信行业漏洞统计

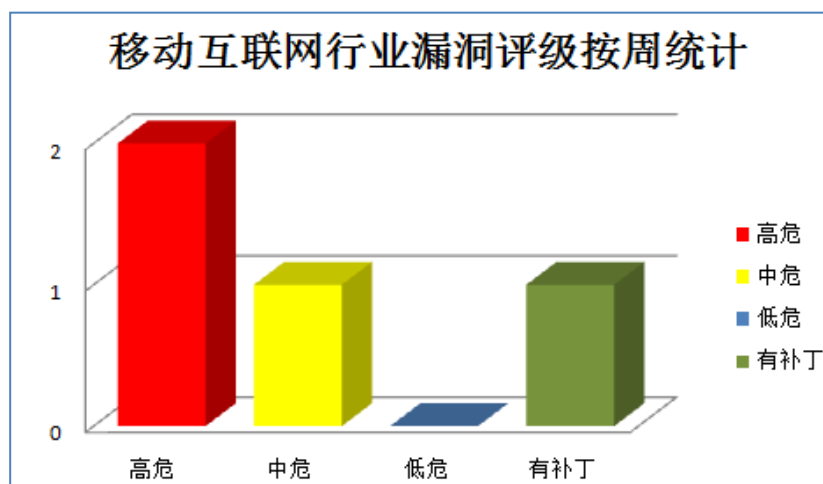


图 3 移动互联网行业漏洞统计

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、Cisco 产品安全漏洞

Cisco WebEx 是一款网络会议解决方案；Cisco Secure Access Control System 是访问策略控制平台；Cisco Global Site Selector 是全球服务器网络负载均衡解决方案。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：Cisco WebEx WRF Player JPEG DHT 索引内存破坏漏洞、Cisco WebEx WRF Player 栈缓冲区溢出漏洞、Cisco WebEx WRF Player 异常处理器内存破坏漏洞、Cisco WebEx WRF Player 堆内存破坏漏洞、Cisco WebEx WRF Player 内存破坏漏洞、Cisco Secure Access Control Server 远程命令执行漏洞、Cisco Secure Access Control System 畸形报文拒绝服务漏洞、Cisco Global Site Selector 跨站请求伪造漏洞等。其中，除“Cisco Secure Access Control System 畸形报文拒绝服务漏洞、Cisco Global Site Selector 跨站请求伪造漏洞”外，其余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-2013-12860>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12861>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12830>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12831>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12832>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12745>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12838>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12833>

2、Linux Kernel 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安全漏洞，攻击者利用漏洞可导致内核崩溃，以内核权限执行任意代码。

CNVD 收录的相关漏洞包括：Linux Kernel 堆缓冲区溢出漏洞(CNVD-2013-12756、CNVD-2013-12755、CNVD-2013-12754、CNVD-2013-12753、CNVD-2013-12751、CNVD-2013-12750、CNVD-2013-12729)、Linux Kernel NULL 指针引用拒绝服务漏洞(CNVD-2013-12728)等。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-2013-12756>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12755>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12754>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12753>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12751>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12750>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12729>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12728>

3、Palo Alto Networks 产品安全漏洞

PAN-OS 是一款控制 Palo Alto Networks 新一代防火墙的作业系统，它提供丰富的防火墙、管理及网路的功能。本周，该产品被披露存在多个安全漏洞。攻击者利用漏洞可以 root 权限执行任意命令。

CNVD 收录的相关漏洞包括：Palo Alto Networks PAN-OS 命令注入漏洞、Palo Alto Networks PAN-OS 设备管理命令行接口任意代码执行漏洞、Palo Alto Networks PAN-OS WEB 管理 UI 验证绕过漏洞、Palo Alto Networks PAN-OS 远程任意 Shell 命令注入漏洞、Palo Alto Networks PAN-OS 任意命令执行漏洞(CNVD-2013-12769、CNVD-2013-12771、CNVD-2013-12770)、Palo Alto Networks PAN-OS 任意 shell 命令执行漏洞等。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-2013-12765>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12766>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12767>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12768>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12769>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12770>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12771>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12772>

4、Citrix 产品安全漏洞

Citrix CloudPortal Services Manager 通过一个 Web 门户来整合并简化托管服务管理，帮助完成应用启动和准备，允许用户以自助方式完成添加、移动和修改操作。本周，该产品被披露存在多个漏洞，攻击者利用漏洞可获得未授权的访问，获取敏感信息。

CNVD 收录的相关漏洞包括：Citrix CloudPortal Services Manager 调试消息存在未明漏洞、Citrix CloudPortal Services Manager WEB 服务存在未明访问漏洞、Citrix CloudPortal Services Manager 存在未明漏洞、Citrix CloudPortal Services Manager 存在未明漏洞(CNVD-2013-12858、CNVD-2013-12856、CNVD-2013-12855、CNVD-2013-12854、CNVD-2013-12853)。其中，“Citrix CloudPortal Services Manager 调试消息存在未明漏洞、Citrix CloudPortal Services Manager WEB 服务存在未明访问漏洞”的综合评级均为“高危”。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-2013-12857>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12852>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12859>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12858>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12856>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12855>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12854>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12853>

5、Android 系统 WebView 控件任意命令执行漏洞

Google Android 是一种以 Linux 为基础的开放源代码操作系统，主要使用于便携设备。本周，该产品被披露存在一个综合评级为“高危”的命令执行漏洞。攻击者利用漏洞可以构建恶意 WEB 页，诱使用户解析，执行任意命令。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-2013-12829>

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-2013-12845	Red Hat JBoss Enterprise Application Platform DiskFileItem 类任意文件上传漏洞	高	用户可参考如下厂商提供的安全公告获得补丁信息： https://rhn.redhat.com/errata/RHSA-

			2013-1193.html https://rhn.redhat.com/errata/RHSA-2013-1194.html
CNVD-2013-12851	dBLog CMS 'm'参数 SQL 注入漏洞	高	暂无
CNVD-2013-12783	Triangle MicroWorks 多个产品基于 IP 特制 TCP 报文处理拒绝服务漏洞	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.trianglemicroworks.com/documents/mdnp_scl_whats_new.pdf
CNVD-2013-12834	AdvancePro Technologies Advanceware 远程安全绕过漏洞	高	暂无
CNVD-2013-12791	LibTIFF tiffcp 'td_samplesperpixel' 函数整数溢出漏洞	高	Libtiff 4.0.0 及以上版本已经修复此漏洞，建议用户下载更新： http://www.remotesensing.org/libtiff
CNVD-2013-12807	AVTECH AVN801 '/cgi-bin/user/Config.cgi'远程缓冲区溢出漏洞	高	暂无
CNVD-2013-12733	Imagemagick 'gif.c'内存破坏漏洞	高	用户可联系供应商获得补丁信息： http://www.imagemagick.org/ http://www.imagemagick.org/script/hangelog.php http://www.imagemagick.org/discourse-server/viewtopic.php?f=3&t=23921
CNVD-2013-12809	GreenBrowser 'over_trigger()' 堆缓冲区溢出漏洞	高	暂无
CNVD-2013-12736	Musicbox 存在多个任意文件上传漏洞	高	暂无
CNVD-2013-12781	Destoon 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，PAN-OS、Cisco 多款产品被披露存在多个漏洞，攻击者利用漏洞可执行任意代码，Linux Kernel 和 Citrix CloudPortal Services Manager 被披露存在多个漏洞，攻击者可利用漏洞获得敏感信息，导致内核崩溃。此外，Android 系统被披露存在一个高危零日漏洞，国内许多浏览器、微博、微信等拥有较大用户群体的知名 APP 软件均受到漏洞的影响。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。

CNVD 整理和发布以下重要安全修补信息。

1、Adobe 发布升级程序，修补 Reader/Acrobat 产品安全漏洞

Adobe Reader/Acrobat 是处理 PDF 文件的应用程序。本周，Adobe 发布升级程序，修补 Reader/Acrobat 产品存在的漏洞。远程攻击者可以利用该漏洞构建恶意 PDF 文件，诱使用户解析，可使应用程序崩溃或以应用程序上下文执行任意代码。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/39289>



本周要闻速递

1. 谷歌 iOS 版验证器被曝存漏洞

美国科技博客的消息称，谷歌最新推出的 iOS 版 Google Authenticator(身份验证器)存在漏洞，可删除用户存储在设备上的所有帐户数据。谷歌 3 日对 iOS 版 Google Authenticator 进行了升级，以支持苹果公司的视网膜显示屏和 iPhone5 的 4 英寸屏幕。Google Authenticator 应用本来是用于确保用户登录安全的，但多位用户反映，此次升级存在一个较大的漏洞，可能删除用户的所有设置和令牌。有用户表示，升级到最新版 Google Authenticator 后，他们的 Dropbox、Google Apps、DreamHost、Twilio、Evernote 和其他令牌全部丢失，必须要重新相互同步。还有用户表示，升级后他们根本无法登录，只能寻求技术支持，以便全部重新设置。目前，该应用已经被谷歌从苹果公司的 App Store 应用商店内下架，以修改问题。

参考链接：http://news.xinhuanet.com/info/2013-09/05/c_132695207.htm

2. 手机挂马漏洞首次大规模爆发

近期，微信等多款安卓流行应用曝出高危挂马漏洞：只要点击好友消息或朋友圈中的一条网址，手机就会自动执行黑客指令，出现被安装恶意扣费软件、向好友发送欺诈短信、通讯录和短信被窃取等严重后果。在乌云漏洞平台上，包括安卓版微信、QQ、腾讯微博、QQ 浏览器、快播等大批应用均被曝光同类型漏洞。此前，谷歌公司在安卓开发者文档中已明确指出，“(WebView 中的该接口)会引发严重的安全问题。请尽量不要使用这个接口，除非你能保证 WebView 中加载的内容都是你自己编写的。”国内多家应用开发者则忽略了这项安全规范，导致此次手机挂马漏洞大规模爆发。

参考链接：<http://finance.chinanews.com/it/2013/09-05/5249211.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