

信息安全漏洞周报

2013 年 07 月 29 日-2013 年 08 月 04 日

2013 年第 31 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低。

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 101 个，其中高危漏洞 35 个、中危漏洞 58 个、低危漏洞 8 个。上述漏洞中，可利用来实施远程攻击的漏洞有 92 个。本周收录的漏洞中，已有 73 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“Juniper Networks Junos 存在多个 HTML 注入漏洞”、“Broadkam PJ871 验证绕过漏洞”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 101 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，知道创宇公司、上海交大、High-TechBridge Security Research Lab 以及个人报送者向 CNVD 提交了 56 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	116	0
绿盟科技	67	0
安天实验室	165	0
天融信	110	0
恒安嘉新	32	0
知道创宇	3	3
上海交大	21	21

High-Tech Bridge	2	2
个人	30	30
报送总计	546	56
录入总计	101（去重）	56

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Wireshark Foundation、HP、Symantec 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	Wireshark Foundation	17	17%
2	HP	9	9%
3	Symantec	6	6%
4	PineApp	6	6%
5	IBM	4	4%
6	OpenAFS	2	1%
7	Cisco	2	2%
8	Apache	2	2%
9	McAfee	1	1%
10	Red Hat	1	1%
11	其它	51	50%

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 101 个漏洞。其中应用程序漏洞 78 个，WEB 应用漏洞 8 个，操作系统漏洞 2 个，网络设备漏洞 5 个，安全产品漏洞 8 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	8
网络设备漏洞	5
操作系统漏洞	2
安全产品漏洞	8
数据库漏洞	0

表 3 漏洞按影响类型统计表

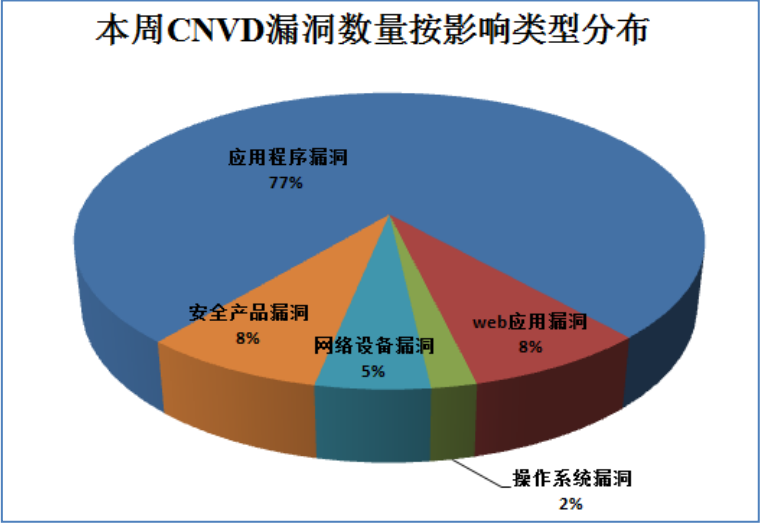


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 4 个电信行业漏洞和 1 个工控系统漏洞（如下列表所示）。其中，“Cogent Real-Time Systems DataHub 远程栈缓冲区溢出漏洞”、ISC BIND 9 DNS RDATA 处理远程拒绝服务漏洞”的综合评级均为“高危”。相关厂商已经发布了漏洞修复程序。本周，CNVD 未收录移动互联网行业漏洞。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
工控系统	CNVD-2013-30240	Cogent Real-Time Systems DataHub 远程栈缓冲区溢出漏洞	高危	有补丁
电信	CNVD-2013-30248	ISC BIND 9 DNS RDATA 处理远程拒绝服务漏洞	高危	有补丁
电信	CNVD-2013-30247	IBM WebSphere Commerce Enterprise 会话劫持验证绕过漏洞	中危	有补丁
电信	CNVD-2013-30246	IBM WebSphere Commerce Enterprise 请求处理验证绕过漏洞	中危	有补丁
电信	CNVD-2013-30225	Cisco Identity Services Engine Software 防火墙实现拒绝服务漏洞	中危	有补丁

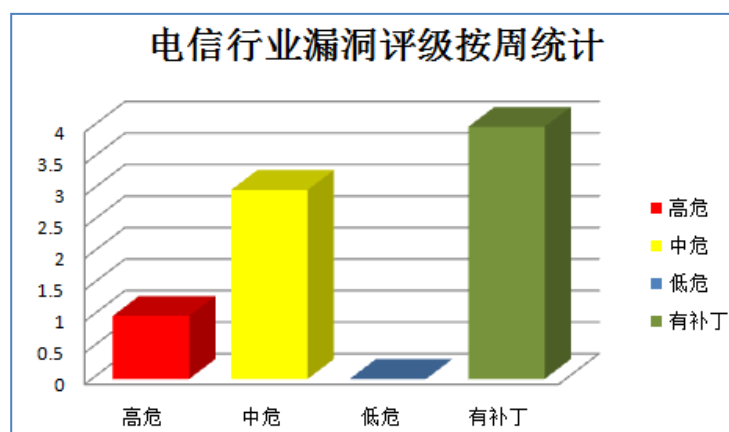


图 2 电信行业漏洞统计

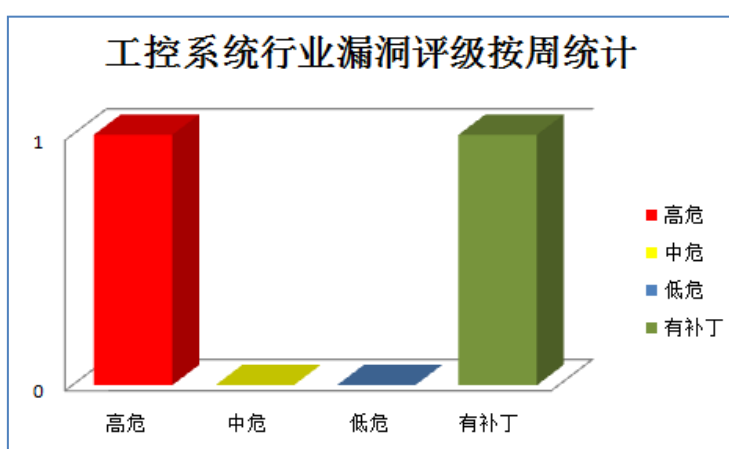


图 3 工控系统行业漏洞统计

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、Google 产品安全漏洞

Google Chrome 是一款开源的 WEB 浏览器。本周，该产品被披露存在安全漏洞，攻击者利用漏洞可导致应用程序崩溃或远程执行任意代码。

CNVD 收录的相关漏洞包括：Google Chrome V8 类型混淆漏洞、Google Chrome MutationObserver 内存错误引用漏洞、Google Chrome DOM 内存错误引用漏洞（CNVD-2013-30450）、Google Chrome 存在多个内存错误引用漏洞、Google v8 FullCodegen / Hydrogen Compare-Literal 行为不一致存在未明漏洞、Google v8 存在未明漏洞、Google Chrome 帧处理源绕过漏洞。上述漏洞中，除“Google v8 FullCodegen / Hydrogen Compare-Literal 行为不一致存在未明漏洞、Google v8 存在未明漏洞、Google Chrome 帧处理源绕过漏洞”外，其余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 提醒广大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-2013-30448>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30449>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30450>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30451>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30452>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30453>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30454>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30447>

2、TP-Link 产品安全漏洞

TP-Link TL-SC3171 IP camera 是一款网络摄像头设备。本周, 该产品被披露存在多个安全漏洞, 远程攻击者利用漏洞可执行未授权的远程固件升级, 上传任意文件, 执行任意命令, 控制该设备。

CNVD 收录的相关漏洞包括: TP-Link TL-SC3171 IP Camera 未授权固件升级漏洞、TP-Link TL-SC3171 IP Camera 未授权文件上传漏洞、TP-Link TL-SC3171 IP Camera 远程命令注入漏洞、TP-Link TL-SC3171 IP Camera OS 命令注入漏洞。其中, “TP-Link TL-SC3171 IP Camera 未授权固件升级漏洞、TP-Link TL-SC3171 IP Camera 未授权文件上传漏洞”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-2013-30481>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30480>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30479>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30478>

3、Siemens 产品安全漏洞

Siemens Scalance W-700 Series 是西门子开发的工业无线交换机设备; Siemens SIMATIC WinCC 基于 Windows 平台, 为工业领域提供完备的监控与数据采集(SCADA)功能。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获取敏感信息, 执行恶意操作, 进行网络钓鱼等攻击。

CNVD 收录的相关漏洞包括: Siemens Scalance W-700 系列身份验证绕过漏洞、Siemens Scalance W-700 系列内置 SSL 证书欺骗漏洞、Siemens SIMATIC WinCC TIA Portal 跨站请求伪造漏洞、Siemens SIMATIC WinCC TIA Portal URL 重定向漏洞。其中, “Siemens Scalance W-700 系列身份验证绕过漏洞”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-2013-30475>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30474>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30476>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30477>

4、Wireshark 安全漏洞

Wireshark 是一款开放源代码的网络协议分析工具。本周，该产品被披露存在多个漏洞。攻击者利用漏洞可导致应用程序崩溃。

CNVD 收录的相关漏洞包括：Wireshark Bluetooth OBEX 解析器整数符号错误拒绝服务漏洞、Wireshark DIS 解析器拒绝服务漏洞、Wireshark PROFINET Real-Time 解析器畸形报文处理拒绝服务漏洞、Wireshark ASN.1 PER 解析器畸形报文处理拒绝服务漏洞、Wireshark Netmon File 解析器畸形 Trace 文件处理拒绝服务漏洞（CNVD-2013-30277）、Wireshark Netmon File 解析器畸形 Trace 文件处理拒绝服务漏洞、Wireshark GSM A Common 解析器特殊报文处理拒绝服务漏洞、Wireshark GSM RR 解析器特殊报文处理拒绝服务漏洞等。其中，“Wireshark Bluetooth OBEX 解析器整数符号错误拒绝服务漏洞、Wireshark DIS 解析器拒绝服务漏洞”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-2013-30271>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30272>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30279>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30278>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30277>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30276>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30275>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30274>

5、Broadkam PJ871 验证绕过漏洞

Broadkam PJ871 是一款 DSL 路由器设备。本周，该产品被披露存在一个验证绕过漏洞。Broadkam PJ871 DSL 路由器对密码更换请求未进行正确的验证，远程攻击者利用漏洞可提交特殊请求，更改任意用户密码，访问未授权的应用设备。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-2013-30223>

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-2013-30467	Cisco Wide Area Application Services Central Manager 远程代	高	Cisco Wide Area Application Services 5.0.3e, 5.1.1c, 5.2.1 已经修

	码执行漏洞		复此漏洞，建议用户下载更新： http://www.cisco.com/go/psirt
CNVD-2013-30458	OpenEMM SOAP API SQL 注入漏洞	高	暂无
CNVD-2013-30465	Adobe Digital Editions 嵌入字体处理内存破坏漏洞	高	Adobe Digital Editions 2.0.1 已经修复此漏洞，建议用户下载更新： http://www.adobe.com/products/digital-editions/download.html
CNVD-2013-30239	ASUS RT-AC66U 存在多个缓冲区溢出漏洞	高	暂无
CNVD-2013-30455	HP SiteScope 存在未明远程代码执行漏洞	高	HP SiteScope v11.22 已经修复此漏洞，建议用户下载更新： http://support.openview.hp.com/selfsolve/patches
CNVD-2013-30237	Symantec Web Gateway 控制台 Radius 验证任意命令执行漏洞	高	Symantec Web Gateway version 5.1.1 已经修复此漏洞，建议用户下载更新： http://www.symantec.com/business/web-gateway
CNVD-2013-30441	Cotonti 'c'参数 SQL 注入漏洞	高	Cotonti 0.9.14 已经修复此漏洞，建议用户下载更新： http://www.cotonti.com/news/announce/siena_0914_released
CNVD-2013-30281	PineApp Mail-SeCure 'test_li_connection.php'远程命令注入漏洞	高	暂无
CNVD-2013-30240	Cogent Real-Time Systems DataHub 远程栈缓冲区溢出漏洞	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.cogentdatahub.com/Info/130712_ZDI-CAN-1915_Response.html
CNVD-2013-30260	Trendnet TEW-812DRU 存在多个命令注入漏洞	高	暂无

表 3 部分高危漏洞列表

小结： 本周，Google Chrome 被披露存在多个漏洞，攻击者利用漏洞可导致应用程序崩溃或执行任意代码，有可能诱发大规模网页篡改和挂马攻击。Wireshark 以及 TP-Link 和 Siemens 的多款产品被披露存在多个漏洞，攻击者利用漏洞可执行恶意操作，控制设备，导致拒绝服务攻击。此外，Broadkam PJ871 路由设备被披露存在一个零日漏洞，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、Cisco 发布升级程序，修补多款产品安全漏洞

Cisco Identity Services Engine 身份服务引擎是一款用于 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，Cisco 发布升级程序，修补多款产品存在的漏洞。攻击者可利用漏洞使进程崩溃，获取敏感信息或者劫持用户会话。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/37958>
<http://www.cnvd.org.cn/patchInfo/show/36560>

本周要闻速递

1. 苹果修补 iOS 装置的充电漏洞

先前研究人员制作了一个名为 Mactans 的恶意充电器，只要连结 iOS 装置，不需要与使用者互动，该装置亦无须越狱，在一分钟内就能将恶意程式安装至装置内。苹果宣称已在 iOS 7 最新的测试版中修补相关漏洞。研究人员则说新版 iOS 7 会额外询问使用者是否信任正要连结的电脑。据报告，所有的 iOS 装置都会受到上述漏洞影响，最简单的一个保障方式就是别把装置插到别人的电脑或充电器上充电。

参考链接：<http://tech.hexun.com/2013-08-04/156774713.html>

2. 部分运营商修复 SIM 卡漏洞

北京时间 8 月 2 日晚间消息，柏林安全研究实验室(Security Research Labs)创始人卡斯滕·诺尔(Karsten Nohl)周三表示，主要的移动运营商已经修复了影响全球 7.5 亿部手机的 SIM 卡安全漏洞。诺尔 7 月 21 日向媒体爆料，称发现部分手机 SIM 卡采用的加密技术存在安全漏洞，网络犯罪分子可以获得 SIM 卡的数字密钥，进而破译 SIM 卡并进行修改。一旦掌握了数字密钥，黑客就可以通过短信向这张 SIM 卡发送病毒。结果，黑客就能窃听机主的通话，通过手机支付系统购买东西，甚至盗用机主的身份从事其他活动。他仅仅通过一台 PC，在大约两分钟内就能破译手机 SIM 卡数字密钥并发送病毒信息。据他估计，全球最多会有 7.5 亿部手机易于遭受这种攻击。诺尔原计划在 7 月 27 日至 8 月 1 日于拉斯维加斯召开的“黑帽大会”上展示该漏洞，但诺尔周三表示，已经有 5 家主要的移动运营商修复了该漏洞，导致他只能展示一部分攻击内容。

参考链接：<http://tech.sina.com.cn/t/2013-08-02/21128601289.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路安全技术协调组织，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