国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2013 年 01 月 14 日-2013 年 01 月 20 日 **2013 年 第3 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 156 个，其中高危漏洞 32 个、中危漏洞 110 个、低危漏洞 14 个。上述漏洞中，可利用来实施远程攻击的漏洞有 140 个。本周收录的漏洞中，已有 136 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“Microsoft Lync 'User-Agent'跨站脚本漏洞”、“sNews CMS 'id'参数 SQL 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报送了本周收录的全部 156 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。

报送单位或个人	漏洞报送数量	原创漏洞数量
启明星辰	162	0
安天实验室	36	0
绿盟科技	145	0
天融信	53	0
恒安嘉新	15	0
东软	3	0
报送总计	414	0
录入总计	156（去重）	0

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、Google、Rockwell Automation、WordPress 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	81	52%
2	Google	12	8%
3	Rockwell Automation	8	5%
4	WordPress	7	4%
5	Apache	5	3%
6	TYPO3	2	1%
7	Redis	2	1%
8	VideoLAN	1	1%
9	Microsoft	1	1%
10	IBM	1	1%
11	其它	36	23%

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 156 个漏洞。其中应用程序漏洞 100 个，WEB 应用漏洞 18 个，操作系统漏洞 8 个，数据库漏洞 25 个，网络设备漏洞 3 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	100
WEB 应用漏洞	18
网络设备漏洞	3
操作系统漏洞	8
数据库漏洞	25
安全产品漏洞	2

表 3 漏洞按影响类型统计表

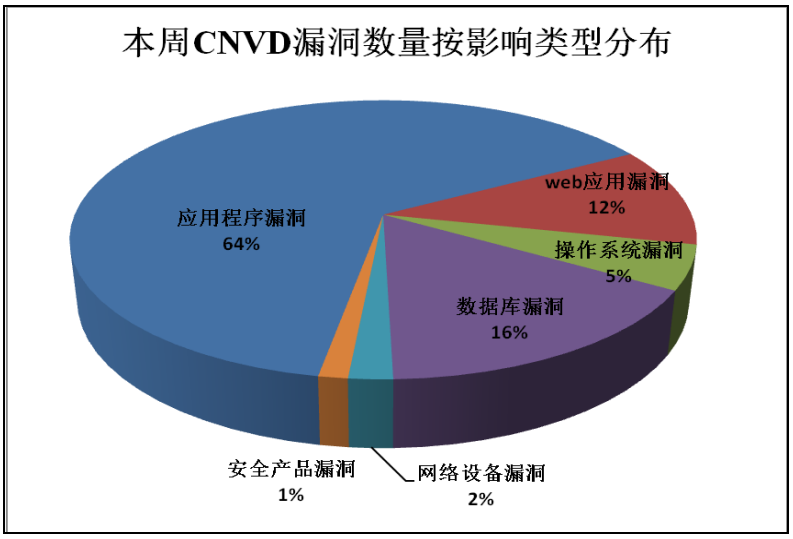

图 1 本周漏洞按影响类型分布

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：TP-LINK TL-WR841N Router 文件包含漏洞、Watson Management Console 目录遍历漏洞、Trimble Infrastructure GNSS Series Receivers 跨站脚本漏洞。上述漏洞的综合评级为“中危”。目前，互联网上已经出现了针对“Watson Management Console 目录遍历漏洞”的攻击代码，相关厂商已经发布了漏洞的修补程序。

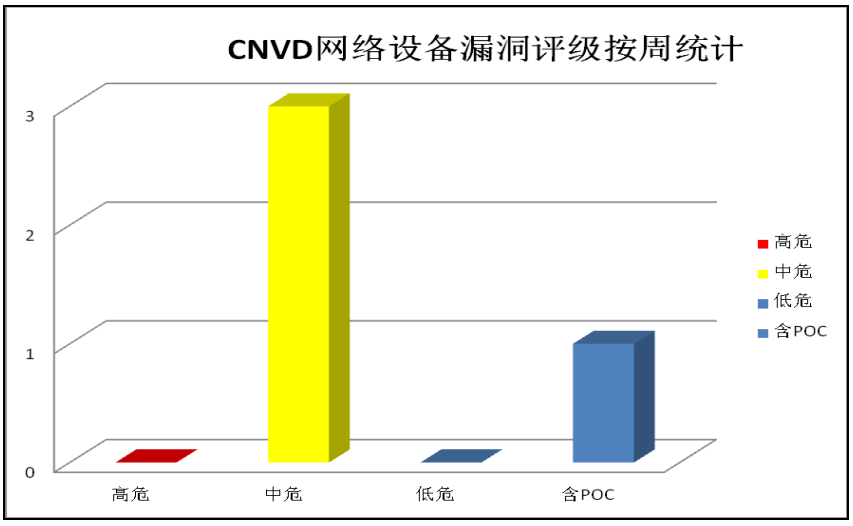

图 2 网络设备漏洞统计

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 Chrome 安全漏洞

Google Chrome 是一款流行的 WEB 浏览器。本周，该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，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：Google Chrome PDF root 处理类型转换漏洞、Google Chrome V8 栈越界访问漏洞、Google Chrome 查询视频越界读漏洞、Google Chrome 共享内存分配整数溢出漏洞、Google Chrome PDF 图像处理越界读漏洞、Google Chrome IPC NUL 结束符缺失漏洞、Google Chrome 文件访问漏洞、Google Chrome 扩展处理路径遍历漏洞等。其中，“Google Chrome PDF root 处理类型转换漏洞”和“Google Chrome V8 栈越界访问漏洞”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-2013-19272

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19267

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19266

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19268

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19271

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19274

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19273

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19275

2、Oracle 产品安全漏洞

Oracle Database 是一款商业性质的大型数据库；Oracle Database Mobile/Lite Server 是 Oralce 公司推出的嵌入式移动数据库系统；Oracle Enterprise Manager 是一款为 ORACLE 融合终结软件提供强化的管理套装；Oracle Java Runtime Environment 是一款为 JAVA 应用程序提供可靠的运行环境的解决方案。本周，Oracle 发布安全更新，修复了上述产品存在的多个安全漏洞。

CNVD 收录的相关漏洞包括：Oracle Database Server 远程漏洞（CNVD-2013-19363）、Oracle Database Mobile/Lite Server 远程漏洞（CNVD-2013-19353、CNVD-2013-19361、CNVD-2013-19357、CNVD-2013-19351、CNVD-2013-19359）、Oracle Enterprise Manager Grid Control 远程漏洞（CNVD-2013-19356）、Oracle Java Runtime Environment 存在未明远程代码执行漏洞（CNVD-2013-19307）等。上述漏洞的综合评级均为“高危”。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-2013-19363

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19353

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19361

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19357

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19356

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19351

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19359

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19307

3、Apache 产品安全漏洞

CouchDB 是一款面向文档的数据库系统；Apache Axis2/C 是一款实现 Web Service 的技术架构。CloudStack 是一个开源的云计算平台。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，执行任意代码。

CNVD 收录的相关漏洞包括：Apache CouchDB 远程代码执行漏洞、Apache CouchDB 目录遍历漏洞、Apache CouchDB 跨站脚本漏洞、Apache Axis2/C SSL 证书验证安全绕过漏洞、Apache CloudStack/Citrix CloudPlatform 日志信息泄露漏洞。其中，厂商已发布了“Apache CouchDB 远程代码执行漏洞、Apache CouchDB 目录遍历漏洞、Apache CouchDB 跨站脚本漏洞”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-2013-19324

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19323

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19325

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19279

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19280

4、Rockwell Automation 产品安全漏洞

Rockwell Automation MicroLogix 是一款用于电子控制和通讯的可编程控制器平台。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可编辑系统配置，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Rockwell Automation ControlLogix 远程拒绝服务漏洞（CNVD-2013-19291、CNVD-2013-19290、CNVD-2013-19288、CNVD-2013-19294、CNVD-2013-19287）、Rockwell Automation ControlLogix 固件上传漏洞、Rockwell Automation ControlLogix 重放漏洞等。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-2013-19291

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19290

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19288

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19294

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19287

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19289

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19292

5、Microsoft Lync 'User-Agent'跨站脚本漏洞

Microsoft Lync 是一款企业整合沟通平台(前身为 Communications Server)。本周，该产品被披露存在跨站脚本漏洞。由于 Microsoft Lync 2010 未能正确过滤“User-Agent Header”参数输入，攻击者利用漏洞可注入恶意脚本代码和 HTML 代码，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/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19306

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-2013-19334	Perl 'Digest::SHA'模块两次释放内存破坏漏洞	高	用户可参考如下厂商提供的安全补丁：https://metacpan.org/diff/release/MSHELOR/Digest-SHA-5.80/MSHELOR/Digest-SHA-5.81
CNVD-2013-19305	Icinga history.cgi 'show_history()'缓冲区溢出漏洞	高	Icinga 1.6.2, 1.7.4 或 1.8.4 已经修复此漏洞，建议用户下载使用：https://www.icinga.org
CNVD-2013-19302	phpshop CMS SQL 注入漏洞	高	暂无
CNVD-2013-19303	CoDeSys 验证绕过漏洞	高	CoDeSys 3.x 已经修复此漏洞，建议用户下载使用：http://www.3s-software.com/index.shtml?en_V23_en
CNVD-2013-19278	phpLiteAdmin 'phpliteadmin.php'远程 PHP 代码注入漏洞	高	暂无
CNVD-2013-19312	WordPress 插件 Simple Login Log SQL 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：http://wordpress.org/extend/plugins/simple-login-log/changelog

CNVD-2013-19283	Ruby multi_xml 任意命令执行漏洞	高	multi_xml gem for Ruby 0.5.2 已经修复此漏洞，建议用户下载使用：https://gist.github.com/d7f6d9f4925f413621aa
CNVD-2013-19286	TYPO3 T3 jQuery 扩展插件 PHP 代码执行漏洞	高	T3 jQuery (t3jquery) Extension for TYPO3 2.2.1 已经修复此漏洞，建议用户下载使用：http://typo3.org/teams/security/security-bulletins/typo3-extensions/

表 3 部分高危漏洞列表

小结：本周，Oralce 发布安全更新，修复其多款产品存在的多个漏洞，其中包括此前被利用于挂马攻击构成较大威胁的 Java 7 远程代码执行漏洞。本周，Google 浏览器被披露存在多个漏洞，同样也可能被用于挂马攻击。此外，可用于工业控制的 Rockwell Automation MicroLogix 平台和用于企业级应用的 CouchDB 数据库被披露存在多个漏洞，攻击者利用漏洞可获得敏感信息，执行任意代码或发起拒绝服务攻击。此外，Microsoft Lync 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、IBM 发布升级程序，修补 Cognos TM1 漏洞

IBM Cognos TM1 中小企业群市场版本是一套一体化的业务分析解决方案，用以有效管理并提升财务绩效。本周，IBM 修补了 Cognos TM1 存在的漏洞。攻击者可以利用漏洞获得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/sites/main/preview/bdgg_preview.htm?tid=29312

本周要闻速递

1. Java 再曝任意代码漏洞

根据 PC World 的报道，波兰安全探索的研究人员两个安全漏洞，允许攻击者在用户机器上运行任意代码。这两个漏洞是在过去的几个星期确定的，因此进一步的攻击也是可能的。希望甲骨文有时间在漏洞被恶意运用前解决问题。比较光明的一面是，Java 7 Update 11 会提示用户确认是否运行一个 applet 小程序，这稍微增加了运行攻击代码的难度。但不幸的是，大多数的用户都只会盲目地点“是”，所以这很大程度上也不能提供很好的保护。"Krebs on Security"已经有了一篇如何在 Windows 和 Mac 上不同的浏览

器里禁用 Java 的文章，不了解的用户们可以尝试一下。

参考链接：http://mobile.163.com/13/0121/08/8LNSPP9V0011665S.html

2. Exynos 漏洞补丁优化 4G 性能

一个月前三星的 Exynos 处理器被曝光存在安全漏洞，本月开始三星从英国开始陆续在全球推送最新的安全补丁，而今天美国运营商 Verizon 正式宣布将为旗下的 Note II 推送名为 LL4 的补丁，除了修复以上漏洞以外还对 4G LTE 等部分进行了优化和加强。目前这份从 LJB 到 LL4 的升级包已经确定能够试用于所有使用 Jelly Bean 系统的手机型号。

参考链接：http://www.enet.com.cn/article/2013/0120/A20130120232333.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