

信息安全漏洞周报

2013 年 05 月 13 日-2013 年 05 月 19 日

2013 年第 20 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 168 个，其中高危漏洞 67 个、中危漏洞 89 个、低危漏洞 12 个。上述漏洞中，可利用来实施远程攻击的漏洞有 155 个。本周收录的漏洞中，已有 124 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“No-IP Dynamic Update Client 'i'参数远程栈溢出漏洞”、“WordPress 插件 Securimage-WP 'siwp_test.php'跨站脚本漏洞”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 168 个漏洞。各单位报送情况如表 1 所示。其中，天融信、安天实验室等单位报送数量较多。此外，中国电力科学研究院信息安全实验室以及个人报送者向 CNVD 提交了 7 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	58	0
绿盟科技	96	0
安天实验室	162	0
天融信	129	0
恒安嘉新	15	0
东软	1	0
中国电力科学研究院 信息安全实验室	3	3
个人	4	4
报送总计	468	7

录入总计	168（去重）	7
------	---------	---

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Microsoft、Adobe、Cisco 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	Microsoft	31	18%
2	Adobe	24	14%
3	GroundWork	15	9%
4	Cisco	13	8%
5	IBM	6	4%
6	Brother International Corporation	6	4%
7	Wordpress	5	3%
8	Apache	4	2%
9	EMC	4	2%
10	AirDisk	3	2%
11	其它	57	34%

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 168 个漏洞。其中应用程序漏洞 130 个，WEB 应用漏洞 17 个，操作系统漏洞 5 个，网络设备漏洞 10 个，安全产品漏洞 6 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	130
WEB 应用漏洞	17
网络设备漏洞	10
操作系统漏洞	5
安全产品漏洞	6
数据库漏洞	0

表 3 漏洞按影响类型统计表

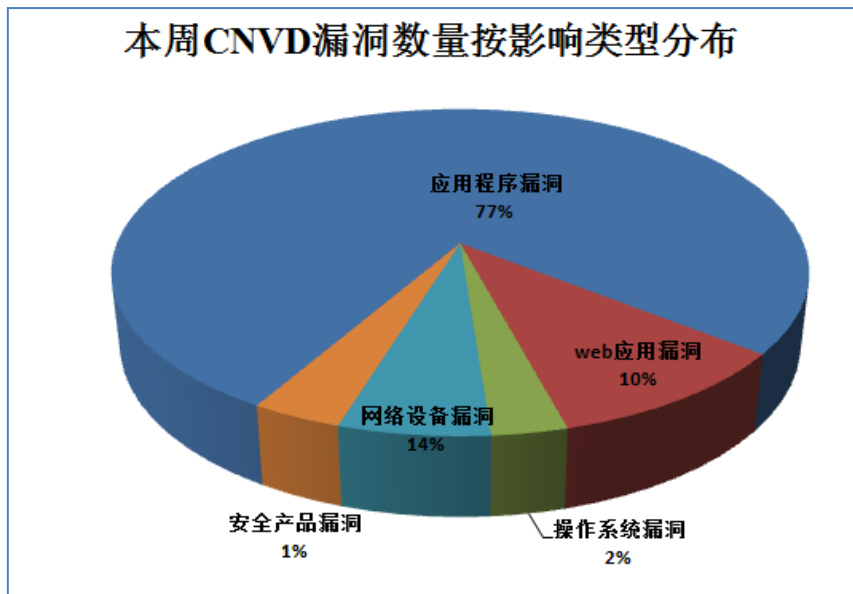


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 10 个网络设备漏洞：Cisco Unified Communications Manager 本地信息泄露漏洞、Cisco ISR G2 路由器 ISM 模块拒绝服务漏洞、Cisco IOS Aggregation Services Router Processor 拒绝服务漏洞、Brother MFC-9970CDW 存在多个跨站脚本漏洞、Brother MFC-9970CDW '/admin/admin_main.html'跨站脚本漏洞、Brother MFC-9970CDW 密码字段自动完成漏洞、Brother MFC-9970CDW Printer 信息泄露漏洞、Brother MFC-9970CDW 点击劫持漏洞、Brother MFC-9970CDW 信息泄露漏洞、Fujitsu Lifebook A512 多个搜索路径处理本地权限提升漏洞。其中，“Brother MFC-9970CDW 密码字段自动完成漏洞”的综合评级为“高危”。相关厂商已经发布了漏洞修补程序。

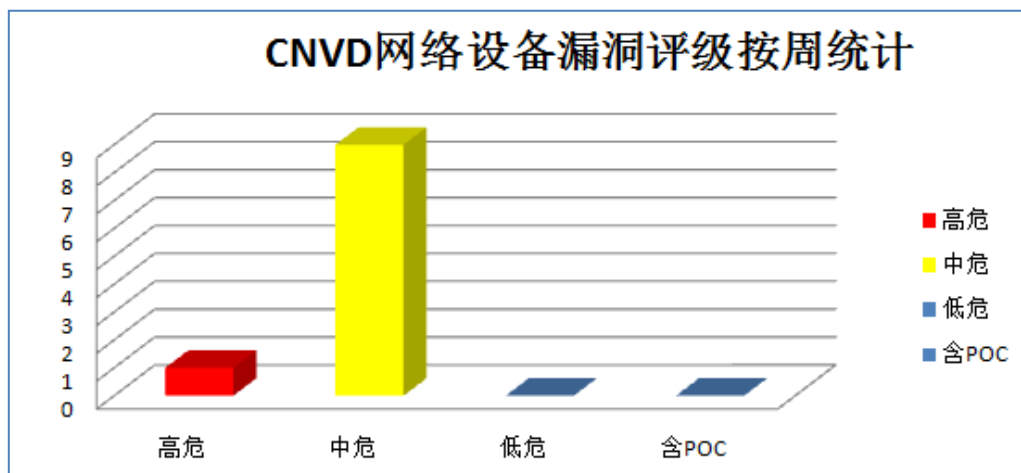


图 2 网络设备漏洞统计



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、Microsoft 产品安全漏洞

5 月 15 日，微软发布了 2013 年 5 月份的月度例行安全公告，共含 10 项更新，修复了涉及 Microsoft Windows、Internet Explorer、.NET Framework、Lync 和 Office 多个产品中存在的 33 个安全漏洞。利用上述漏洞，攻击者可以远程执行代码、进行拒绝服务攻击、窃取泄露敏感信息或提升特权。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer 内存错误引用远程代码执行漏洞（CNVD-2013-24603、CNVD-2013-24604）、Microsoft .NET Framework 身份验证旁路漏洞、Microsoft Windows 'Win32k.sys'窗口句柄漏洞、Microsoft Windows Kernel 'Win32k.sys'本地权限提升漏洞、Microsoft Windows DirectX 图形内核子系统双重提取漏洞、Microsoft Publisher 远程代码执行漏洞（CNVD-2013-24641）、Microsoft Lync 远程代码执行漏洞等。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-2013-24603>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-24604>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-24635>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-24638>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-24639>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-24640>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-24641>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-24660>

2、Adobe 产品安全漏洞

Adobe Reader/Acrobat 是处理 PDF 文件的应用程序。本周，上述产品被披露存在安全漏洞，攻击者利用漏洞可获得敏感信息，使应用程序崩溃或执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Reader 黑名单域处理存在未明漏洞、Adobe Reader/Acrobat 存在未明内存破坏漏洞（CNVD-2013-24626、CNVD-2013-24625、CNVD-2013-24624、CNVD-2013-24622、CNVD-2013-24621、CNVD-2013-24620）Adobe Reader / Acrobat Javascript API 存在未明信息泄漏漏洞等。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-2013-24627>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-24626>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-24625>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-24624>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-24623>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-24622>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-24621>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-24620>

3、Apache 产品安全漏洞

Apache HTTP Server 是开源 HTTP 服务器； Apache Tomcat 是开源的 JSP 应用程序。本周，上述 Apache 产品被披露存在多个安全漏洞。远程攻击者利用漏洞获得敏感信息，发起拒绝服务攻击，执行任意命令。

CNVD 收录的相关漏洞包括：Apache HTTP Server 日志内终端转义序列命令注入漏洞、Apache Tomcat 拒绝服务漏洞（CNVD-2013-24490）、Apache Tomcat 'AsyncListener' 信息泄露漏洞、Apache Tomcat FORM 认证会话固定漏洞。其中，“Apache HTTP Server 日志内终端转义序列命令注入漏洞”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-2013-24408>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-24490>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-24491>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-24492>

4、Apple 产品安全漏洞

WiFi Photo Transfer 是一款通过无线传送图片和视频的应用。 WiFi Photo & Video Access 用于把图像和视频传送到 iPhone 或 iPad 等设备的工具。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可获得敏感信息或劫持用户会话，执行任意命令。

CNVD 收录的相关漏洞包括：WiFi Album 文件夹名处理任意命令执行漏洞、Wifi Photo Transfer 多个文件扩展上传任意代码执行漏洞、Wifi Photo Transfer 相册名处理任意命令执行漏洞、WiFi Photo & Video Access 畸形图像请求拒绝服务漏洞、Wifi Photo Transfer 文件名跨站脚本漏洞、Wifi Photo Transfer 文件泄漏漏洞。其中，“WiFi Album 文件夹名处理任意命令执行漏洞、Wifi Photo Transfer 多个文件扩展上传任意代码执行漏洞、Wifi Photo Transfer 相册名处理任意命令执行漏洞”的综合评级均为“高危”。厂商尚未发布上述漏洞的修补程序。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-2013-24569>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-24571>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-24574>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-24570>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-24572>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-24573>

5、No-IP Dynamic Update Client 'i'参数远程栈溢出漏洞

No-IP Dynamic Update Client 是一款用于保持 IP 地址与特定 DNS 主机名同步的工具。本周，该产品被披露存在一个综合评级为“高危”的栈溢出漏洞。No-IP Dynamic Update Client 未能正确过滤用户提交给“i”参数的数据，远程攻击者利用漏洞可进行缓冲区溢出攻击，执行任意代码。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-2013-24691	Cisco TelePresence Supervisor MSE 拒绝服务漏洞	高	厂商已发布的最新版本或补丁： http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130515-mse
CNVD-2013-24577	ZyXEL ZyWALL Web 接口默认账户漏洞	高	暂无
CNVD-2013-24551	Libreswan atodn() DNS TXT 记录处理溢出漏洞	高	libreswan 3.2 或 3.3 版本已经修复此漏洞，建议用户下载更新： https://libreswan.org
CNVD-2013-24568	Strongswan atodn() DNS TXT 记录记录缓冲区溢出漏洞	高	暂无
CNVD-2013-24528	Linux kernel 'kernel/events/core.c'本地权限提升漏洞	高	厂商已发布的最新版本或补丁： http://news.ycombinator.com/item?id=5703758
CNVD-2013-24469	Dolibarr ERP/CRM 命令注入漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： https://github.com/Dolibarr/dolibarr/commit/9427e32e2ed54c1a2bc519a88c057207836df489
CNVD-2013-24567	SonicWall TZ Series Firewall Web 接口默认账户漏洞	高	暂无
CNVD-2013-24398	EMC AlphaStor 缓冲区溢出漏洞	高	厂商已发布的最新版本或补丁： http://archives.neohapsis.com/archives/bugtraq/2013-05/att-0035/ESA-2013-037.txt
CNVD-2013-24556	Openswan atodn() DNS TXT 记录记录缓冲区溢出漏洞	高	暂无

CNVD-2013-24348	CHICKEN POSIX 'select()'函数不完整修复远程缓冲区溢出漏洞	高	用户可参考如下第三方补丁以修复此漏洞： http://code.call-cc.org/cgi-bin/gitweb.cgi?p=chicken-core.git;a=commitdiff;h=766056cd5f26b1d529405705449cb534609c113
-----------------	--	---	--

表 3 部分高危漏洞列表

小结：本周，微软发布了 2013 年 5 月份的月度例行安全公告，共含 10 项更新，修复了涉及 Microsoft Windows、Internet Explorer、.NET Framework、Lync 和 Office 多个产品中存在的 33 个安全漏洞。Adobe Reader/Acrobat 和 Apache Tomcat/HTTP Server 被披露存在安全漏洞，攻击者利用漏洞可获得敏感信息，使应用程序崩溃或执行任意代码。Apple AppStore 多款应用存在漏洞，攻击者利用漏洞可获取敏感信息。此外，No-IP Dynamic Update Client 被披露存在高危漏洞，建议相关管理员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、Symantec 发布升级程序，修补 Brightmail Gateway 产品安全漏洞

Symantec Brightmail Gateway 是一款实时反垃圾邮件和病毒防护、高级内容过滤、防数据泄露解决方案。本周，Symantec 发布升级程序，修补了 Brightmail Gateway 存在的 HTML 注入漏洞。远程攻击者可以利用漏洞注入恶意 HTML 或脚本代码，获取敏感信息或劫持用户会话。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/33887>

本周要闻速递

1. 苹果曝漏洞 iPhone 能搜已删短信

通过 iPhone 的搜索功能却可以让短信“死而复生”。针对此问题，昨日下午记者致电苹果官方售后中心，售后客服人员表示，该问题在苹果系统研发至今存在的一个漏洞，各种版本的 iPhone 均存在类似的问题。在用户手机使用一段时间后，通过 Spotlight 搜索功能能够搜索到删除的信息。对于果粉们担心删除的信息被别人搜索到，苹果公司的客服人员提出了两种建议，一是在手机的“通用”设置页面中，将“Spotlight 搜索”选项中的“信息”选项前的勾选去除，关闭短信搜索功能。另外一种方法就是通过“恢复”手机更新系统，但客服人员提醒这种方法让手机里的信息被抹除，而且一段时间后，上

述问题可能还是会“复发”。对于如何能彻底解决该问题，该客服人员表示会尽快向相关负责人反映。

参考链接：<http://fj.sina.com.cn/news/b/2013-05-18/092730504.html>

2. 新的 Java 漏洞已成为大规模攻击的目标

最近修补的 Java 远程执行代码漏洞已经被网络犯罪分子利用，通过恐吓软件进行大规模的攻击。据国外媒体报道，一个标识为 CVE-2013-2423 的漏洞已经成为网络犯罪分子攻击的目标，而它正是甲骨文 4 月 16 日公布的 Java 7 Update 21 修复的 42 个问题之一。但甲骨文声称该漏洞仅影响客户端，而不是服务器。对于该漏洞造成的影响，甲骨文根据常见漏洞评分系统(CVSS)给出一个 4.3 的分数(满分为 10 分)，并且甲骨文还补充说：“只有不受信任的 Java Web Start 程序和不受信任的 Java applet 才可能利用该漏洞。”需要使用 Java 的用户(尤其是浏览器)应当尽快升级 Java 安装程序——Java 7 Update 21。这个版本还改变了网站加载 Web Java 程序时的安全提示，以便更好地区分不同类型的应用程序运行的风险。

参考链接：<http://it.anhuinews.com/872923/356514112604b.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