

信息安全漏洞周报

2013 年 07 月 08 日-2013 年 07 月 14 日

2013 年第 28 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 137 个，其中高危漏洞 70 个、中危漏洞 55 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 120 个。本周收录的漏洞中，已有 110 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“Android 绕过数字签名可修改代码漏洞”、“Nokia 1280 消息处理拒绝服务漏洞”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 家成员单位和合作伙伴及个人报送了本周收录的全部 137 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，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
安天实验室	160	0
天融信	108	0
启明星辰	107	0
绿盟科技	75	0
恒安嘉新	25	0
东软	1	0
天讯瑞达通信技术有限公司	15	0
个人	7	7

报送总计	498	7
录入总计	137（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、FFmpeg、Adobe 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	Microsoft	33	24%
2	FFmpeg	19	14%
3	Adobe	6	4%
4	Linux	4	3%
5	IBM	4	3%
6	D-Link	2	1%
7	Cisco	2	1%
8	Dell	2	1%
9	Apache	1	1%
10	McAfee	1	1%
11	其它	63	47%

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 137 个漏洞。其中应用程序漏洞 104 个，WEB 应用漏洞 14 个，操作系统漏洞 16 个，网络设备漏洞 3 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	104
WEB 应用漏洞	14
网络设备漏洞	3
操作系统漏洞	16
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

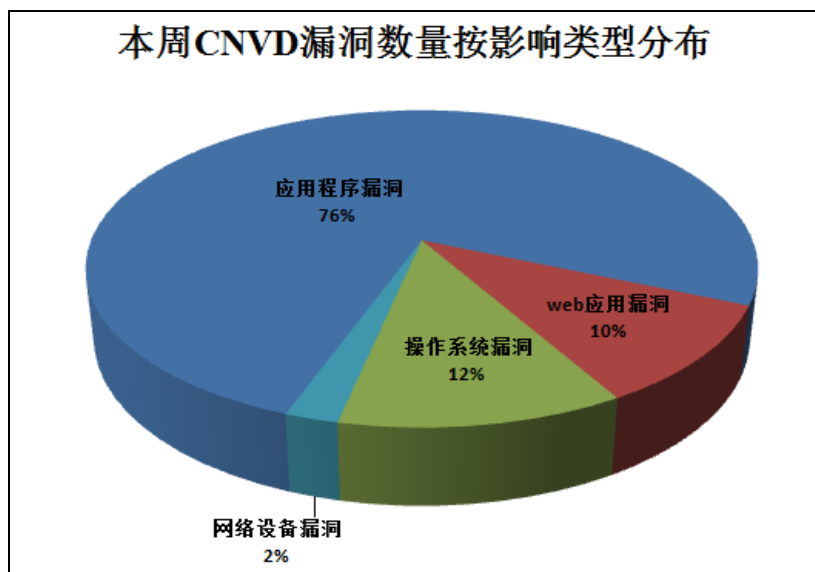


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 3 个网络设备漏洞：Nokia 1280 消息处理拒绝服务漏洞、多个 D-link 产品远程验证绕过漏洞、多个 D-Link 产品 UPnP SOAP 接口存在多个命令注入漏洞。其中，“多个 D-Link 产品 UPnP SOAP 接口存在多个命令注入漏洞”的综合评级为“高危”。目前，互联网上已经出现了针对“Nokia 1280 消息处理拒绝服务漏洞”的攻击代码。相关厂商已经发布了漏洞修复程序。

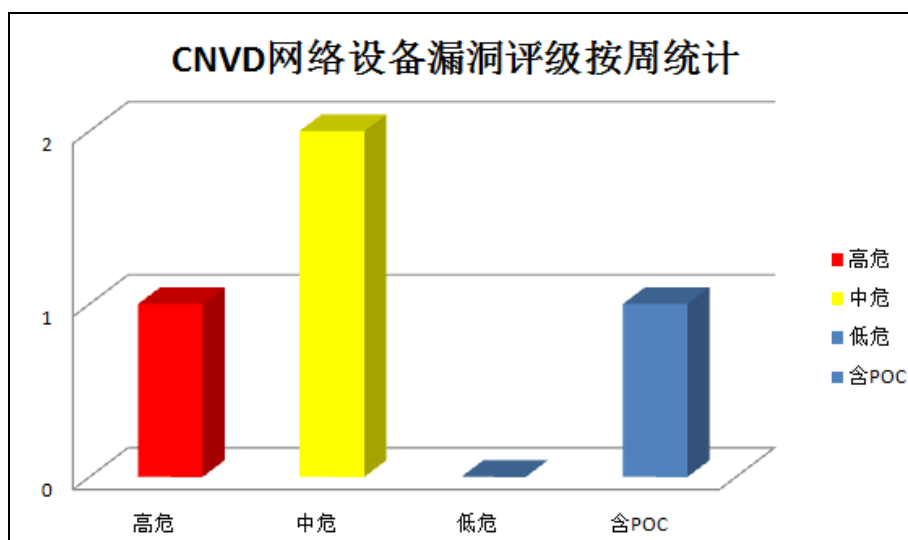


图 2 网络设备漏洞统计

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

7月10日，微软发布了2013年7月份的月度例行安全公告，共含7项更新，修复了Microsoft Windows、.NET Framework、Silverlight、Office、Visual Studio、Lync、Internet Explorer 和 Windows Defender 中存在的36个安全漏洞。其中，6项更新综合评级均为最高级“严重”（微软最高危害级别），剩余1项更新综合评级均为“重要”级别。利用上述漏洞，攻击者可以利用漏洞远程执行代码，提升特权。

CNVD收录的相关漏洞包括：Microsoft Windows win32k.sys 内存对象处理本地缓冲区溢出漏洞（CNVD-2013-28475）、Microsoft Windows win32k.sys 内存对象处理本地信息泄漏漏洞、Microsoft Internet Explorer 内存破坏漏洞（CNVD-2013-28466、CNVD-2013-28465、CNVD-2013-28427、CNVD-2013-28429）、Microsoft .NET Framework 权限提升漏洞、Microsoft .NET Framework 数组分配漏洞等。厂商已发布上述漏洞的修补程序。CNVD提醒广大Microsoft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-2013-28475>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28473>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28466>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28465>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28448>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28447>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28427>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28429>

2、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，攻击者利用漏洞可执行未经授权的操作，发起拒绝服务攻击或执行任意代码。

CNVD收录的相关漏洞包括：Google Chrome 存在漏洞（CNVD-2013-28589）、Google Chrome 内容错误引用漏洞（CNVD-2013-28586）、Google Chrome 内容错误引用漏洞、Google Chrome 内存错误引用远程代码执行漏洞、Google Chrome 存在多个未明漏洞（CNVD-2013-28576）、Google Chrome NPAPI 扩展漏洞（CNVD-2013-28588）、Google Chrome 拒绝服务漏洞（CNVD-2013-28587）、Google Android 'APK'代码远程安全绕过漏洞等。其中，除“Google Chrome NPAPI 扩展漏洞（CNVD-2013-28588）”和“Google Chrome 拒绝服务漏洞（CNVD-2013-28587）”外，其余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-2013-28589>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28586>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28585>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28583>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28576>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28546>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28588>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28587>

3、Adobe 产品安全漏洞

Adobe Shockwave Player 是一款用于播放使用 Director Shockwave Studio 制作的网页的软件；Adobe Flash Player 是一款 Flash 文件处理程序；Adobe ColdFusion 是一个动态 Web 服务器。本周，上述产品被披露存在多个安全漏洞。攻击者利用漏洞可导致应用程序崩溃或执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Shockwave Player 内存破坏漏洞（CNVD-2013-28439）、Adobe Flash Player PCM 缓冲区采样整数溢出漏洞、Adobe Flash Player 存在未明内存破坏漏洞、Adobe Flash Player 存在未明堆缓冲区溢出漏洞、Adobe ColdFusion 安全绕过漏洞（CNVD-2013-28435）、Adobe ColdFusion 存在未明远程拒绝服务漏洞。其中，除“Adobe ColdFusion 存在未明远程拒绝服务漏洞”外，其余漏洞的综合评级为“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-2013-28439>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28438>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28437>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28436>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28435>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28434>

4、FFmpeg 安全漏洞

FFmpeg 是一款用于录制、转换和流化音频和视频的完整解决方案。本周，FFmpeg 被披露存在多个漏洞。远程攻击者利用漏洞可导致应用程序崩溃或执行任意代码。

CNVD 收录的相关漏洞包括：FFmpeg/libav 'decode_band()' 内存破坏漏洞、FFmpeg/libav 'decode_band()' 内存破坏漏洞、FFmpeg/libav 'ivi_decode_coded_blocks' 数组索引处理存在未明漏洞、FFmpeg/libav 'ivi_process_empty_tile' 数组索引处理存在未明漏洞、FFmpeg/libav BLK 宏像素位置范围处理漏洞、FFmpeg/libav 'synthfilt_build_sb_samples' 存在未明漏洞、FFmpeg/libav 'wsvqa_read_header' 两次释放漏洞、FFmpeg/libav 'vqa_decode_init' 缓冲区溢出漏洞等。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-2013-28383>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28382>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28381>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28380>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28379>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28378>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28377>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28376>

5、Android 绕过数字签名可修改代码漏洞

Android 是基于 Linux 开放性内核的操作系统, 是 Google 公司在 2007 年 11 月 5 日公布的手机操作系统。本周, 该产品被披露存在一个高危漏洞。攻击者利用漏洞可修改 APK 代码, 不破坏应用的加密签名, 将合法应用转变为恶意代码的程序。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-2013-28152>

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-2013-28568	VideoLAN VLC media player 存在多个缓冲区溢出漏洞	高	暂无
CNVD-2013-28480	OTRS/OTRS ITSM SQL 注入漏洞	高	OTRS 3.0.22, 3.1.18, 3.2.9, OTRS ITSM 3.0.9, 3.1.10, 3.2.7 已经修复此漏洞, 建议用户下载更新: http://www.otrs.com/
CNVD-2013-28398	Time Out Internet 53 端口 SSH 通道验证绕过漏洞	高	暂无
CNVD-2013-28479	Nagios Remote Plug-In Executor 任意命令执行漏洞	高	Nagios Remote Plug-In Executor (NRPE) 2.14 已经修复此漏洞, 建议用户下载更新: http://sourceforge.net/projects/nagios/files/nrpe-2.x/
CNVD-2013-28397	Supermicro BMC 实现验证绕过 IPMI 命令执行漏洞	高	暂无
CNVD-2013-28477	多个 QNX 产品栈缓冲区溢出漏洞	高	用户可参考如下厂商提供的安全补丁以修复此漏洞: http://www.qnx.com/download/feature.ht

			ml?programid=24850
CNVD-2013-28395	OpenNetAdmin 'ona.log'文件远程 PHP 代码执行漏洞	高	暂无
CNVD-2013-28399	Triangle Research Nano-10 PLC 特制报文拒绝服务漏洞	高	Triangle Research Nano-10 PLC r81 已经修复此漏洞，建议用户下载更新： http://www.tri-plc.com/nano10.htm
CNVD-2013-28393	IPMI RAKP 验证密码哈希泄漏漏洞	高	暂无
CNVD-2013-28313	IBM AIX TFTP Client 安全绕过漏洞	高	目前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://aix.software.ibm.com/aix/efixes/security/tftp_advisory.asc

表 3 部分高危漏洞列表

小结：本周，微软发布了 2013 年 7 月份的月度例行安全公告，共含 7 项更新，修复了 Microsoft Windows、.NET Framework、Silverlight、Office、Visual Studio、Lync、Internet Explorer 和 Windows Defender 中存在的 36 个安全漏洞。攻击者可以利用漏洞远程执行代码，提升特权。Google Chrome 被披露存在多个漏洞，攻击者利用漏洞可执行任意代码或导致大规模网页篡改。FFmpeg 和 Adobe 多款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或执行任意代码。此外，Android 操作系统被披露存在一个签名绕过的高危零日漏洞，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、McAfee 发布升级程序，修补 Data Loss Prevention 漏洞

McAfee Data Loss Prevention 是一款数据丢失防护应用。本周，McAfee 发布升级程序，修补了 Data Loss Prevention 存在的信息泄露漏洞。远程攻击者利用漏洞使用"filepath"和"filename"参数指定任意文件，读取服务器上存储的任意文件。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/35063>

本周要闻速递

1. CM 10.1.2 修复第二个致命漏洞

CyanogenMod10.1.1 整合了 Google 早在二月份就发布的所谓“万能密钥”(Master Key)漏洞补丁,据说当前 99%的安卓手机都存在此问题。10.1.2 修补的漏洞是刚刚被曝光的,编号 bug 9695860,和上述“万能密钥”漏洞类似也可以让没有签名认证的 apk 直接运行。这也是新版本唯一的变化,防止安卓应用绕过签名认证来擅自运行。建议使用 CM 10.1.x 的玩家尽快更新到 10.1.2。

参考链接: <http://news.mydrivers.com/1/269/269047.htm>

2. 微软警示 IE 漏洞已被利用

7 月 10 日,微软推送了 7 月份安全补丁,其中 MS13-055 是针对 IE 的累积性安全补丁,修复了 17 个秘密报告的漏洞,这些漏洞可能导致远程代码执行,影响 IE6、IE7、IE8、IE9 和 IE10。在该补丁发布几个小时后,微软悄然对其页面进行了修改,之前微软表示并没有人利用这些漏洞实施网络攻击,用户尚未受到影响。然而,事实是,已经有 IE8 用户受到攻击。微软证实,利用 MS13-055 所修复的漏洞进行的攻击已经存在了,有 IE8 用户向微软报告了此事,因此建议大家尽早安装 MS13-055。“微软发现有人利用 CVE-2013-3163 漏洞进行的对 IE8 的攻击。”目前还没有发现针对其它版本 IE 进行的攻击,但是微软督促所有用户抓紧时间安装补丁,避免遭受不必要的损失。

参考链接: <http://news.zol.com.cn/tech/90411.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