国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2013 年 03 月 11 日-2013 年 03 月 17 日 **2013 年 第 11 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 124 个，其中高危漏洞 54 个、中危漏洞 70 个、低危漏洞 10 个。上述漏洞中，可利用来实施远程攻击的漏洞有 109 个。本周收录的漏洞中，已有 71 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“PHP CMS 文件后缀提取错误代码上传漏洞”、“McAfee Vulnerability Manager 'cert_cn'参数跨站脚本漏洞”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 7 家成员单位和多个合作伙伴报送了本周收录的全部 124 个漏洞。各单位报送情况如表 1 所示。其中，启明星辰、绿盟科技等单位报送数量较多。此外，奇虎公司以及个人报送者向 CNVD 提交了 5 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	63	0
绿盟科技	106	0
安天实验室	38	0
天融信	35	0
恒安嘉新	28	0
东软	3	0
奇虎 360	3	3
个人	2	2
报送总计	278	5

录入总计	124（去重）	5

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、WordPress、Adobe、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	Microsoft	22	18%
2	WordPress	17	14%
3	Adobe	9	7%
4	Linux	9	7%
5	Apple	7	6%
6	Puppet	7	6%
7	FFmpeg	7	6%
8	Oracle	5	4%
9	Cisco	3	2%
10	GroundWork	3	2%
11	其它	35	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 124 个漏洞。其中应用程序漏洞 76 个，WEB 应用漏洞 25 个，操作系统漏洞 20 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	76
WEB 应用漏洞	25
网络设备漏洞	3
操作系统漏洞	20
数据库漏洞	0
安全产品漏洞	0

表 3 漏洞按影响类型统计表

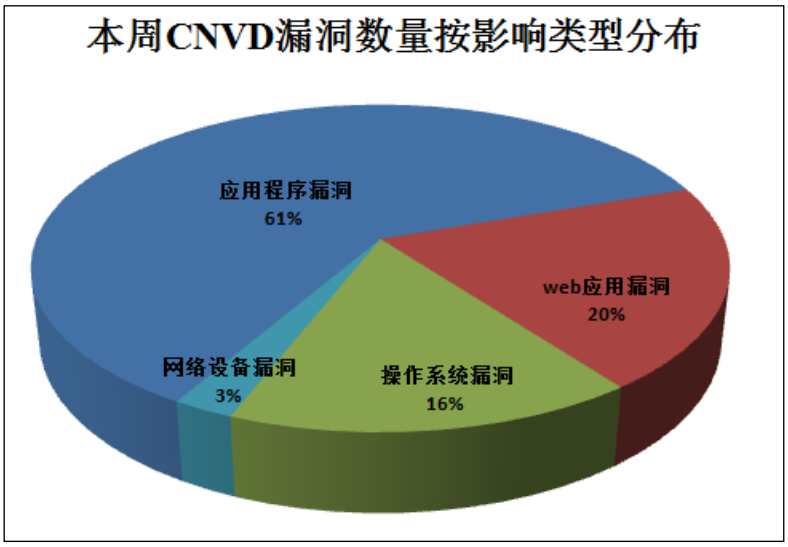

图 1 本周漏洞按影响类型分布

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：Samsung TV 'SOAPACTION'拒绝服务漏洞、Cisco Wireless LAN Controller 远程拒绝服务漏洞、TP-LINK 部分路由器存在后门漏洞。

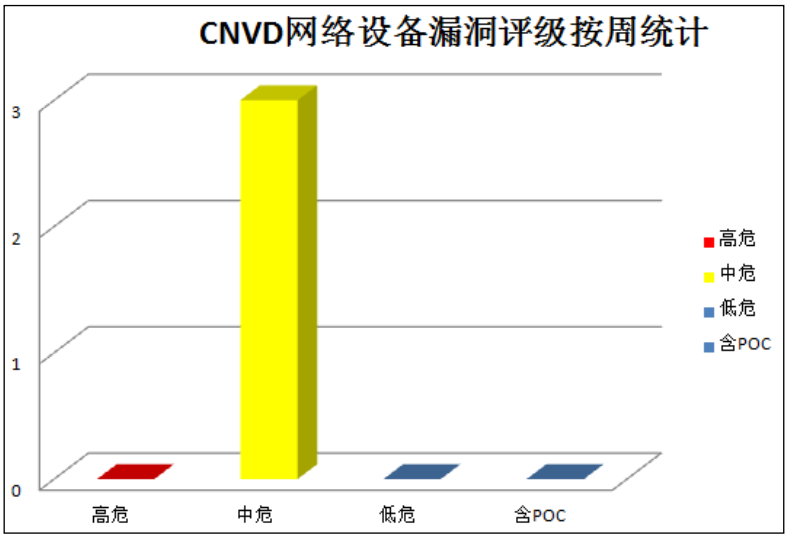

图 2 网络设备漏洞统计

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

3 月 13 日，微软发布了 2013 年 3 月份的月度例行安全公告，共含 7 项更新，修复

了 Microsoft Windows、Internet Explorer、Silverlight、Office 和服务器软件中存在的 20 个安全漏洞。其中，4 项更新为最高级“严重”级别（微软定义的威胁最高级别），其余 3 项为“重要”。利用上述漏洞，攻击者可以远程执行代码、提升特权、窃取敏感信息。

CNVD 收录的相关漏洞包括：Microsoft Silverlight 两次引用远程代码执行漏洞、Microsoft Visio Viewer VSD 文件格式代码执行漏洞、Microsoft SharePoint 拒绝服务漏洞、Microsoft Internet Explorer 内存错误引用代码执行漏洞（CNVD-2013-20795、CNVD-2013-20794、CNVD-2013-20793、CNVD-2013-20792、CNVD-2013-20787）等。上述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/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20808

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20804

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20801

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20795

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20794

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20793

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20792

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20787

2、Oracle 产品安全漏洞

Oracle Java Runtime Environment (JRE)是一款为 JAVA 应用程序提供可靠运行环境的解决方案。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可远程执行任意代码。

CNVD 收录的相关漏洞包括：Oracle Java SE 存在未明任意代码执行漏洞（CNVD-2013-20761、CNVD-2013-20765、CNVD-2013-20764）、Oracle Java SE 存在未明堆缓冲区溢出漏洞、Oracle Java SE 远程代码执行漏洞（CNVD-2013-20726）。上述漏洞的综合评级均为“高危”。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/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20761

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20765

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20764

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20763

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20726

3、Adobe 产品安全漏洞

Adobe Reader 是一款流行的 PDF 处理程序；Adobe Flash Player 是一款 Flash 文件处

理程序。本周，上述 Adobe 产品被披露存在多个安全漏洞，攻击者利用漏洞可执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Reader 存在未明远程代码执行漏洞（CNVD-2013-20721）、Adobe Flash Player 存在未明远程代码执行漏洞、Adobe Reader 存在未明任意代码执行漏洞、Adobe Reader 存在未明沙盒绕过代码执行漏洞、Adobe Flash Player 存在未明漏洞（CNVD-2013-20759）、Adobe Flash Player/AIR 内存破坏漏洞（CNVD-2013-20785）、Adobe Flash Player/AIR 内存错误引用远程代码执行漏洞、Adobe Flash Player/AIR 堆缓冲区溢出漏洞等。上述漏洞的综合评级均为“高危”。厂商已发布了“Adobe Flash Player/AIR 内存破坏漏洞（CNVD-2013-20785）、Adobe Flash Player/AIR 内存错误引用远程代码执行漏洞、Adobe Flash Player/AIR 堆缓冲区溢出漏洞”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/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20721

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20720

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20762

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20760

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20759

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20785

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20784

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20786

4、Linux Kernel 安全漏洞

Linux Kernel 是 Linux 操作系统的内核。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可提升权限，获得敏感信息，导致系统崩溃，造成拒绝服务攻击。

CNVD 收录的相关漏洞包括：Linux Kernel 'sa_restorer'本地信息泄露漏洞、Linux Kernel 'i915 DRM'驱动程序整数溢出漏洞、Linux Kernel 'xfrm_user'本地权限提升漏洞、Linux Kernel 'xfrm_user'本地权限提升漏洞、Linux Kernel 'chase_port()' USB 拔掉拒绝服务漏洞、Linux Kernel 'install_user_keyrings()' 竞争条件漏洞、Linux Kernel 蓝牙 HIDP 实现信息泄露漏洞。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/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20777

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20755

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20754

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20752

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20730

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20716

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20732

5、PHPCMS 文件后缀提取错误代码上传漏洞

PHPCMS 一款网站管理系统。本周，该产品被披露存在一个综合评级为“高危”的上传漏洞。攻击者利用漏洞可绕过安全限制，上传网站后门，严重的可获得服务器主机权限。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/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20717

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/publish/main/52/index.html

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2013-20783	TP-LINK 部分路由器存在后门漏洞	高	暂无
CNVD-2013-20741	FFmpeg 'old_codec37()'函数数组外访问漏洞	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://ffmpeg.org/security.html
CNVD-2013-20719	WebKit 类型混淆远程代码执行漏洞	高	Google Chrome 25.0.1364.160 已经修复此漏洞，建议用户下载更新：http://googlechromereleases.blogspot.com/2013/03/stable-channel-update_7.html
CNVD-2013-20748	Ruby ftpd 'filename'参数任意命令执行漏洞	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：https://rubygems.org/gems/ftpd
CNVD-2013-20743	Websense TRITON Unified Security Center 存在多个漏洞	高	暂无
CNVD-2013-20731	FFmpeg 'advance_line()'函数数组外访问漏洞	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://ffmpeg.org/security.html
CNVD-2013-20744	Websense TRITON Unified Security Center SQL 注入漏洞	高	暂无
CNVD-2013-20727	Ruby crack Gem XML 参数解析漏洞	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://rubygems.org/gems/crack

CNVD-2013-20717	PHPCMS 文件后缀提取错误代码上传漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周二，微软发布了 2013 年 3 月份的月度例行安全公告，共含 7 项更新，修复了 Microsoft Windows、Internet Explorer、Silverlight、Office 和服务器软件中存在的 20 个安全漏洞，建议服务器和桌面操作系统用户及时更新 Oracle JRE 和 Adobe 的多款产品也被披露存在多个漏洞，攻击者利用漏洞发起大规模挂马攻击，而 Linux Kernel 被披露存在多个安全漏洞，攻击者利用漏洞可提升权限，，窃取信息或导致拒绝服务攻击。

此外，国内应用广泛的 PHPCMS 被披露存在零日漏洞，相关网站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 Network Admission Control 和 WLC 漏洞

Cisco WLC 负责全系统的无线 LAN 功能，例如安全策略、入侵保护、RF 管理，服务质量和移动性。Cisco Network Admission Control 是提供 Cisco TrustSec 解决方案的策略组件。本周，Cisco 修补了 Network Admission Control 和 WLC 存在的漏洞。攻击者可利用此漏洞获得敏感信息或造成拒绝服务。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/sites/main/preview/bdgg_preview.htm?tid=32756

http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=32755

本周要闻速递

1. 傲游云浏览器修复 HTML5 漏洞

3 月 15 日消息，傲游昨日在其论坛发布了 Windows 版傲游云浏览器新版，此次更新版的傲游云浏览器 Windows 版 4.0.5.600beta 修复了 HTML5“硬盘爆仓”漏洞，免遭恶意程序的攻击，保障用户的存储安全。据悉，这是新一代网页编程语言 HTML5 的“硬盘爆仓”漏洞，利用该漏洞，用户的硬盘中可产生大量本地存储文件，导致其硬盘最终被占满。对此，傲游迅速在更新版中修复了这一漏洞，阻止了用户的硬盘空间在短时间内被大量吃掉。用户可以通过自测形式，来检验自己使用的浏览器是否存在这一爆仓风险。在浏览器地址中输入 http://www.filldisk.com/，会看到如下图所示的测试网站，在这里可以看到自动播放各种猫的图片，然后不断的填充下载到用户当前的硬盘里面，直到塞满为止。当然，只要点击图片下方的“Stopthemadness”按钮，它就会将所有吞下的

空间完全释放掉。

参考链接：http://www.techweb.com.cn/news/2013-03-15/1283368.shtml

2. iOS 爆新漏洞威胁用户数据

iOS 爆出配置文件漏洞可用来盗取用户数据。漏洞由以色列信息安全公司 Skycure 发布。黑客可以利用 iOS 的配置文件 mobileconfig 中的漏洞绕开苹果的恶意软件保护系统，窃取用户信息。iPhone 与 iPad 用户的数据通信将遭受威胁。 Skycure 公司建议 iOS 用户禁止任何非信任网站和应用程序的任何配置请求。在使用 mobileconfig 配置文件相关的应用时，最好事先咨询相关应用开发公司。

参考链接：http://news.xinhuanet.com/info/2013-03/15/c_132236137.htm

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