国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2013 年 04 月 15 日-2013 年 04 月 21 日 **2013 年第 16 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**高**。

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 267 个，其中高危漏洞 55 个、中危漏洞 159 个、低危漏洞 53 个。上述漏洞中，可利用来实施远程攻击的漏洞有 225 个。本周收录的漏洞中，已有 228 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“NetGear WNR1000 '.jpg'安全绕过漏洞”、“Todoo Forum todooforum.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 8 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 267 个漏洞。各单位报送情况如表 1 所示。其中，绿盟科技、启明星辰、天融信等单位报送数量较多。此外，天融信、知道创宇、奇虎公司、 High-Tech Bridge Security Research Lab 以及个人报送者向 CNVD 提交了 27 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	241	0
绿盟科技	170	0
安天实验室	62	0
天融信	123	1
恒安嘉新	22	0
知道创宇	3	3
奇虎 360	3	3
东软	3	0

High-Tech Bridge Security Research Lab	2	2
个人	18	18
报送总计	647	27
录入总计	267（去重）	27

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Oracle、Linux、CMSLogik、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	Oracle	152	57%
2	Linux	12	4%
3	CMSLogik	8	3%
4	Cisco	7	3%
5	IBM	5	2%
6	Google	5	2%
7	Mediawiki	5	2%
8	Novell	2	1%
9	RedHat	2	1%
10	OpenStack	2	1%
11	其它	67	24%

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 267 个漏洞。其中应用程序漏洞 170 个，WEB 应用漏洞 31 个，操作系统漏洞 28 个，数据库漏洞 28 个，网络设备漏洞 8 个，安全产品漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	170
WEB 应用漏洞	31
网络设备漏洞	8
操作系统漏洞	28
安全产品漏洞	2
数据库漏洞	28

表 3 漏洞按影响类型统计表

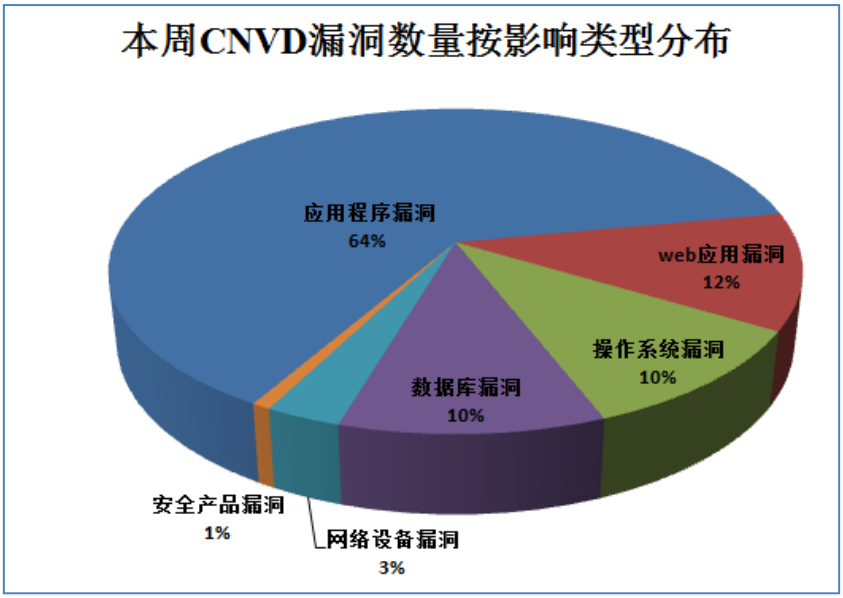

图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 8 个网络设备漏洞：Linksys EA2700 源代码泄露漏洞、Cisco IOS XE 组播 Leaf Recycle Elimination 拒绝服务漏洞、Arecont Vision AV1355DN 拒绝服务漏洞、多个 Motorola 产品 root 访问漏洞、多个 Motorola 产品 bootloader 解锁漏洞、Sitecom WLM-3500 后门账户验证绕过漏洞、TRENDNet IP Camera 特制 URL 处理验证绕过漏洞、NetGear WNR1000 '.jpg'安全绕过漏洞。其中，“Cisco IOS XE 组播 Leaf Recycle Elimination 拒绝服务漏洞、Arecont Vision AV1355DN 拒绝服务漏洞、Sitecom WLM-3500 后门账户验证绕过漏洞”的综合评级均为“高危”。目前，互联网上已经出现了针对“TRENDNet IP Camera 特制 URL 处理验证绕过漏洞、NetGear WNR1000 '.jpg'安全绕过漏洞”的攻击代码，相关厂商已经发布了漏洞修补程序。

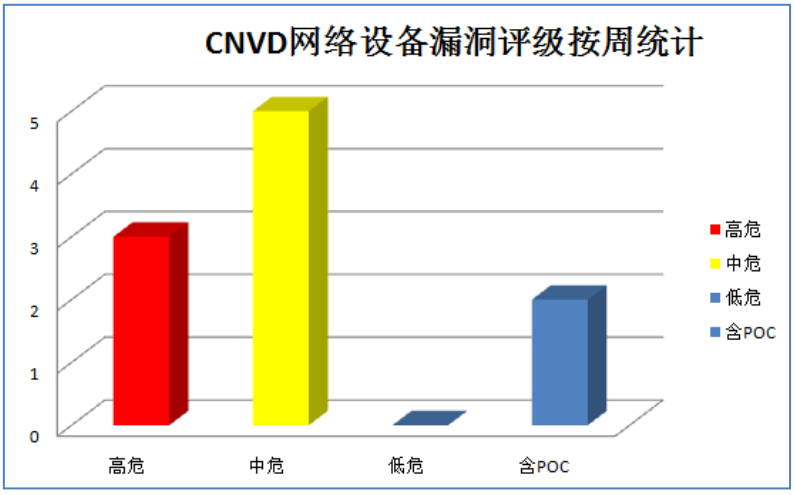

图 2 网络设备漏洞统计

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、Oracle 产品安全漏洞

Oracle PeopleSoft Enterprise 是一款企业人力资本管理软件；Oracle Java Runtime Environment 是一款为 JAVA 应用程序提供运行环境的解决方案；Oracle Database Server 是一款商业性质的大型数据库。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可远程执行任意代码。

CNVD 收录的相关漏洞包括：Oracle PeopleSoft Enterprise PeopleTools WorkCenter 子件存在未明远程漏洞、Oracle PeopleSoft Enterprise PeopleTools WorkCenter 子件存在未明远程漏洞、Oracle PeopleSoft Enterprise PeopleTools PIA Core Technology 子件存在未明远程漏洞、Oracle Java JDK/JRE Deployment 子件存在未明任意代码执行漏洞（CNVD-2013-22465、CNVD-2013-22462）、Oracle Database Server Workload Manager 组件远程安全漏洞、Oracle Java JDK/JRE 2D 子件存在未明任意代码执行漏洞、Oracle Java JDK/JRE Install 子件存在未明任意代码执行漏洞等。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-2013-22571

http://www.cnvd.org.cn/flaw/show/CNVD-2013-22568

http://www.cnvd.org.cn/flaw/show/CNVD-2013-22566

http://www.cnvd.org.cn/flaw/show/CNVD-2013-22465

http://www.cnvd.org.cn/flaw/show/CNVD-2013-22462

http://www.cnvd.org.cn/flaw/show/CNVD-2013-22398

http://www.cnvd.org.cn/flaw/show/CNVD-2013-22421

http://www.cnvd.org.cn/flaw/show/CNVD-2013-22419

2、Google Chrome OS 安全漏洞

Google Chrome OS 是一款轻量级开源操作系统。本周，该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，执行恶意操作。

CNVD 收录的相关漏洞包括：Google Chrome OS O3D 插件内存信息泄露漏洞、Google Chrome OS O3D 插件内存错误引用漏洞、Google Chrome OS O3D 和 Goolge Talk 插件源锁定绕过漏洞（CNVD-2013-22390、CNVD-2013-22391）。上述漏洞中，除“Google Chrome OS O3D 插件内存信息泄露漏洞”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-2013-22388

http://www.cnvd.org.cn/flaw/show/CNVD-2013-22389

http://www.cnvd.org.cn/flaw/show/CNVD-2013-22390

http://www.cnvd.org.cn/flaw/show/CNVD-2013-22391

3、Linux 产品安全漏洞

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，攻击者利用漏洞获得敏感信息，绕过安全限制，执行未授权的操作，导致内核崩溃。

CNVD 收录的相关漏洞包括：Linux Kernel 存在多个本地安全绕过漏洞、Linux Kernel 存在多个本地信息泄露漏洞、Linux Kernel Tracing 存在多个本地拒绝服务漏洞、Linux Kernel CIFS NULL 指针引用拒绝服务漏洞、Linux Kernel'net/xfrm/xfrm_user.c'本地信息泄露漏洞（CNVD-2013-22179）、Linux Kernel ATM 本地信息泄露漏洞、Linux Kernel Bluetooth RFCOMM 本地信息泄露漏洞、Linux Kernel Bluetooth 协议栈本地信息泄露漏洞等。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-2013-22387

http://www.cnvd.org.cn/flaw/show/CNVD-2013-22386

http://www.cnvd.org.cn/flaw/show/CNVD-2013-22366

http://www.cnvd.org.cn/flaw/show/CNVD-2013-22364

http://www.cnvd.org.cn/flaw/show/CNVD-2013-22179

http://www.cnvd.org.cn/flaw/show/CNVD-2013-22134

http://www.cnvd.org.cn/flaw/show/CNVD-2013-22135

http://www.cnvd.org.cn/flaw/show/CNVD-2013-22136

4、Cisco 产品安全漏洞

Cisco Jabber XCP 是一款可扩展通信平台；Cisco IOS 是一款互联网络操作系统；Cisco Firewall Services Module 是防火墙服务模块；Cisco Adaptive Security Appliance 提供安全和 VPN 服务的模块。本周，上述思科产品被披露存在多个安全漏洞，攻击者利用漏洞可发起拒绝服务攻击。

CNVD 收录的相关漏洞包括： Cisco IOS XE 组播 Leaf Recycle Elimination 拒绝服务漏洞、Cisco Jabber 可扩展通信平台拒绝服务漏洞、多个 Cisco 产品拒绝服务漏洞。其中，“Cisco IOS XE 组播 Leaf Recycle Elimination 拒绝服务漏洞”的综合评级为“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-2013-22152

http://www.cnvd.org.cn/flaw/show/CNVD-2013-22151

http://www.cnvd.org.cn/flaw/show/CNVD-2013-22150

5、Todoo Forum todooforum.php 跨站脚本漏洞

Todoo Forum 是一款基于 WEB 的论坛建站程序。本周，该产品被披露存在一个跨站脚本漏洞。由于 Todoo Forum todooforum.php 未能正确过滤用户通过'id_post'和'pg'参数传递的输入，远程攻击者利用漏洞可进行跨站脚本攻击，获得敏感信息或劫持用户会话。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-2013-22646

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-2013-22363	RubyGems 'md2pdf'远程命令注入漏洞	高	暂无
CNVD-2013-22448	Oracle Java JDK/JRE JavaFX 子件存在未明任意代码执行漏洞（CNVD-2013-22448）	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.oracle.com/technetwork/topics/security/javacpuapr2013-1928497.html
CNVD-2013-22334	RubyGems kelredd-pruview 存在多个远程命令注入漏洞	高	暂无
CNVD-2013-22362	phpVMS Virtual Airline Administration SQL 注入漏洞	高	暂无
CNVD-2013-22154	Electro Industries GaugeTech Nexus 设备默认账户漏洞	高	暂无
CNVD-2013-22357	AT-TFTP 服务器栈缓冲区溢出漏洞	高	暂无
CNVD-2013-22142	IBM Sterling B2B Integrator 远程命令执行漏洞	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-01.ibm.com/support/docview.wss?uid=swg24034725
CNVD-2013-22349	MinaliC 远程缓冲区溢出漏洞	高	暂无
CNVD-2013-22433	Oracle Java JDK/JRE JavaFX 子件存在未明任意代码执行漏洞	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.oracle.com/technetwork/topics/security/javacpuapr2013-1928497.htm

			1
CNVD-2013-22343	Arecont Vision AV1355DN 拒绝服务漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，Google Chrome OS、Linux Kernel 被披露存在多个漏洞，攻击者利用漏洞可获得敏感信息，执行恶意操作。Oracle 和 Cisco 多款产品也被披露存在多个漏洞，攻击者利用漏洞可远程执行任意代码，发起拒绝服务攻击。此外，Todoo Forum 被披露存在零日漏洞，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、RedHat 发布升级程序，修补 JBoss Enterprise Portal Platform 产品安全漏洞

JBoss Enterprise Portal Platform 是一款构建和管理动态网站的平台。本周，RedHat 发布升级程序，修补了 JBoss Enterprise Portal Platform 存在的漏洞。远程攻击者可利用漏洞读取任意文件，修改站点内容，删除站点，或修改应用在站点 portlet 中的访问控制。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/33276

http://www.cnvd.org.cn/patchInfo/show/33277

本周要闻速递

1. Android 被指存在危险漏洞

本周，ACLU 提交了一份 17 页的报告，因为无法提供即时的系统升级，黑客们会有机会窃取隐私数据。谷歌 Android 操作系统可以被各种厂商使用，谷歌尽力与这些厂商合作，希望时刻保证用户能升级至最新的 Android 系统。ACLU 的报告中提到目前几千万台 Android 设备中有 2%运行的是最新的系统，大部分设备仍然运行已经有 2 年的版本了，还有一半的 Android 用户运行版本更旧的系统。这种现象让用户的隐私性受到了威胁。

参考链接：http://mobile.qudong.com/2013/0421/142085.shtml

2. 甲骨文 Java 修补 42 个漏洞

甲骨文在本周二（4/16）发布重大修补更新（Critical Patch Update，CPU），放出 Java 7 Update 21，以修补 42 个 Java 安全漏洞。Java 7 Update 21 提供了包含安全性及非安全

性的更新，在 42 个安全更新中有 39 个漏洞允许远程攻击。甲骨文以 CVSS 2.0 (Common Vulnerability Scoring System) 评等漏洞的严重程度，从 0.0 到 10.0 分，10 分代表最危急，其中有 19 个漏洞被评为 10 分。甲骨文强烈建议用户尽快部署 Java 7 Update 21。另外，甲骨文也改变了 Java 7 Update 21 中的安全控制功能，当用户要通过浏览器执行任何 Java 程序时都会跳出警告窗口要求用户确认。信息的内容将会依据 Java 程序的风险等级而有所不同。若是低风险等级的 Java 程序只会出现简单的提醒并允许用户存取更多信息，而高风险等级的程序意味着该程序未经 CA 认证或使用无效认证。

参考链接：http://www.enet.com.cn/article/2013/0418/A20130418275392.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