

信息安全漏洞周报

2013 年 05 月 20 日-2013 年 05 月 26 日

2013 年第 21 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 164 个，其中高危漏洞 66 个、中危漏洞 85 个、低危漏洞 13 个。上述漏洞中，可利用来实施远程攻击的漏洞有 150 个。本周收录的漏洞中，已有 138 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“MiniWeb HTTP Server POST 请求处理拒绝服务漏洞”、“ZPanel 'templateparser.class.php' PHP 代码注入漏洞”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 家成员单位和多个合作伙伴及个人报送了本周收录的全部 164 个漏洞。各单位报送情况如表 1 所示。其中，安天实验室、绿盟科技等单位报送数量较多。此外，CNCERT 分中心、奇虎公司以及个人报送者向 CNVD 提交了 17 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	19	0
绿盟科技	76	0
安天实验室	149	0
天融信	63	0
恒安嘉新	8	0
奇虎 360	25（去重）	25
CNCERT 相关分中心	2	2
个人	13	13
报送总计	355	40

录入总计	164（去重）	40
------	---------	----

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Apple、Adobe、Google、Mozilla 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	21	13%
2	Adobe	16	10%
3	Google	15	9%
4	Mozilla	14	9%
5	WordPress	13	8%
6	ownCloud	12	7%
7	IBM	9	5%
8	Wireshark	8	5%
9	Juniper Networks	7	4%
10	Joomla!	3	2%
11	其它	46	28%

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 164 个漏洞。其中应用程序漏洞 133 个，WEB 应用漏洞 22 个，网络设备漏洞 2 个，操作系统漏洞 7 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	133
WEB 应用漏洞	22
网络设备漏洞	2
操作系统漏洞	7
安全产品漏洞	0
数据库漏洞	0

表 3 漏洞按影响类型统计表

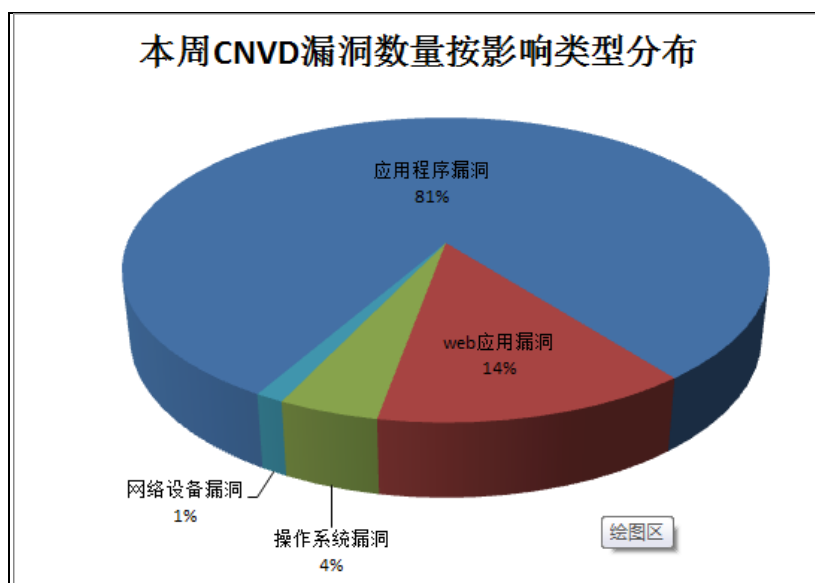


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 2 个网络设备漏洞：TURCK BL20/BL67 FTP 内置账户安全绕过漏洞、Huawei Quidway 交换机 SPU 防火墙模块信息泄漏漏洞。其中，“TURCK BL20/BL67 FTP 内置账户安全绕过漏洞”的综合评级为“高危”。相关厂商已经发布了漏洞修补程序。

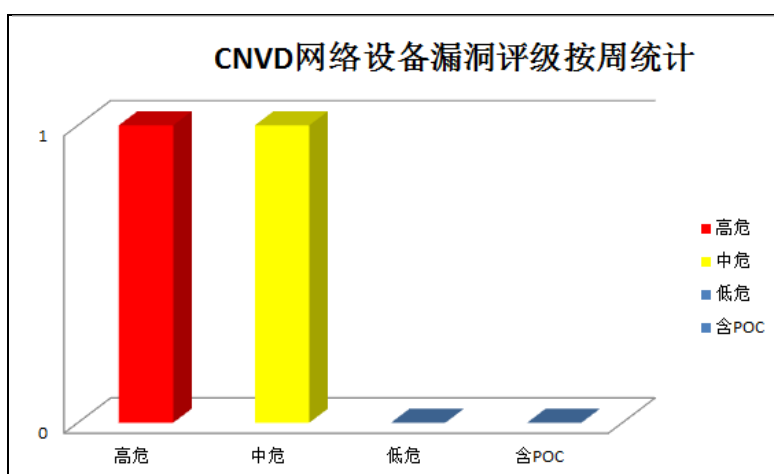


图 2 网络设备漏洞统计

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、Google 产品安全漏洞

Google Chrome 是一款 Web 浏览器。本周，该产品被披露存在安全漏洞，远程攻击

者利用漏洞通过未知向量可导致拒绝服务。

CNVD 收录的相关漏洞包括：Google Chrome 内存错误引用漏洞(CNVD-2013-25135、CNVD-2013-25132、CNVD-2013-25131、CNVD-2013-25130、CNVD-2013-25126)、Google Chrome 拒绝服务漏洞(CNVD-2013-25133)、Google ChromeWeb Audio 功能漏洞、Google Chrome 存在多个漏洞等。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-2013-25135>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25133>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25132>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25131>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25130>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25127>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25126>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25136>

2、Apple 产品安全漏洞

WebKit 是一款开源的浏览器引擎。本周，该产品被披露存在安全漏洞，攻击者利用漏洞可使应用程序崩溃或执行任意代码。

CNVD 收录的相关漏洞包括：Apple iTunes 内存破坏漏洞（CNVD-2013-25016、CNVD-2013-25015、CNVD-2013-25014、CNVD-2013-25013、CNVD-2013-25012、CNVD-2013-25011、CNVD-2013-25010、CNVD-2013-25009）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-2013-25016>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25015>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25014>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25013>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25012>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25011>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25010>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25009>

3、Wireshark 安全漏洞

Wireshark 是一款开源的网络协议分析器。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使应用程序崩溃，导致拒绝服务攻击。

CNVD 收录的相关漏洞包括：Wireshark Websocket 解析器远程拒绝服务漏洞、Wireshark PPP CCP 解析器远程拒绝服务漏洞、Wireshark MySQL 解析器远程拒绝服务

漏洞、Wireshark MPEG DSM-CC 解析器远程拒绝服务漏洞、Wireshark GTPv2 解析器远程拒绝服务漏洞、Wireshark ETCH 解析器远程拒绝服务漏洞、Wireshark DCP ETSI 解析器远程拒绝服务漏洞、Wireshark ASN.1 BER 解析器远程拒绝服务漏洞。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-2013-25089>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25086>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25085>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25084>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25083>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25082>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25081>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25080>

4、Juniper 产品安全漏洞

Juniper Networks JUNOS 是一款 Juniper 网络公司的系列边界路由器所运行的操作系统。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使应用程序崩溃，导致拒绝服务攻击。

CNVD 收录的相关漏洞包括：Juniper Networks Junos SIP 报文拒绝服务漏洞、Juniper Networks Junos Proxy ARP 拒绝服务漏洞、Juniper Networks Junos J-Web Sajax 远程代码执行漏洞、Juniper Networks Junos IPv6 Egress 过滤器拒绝服务漏洞、Juniper Networks Junos GRE 报文处理拒绝服务漏洞、Juniper Networks Junos 防火墙绕过拒绝服务漏洞、Juniper Networks Junos Ethernet 报文拒绝服务漏洞。其中，“Juniper Networks Junos SIP 报文拒绝服务漏洞、Juniper Networks Junos Proxy ARP 拒绝服务漏洞、Juniper Networks Junos J-Web Sajax 远程代码执行漏洞、Juniper Networks Junos IPv6 Egress 过滤器拒绝服务漏洞”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-2013-25096>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25046>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25045>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25044>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25043>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25042>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-25041>

5、ZPanel 'templateparser.class.php' PHP 代码注入漏洞

ZPanel 是一个免费的虚拟主机控制面板,支持 Windows,Linux,UNIX 和 MacOSX 等

多个操作系统。本周，该产品被披露存在一个综合评级为“高危”的 PHP 代码注入漏洞。ZPanel 'templateparser.class.php'未能正确过滤用户提交的恶意代码，远程攻击者利用漏洞可注入恶意代码，并结合 ZPanels `zsudo`程序，以 root 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-2013-24554>

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-2013-25106	SAProuter NI 路由消息处理漏洞	高	SAP Note 1820666 已修复此漏洞，建议用户下载使用： http://help.sap.com/saphelp_nw04/helpdata/en/4f/992ce8446d11d189700000e8322d00/frameset.htm
CNVD-2013-25102	TRIDIUM NiagaraAX 存在未明漏洞	高	暂无
CNVD-2013-25078	Trend Micro DirectPass 本地命令注入漏洞	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： http://esupport.trendmicro.com/solution/en-US/1096805.asp
CNVD-2013-25100	Quick Search 搜索字段缓冲区溢出漏洞	高	暂无
CNVD-2013-25075	TinyMCE MCIImageManager 插件任意文件上传漏洞	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://www.moxiecode.com
CNVD-2013-25073	Joomla! S5 Clan Roster 组件 SQL 注入漏洞	高	暂无
CNVD-2013-24962	Mutiny 存在多个目录遍历漏洞	高	厂商已经修复此漏洞，建议用户下载更新： http://www.mutiny.com/mutiny-support/update/
CNVD-2013-25070	php-Charts 'index.php'任意 PHP 代码执行漏洞	高	暂无
CNVD-2013-24970	ownCloud 'lib/db.php'脚本 SQL 注入漏洞	高	ownCloud 5.0.6 已经修复此漏洞，建议用户下载更新： http://download.owncloud.org

CNVD-2013-25067	MyHeritage SEQueryObject ActiveX AddLastNameTokens 方法任意代码执行漏洞	高	暂无
-----------------	---	---	----

表 3 部分高危漏洞列表

小结：本周，Google Chrome、WebKit 被披露存在多个安全漏洞，远程攻击者利用漏洞可使应用程序崩溃或执行任意代码。Wireshark、Juniper Networks JUNOS 存在的漏洞也会导致系统崩溃，造成拒绝服务攻击，相关管理员用户应及时升级软件。此外，ZPanel 被披露存在高危漏洞，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、Apache 发布升级程序，修补 Struts 产品安全漏洞

Apache Struts 是一个基于 Java Servlets,JavaBeans 和 JavaServer Pages (JSP)的 Web 应用框架。本周，Apache 发布升级程序，修补了 Struts 存在的漏洞。远程攻击者可利用漏洞执行任意命令。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/34266>

（注：对应最新版本为 2.3.14.2）

本周要闻速递

1. 多个游戏引擎爆 0day 漏洞

国外安全公司 ReVuln 的研究人员 Luigi Auriemma 和 Donato Ferrante 近期发表一篇名为“Exploiting Game Engines For Fun & Profit”的报告，报告中称发现多个游戏引擎如 CryEngine 3、id Tech 4 和 Hydrogen Engine 等游戏引擎的漏洞，成功利用可能获取控制权限。报告中提到，攻击者可以设置一个中介服务器，在游戏中会显示该服务器 IP，如果你加入了该服务器，可能就会利用远程代码执行漏洞，攻击你的计算机。另外一方面，攻击者会定制一些存在问题的地图，当你更新地图的时候可能会触发拒绝服务漏洞。参考链接：<http://labs.chinamobile.com/news/94750>

2. Struts2 再爆远程代码执行漏洞

Apache 官方的 struts2 产品，最近出了一个远程代码执行漏洞，编号“S2-013”，官方没有修补方案。Struts2 标签库中的 url 标签和 a 标签的 includeParams 这个属性，代表显示请求访问参数的含义，一旦它的值被赋予 ALL 或者 GET 或者 POST，就会显示具

体请求参数内容。按照正常的需求，把参数 urlencode 一下也就够了，struts 多做了一步，把参数做了 OGNL 解析，最终 TextParseUtil.translateVariables 会直接调用 OGNL 解析执行。

参考链接：<http://it.tom.com/network/242166/742172785558b.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