

信息安全漏洞周报

2013 年 06 月 03 日-2013 年 06 月 16 日

2013 年 第23、24 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 250 个，其中高危漏洞 93 个、中危漏洞 134 个、低危漏洞 23 个。上述漏洞中，可利用来实施远程攻击的漏洞有 219 个。本周收录的漏洞中，已有 159 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“QNAP VioStor NVR/QNAP NAS 远程命令执行漏洞”、“gpEasy CMS 任意文件上传漏洞”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 250 个漏洞。各单位报送情况如表 1 所示。其中，启明星辰、天融信、安天实验室、绿盟科技等单位报送数量较多。此外，奇虎 360 和 High-Tech Bridge Security Research Lab 以及个人报送者向 CNVD 提交了 45 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	247	0
绿盟科技	117	0
安天实验室	174	0
天融信	126	0
恒安嘉新	34	0
东软	3	0
知道创宇	1	0
奇虎 360	43	43

High-Tech Bridge	1	1
个人	11	11
报送总计	757	55
录入总计	250（去重）	55

表 1 成员单位上报漏洞统计

CNVD 整理和发布的漏洞涉及 Apple、Google、HP、Linux 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	Apple	19	8%
2	HP	15	6%
3	Linux	15	6%
4	Google	13	5%
5	TYPO3	12	5%
6	IBM	11	4%
7	Wireshark	10	4%
8	Novell	5	2%
9	Apache	5	2%
10	XenSource	3	1%
11	其它	142	57%

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 250 个漏洞。其中应用程序漏洞 159 个，WEB 应用漏洞 44 个，网络设备漏洞 7 个，操作系统漏洞 34 个，安全产品漏洞 1 个、数据库漏洞 5 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	159
WEB 应用漏洞	44
网络设备漏洞	7
操作系统漏洞	34
安全产品漏洞	1
数据库漏洞	5

表 3 漏洞按影响类型统计表

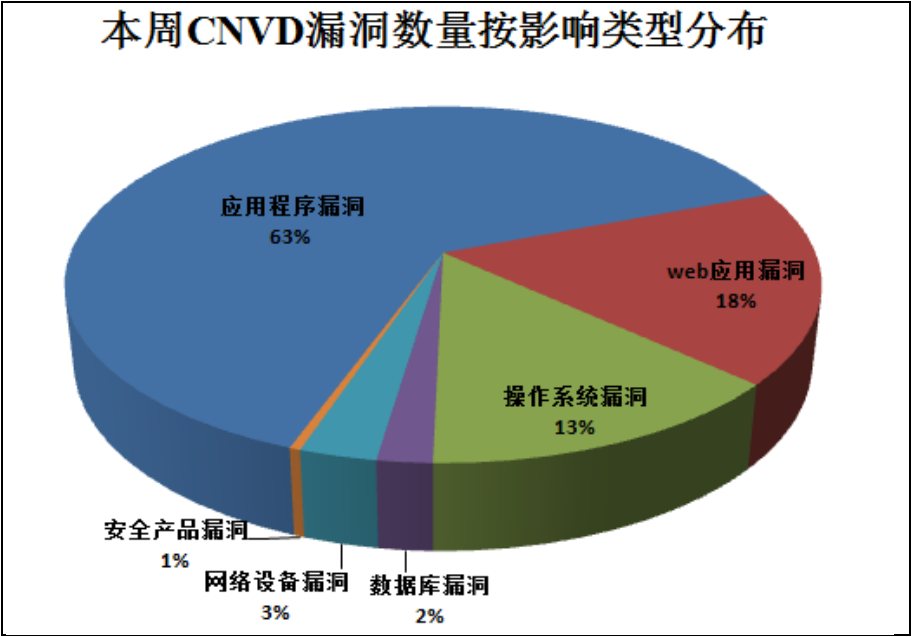


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 7 个网络设备漏洞：TP-Link IP Cameras 硬编码凭据安全绕过漏洞、TP-LINK IP Cameras 命令注入漏洞、Zavio IP Cameras 硬编码凭证身份验证安全绕过漏洞、NetGear WPN824v3 信息泄漏漏洞、NetGear DGN1000 'currentsetting.htm'安全绕过漏洞、多个 Netgear DGN 设备远程身份验证绕过漏洞。其中，“TP-Link IP Cameras 硬编码凭据安全绕过漏洞”、“TP-LINK IP Cameras 命令注入漏洞”和“Zavio IP Cameras 硬编码凭证身份验证安全绕过漏洞”的综合评级为“高危”。

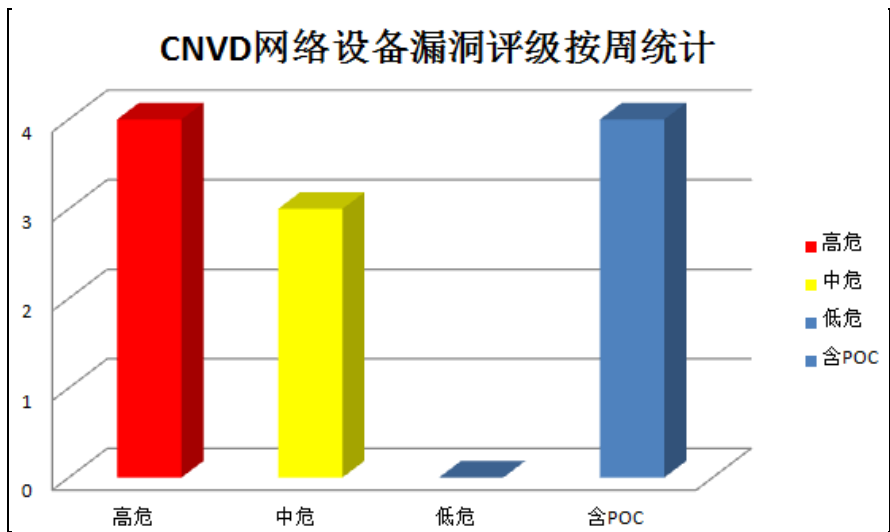


图 2 网络设备漏洞统计

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、Apple 产品安全漏洞

Apple Safari 是一款流行的 WEB 浏览器。Apple Mac OS X 是一款苹果公司开发的操作系统。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破坏内存或执行任意代码。

CNVD 收录的相关漏洞包括：Apple Safari Webkit 子帧处理跨站脚本漏洞、Apple Safari Webkit XSS 审核程序 URL 操作漏洞、Apple Safari 内存破坏漏洞、Apple Mac OS X 文本字形处理漏洞、Apple Mac OS X 本地安全绕过漏洞、Apple Mac OS X SMB 访问控制检查漏洞、Apple Mac OS X 电影文件处理漏洞、Apple Mac OS X Directory Service 远程缓冲区溢出漏洞等。上述漏洞中“Apple Mac OS X Directory Service 远程缓冲区溢出漏洞”的综合评级为“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-2013-25998>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25999>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26000>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25992>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25993>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25994>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25995>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25996>

2、Google Chrome 安全漏洞

Google Chrome 是一款浏览器。本周，Google Chrome 被披露存在安全漏洞，攻击者可以利用漏洞使应用程序崩溃或以应用程序上下文执行任意代码。

CNVD 收录的相关漏洞包括：Google Chrome 存在多个未明漏洞、Google Chrome PDFviewer 不正确释放内存漏洞、Google Chrome 输入处理内存错误引用漏洞、Google Chrome 图像处理内存错误引用漏洞、Google Chrome HTML 5 音频处理内存错误引用漏洞、Google Chrome 本命名空间污染漏洞、Google Chrome workers 访问数据库 API 漏洞、Google Chrome SVG 内存错误引用漏洞。上述漏洞中除“Google Chrome PDF viewer 不正确释放内存漏洞”外，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-2013-26104>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25898>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25899>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25900>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25901>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25902>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25903>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25904>

3、HP Data Protector 安全漏洞

HP Data Protector 是一款备份与恢复软件。本周，上述产品被披露存在多个远程代码执行漏洞。远程攻击者利用漏洞以应用程序上下文执行任意代码。

CNVD 收录的相关漏洞包括：HP Data Protector 远程代码执行漏洞（CNVD-2013-25917、CNVD-2013-25918、CNVD-2013-25919、CNVD-2013-25909、CNVD-2013-25910、CNVD-2013-25911、CNVD-2013-25912、CNVD-2013-25913）。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-2013-25917>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25918>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25919>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25909>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25910>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25911>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25912>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25913>

4、IBM 产品安全漏洞

IBM AIX 是一款商业主机操作系统。IBM DB2 Universal Database Server 是一款大型的商业关系数据库。IBM Tivoli Netcool 是 IBM 推出的网管解决方案。IBM Cúram Social Program Management 用于在一个可配置架构上交付预建社会项目组件、业务流程、工具集和界面。IBM QRadar 通过监控及关联日志和流量识别异常行为。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞提升权限，造成拒绝服务或执行任意代码。

CNVD 收录的相关漏洞包括：IBM AIX 'arp.ib'权限提升漏洞、IBM AIX 'ibstat'权限提升漏洞、IBM Cúram Social Program Management Jsp Scriplet 重定向漏洞、IBM Tivoli Netcool Transaction MIB 缓冲区溢出漏洞、IBM AIX IPv6 报文处理远程拒绝服务漏洞、IBM Tivoli Netcool 存在多个缓冲区溢出漏洞、IBM QRadar 安全信息和事件管理器远程命令注入漏洞、IBM DB2/DB2 Connect Audit Facility 本地权限提升漏洞。其中，“IBM Tivoli Netcool Transaction MIB 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-2013-26251>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26252>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26253>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26010>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26008>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26009>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25845>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25844>

5、Wireshark 产品安全漏洞

Wireshark 是一款开放源代码的网络协议分析工具。本周，上述产品被披露存在多个拒绝服务漏洞。允许远程攻击者利用漏洞使应用程序崩溃。

CNVD 收录的相关漏洞包括：Wireshark PPP 解析器拒绝服务漏洞、Wireshark NBAP 解析器拒绝服务漏洞、Wireshark RDP 解析器拒绝服务漏洞、Wireshark GSMCBCH 解析器拒绝服务漏洞、Wireshark AssaAbloyR3 解析器拒绝服务漏洞、Wireshark HTTP 解析器拒绝服务漏洞、Wireshark Ixia IxVeriWave 文件解析器拒绝服务漏洞、Wireshark DCPETSI 解析器拒绝服务漏洞。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-2013-26512>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26513>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26514>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26515>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26516>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26517>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26518>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-26519>

6、QNAP VioStor NVR/QNAP NAS 远程命令执行漏洞

QNAP VioStor NVR 是一款网络影像监控系统，QNAP NAS 是一款网络存储系统。本周，上述产品被披露存在一个综合评级为“高危”的远程命令执行漏洞。允许任意用户，如 Guest 用户以管理员权限执行任意命令。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-2013-26020>

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-2013-25842	Apache Subversion 'accept()'远程拒绝服务漏洞	高	Apache Subversion 1.7.10 或 1.6.23 已经修复此漏洞，建议用户下载更新： http://subversion.apache.org/
CNVD-2013-25860	TYPO3 'meta_feedit'扩展 SQL 注入漏洞	高	暂无
CNVD-2013-25981	Apache Struts OGNL 表达式注入漏洞（CNVD-2013-25981）	高	Apache Struts 2.3.14.3 已经修复此漏洞，建议用户下载更新： http://struts.apache.org/download.cgi#struts23143
CNVD-2013-26001	CMS Gratis Indonesia 'config.php' PHP 代码注入漏洞	高	暂无
CNVD-2013-26011	ISC BIND 递归查询处理拒绝服务漏洞	高	ISC BIND 9.6-ESV-R9-P1,9.8.5-P1,9.9.3-P1 已经修复此漏洞，建议用户下载更新： http://ftp.isc.org/isc/bind9
CNVD-2013-26016	Parallels Plesk Panel 任意 PHP 代码注入漏洞	高	暂无
CNVD-2013-26269	Openchrome X Window 系统客户端库存在多个整数溢出漏洞	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.x.org/wiki/Development/Security/Advisory-2013-05-23
CNVD-2013-26263	ZPanel 'Protect Directory'模块任意命令执行漏洞	高	暂无
CNVD-2013-26220	PHP 'php_quot_print_encode()'缓冲区溢出漏洞	高	PHP 5.4.16 和 5.3.26 版本已修复此漏洞，建议用户下载使用： http://www.php.net/ChangeLog-5.php
CNVD-2013-26021	QNAP VioStor NVR 跨站请求伪造漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，IBM、HP Data Protector 和 QNAP VioStor NVR 的多款企业级应用被披露存在漏洞，而 Apple Safari、Apple Mac OS X、Google Chrome 和 Wireshark 等桌面操作系统和应用程序也被披露存在多个漏洞，相关企业及个人用户及时升级软件。此外，ISC BIND 本周披露存在高危漏洞，威胁到网络基础设施运行安全。而 Apache Struts 在 5 月底被披露存在远程代码执行高危漏洞后在本周又被披露存在一个高危漏洞，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、TP-Link 发布升级程序，修补 IP Cameras 产品安全漏洞

TP-Link IP Cameras 是一款 IP 摄像机设备。本周，TP-Link 发布升级程序，修补了 IP Cameras 产品存在的漏洞。攻击者可以利用漏洞未经授权访问设备或执行任意命令。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/34435>

<http://www.cnvd.org.cn/patchInfo/show/34417>

本周要闻速递

1. Google 将公布一周内不能修复的安全漏洞

Google 正在针对安全漏洞推行新的“积极”反应时间期限，供应商将会有七天的时间修补漏洞、通知公众或停止运行受感染的产品。如果研究人员发现正被实际攻击利用而以前未曾发觉的严重漏洞，他们将得到 Google 的准许，在向受影响的供应商进行通报七天后公布问题的细节。Google 在周三宣布了新的推荐“积极时间期限”，此举将大幅缩短现行为期 60 天的推荐披露时间。对一些供应商来说，七天的反应期限也许难以达到，Google 工程师坚称，这是一个必要的措施以对有目标的攻击威胁做出反应。

参考链接：<http://article.pchome.net/content-1621505.html>

2. 搜狗输入法惊曝安全漏洞

网络热传搜狗输入法导致用户敏感信息泄露，其中包括语音、照片、证件信息等。搜狗方面表示，系统本身并不存在漏洞，用户信息泄露是由于搜索引擎的违规抓取。上述所谓的漏洞，出自搜狗手机输入法中的“多媒体输入”功能。借助这一去年 5 月发布的功能，用户之间能够分享图片、语音、文字等信息，而其原理就是将用户想要分享的信息，上传到搜狗服务器中，形成一个可以点击查看的链接。在这种模式下，任何人知道相关内容的存储地址，就能点击查看。此事曝出后，搜狗官方回应称，用户的“多媒体输入”信息泄漏，与搜索引擎没有遵守相关 robots.txt 协议有关。并且指出重点问题处在 Bing 搜索引擎中，且搜狗已经与 Bing 一直在沟通解决相关问题。

参考链接：<http://www.taihainet.com/lifeid/science/201306/1080486.html>

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