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 07 日-2013 年 01 月 13 日 **2013 年 第 2 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 163 个，其中高危漏洞 78 个、中危漏洞 69 个、低危漏洞 16 个。上述漏洞中，可利用来实施远程攻击的漏洞有 153 个。本周收录的漏洞中，已有 122 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“Java 7 存在远程代码执行漏洞”、“Samsung Kies 远程缓冲区溢出漏洞”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 163 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、安天实验室等单位报送数量较多。此外，奇虎公司、High-Tech Bridge Security Research Lab 和个人报送者向 CNVD 提交了 6 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	149	0
安天实验室	100	0
绿盟科技	92	0
天融信	57	0
恒安嘉新	43	0
东软	4	0
High-Tech Bridge Security Research Lab	4	4
奇虎 360	1	1
个人报送者	1	1

报送总计	451	6
录入总计	163（去重）	6

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Mozilla、Adobe、Microsoft、Google 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	Mozilla	28	17%
2	Adobe	28	17%
3	Microsoft	13	8%
4	Google	12	7%
5	Sybase	9	6%
6	Red Hat	4	2%
7	Wordpress	4	2%
8	Joomla!	3	2%
9	Cisco	2	1%
10	Linux	1	1%
11	其它	59	37%

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 163 个漏洞。其中应用程序漏洞 123 个，WEB 应用漏洞 20 个，操作系统漏洞 10 个，网络设备漏洞 1 个，数据库漏洞 9 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	123
WEB 应用漏洞	20
网络设备漏洞	1
操作系统漏洞	10
数据库漏洞	9
安全产品漏洞	0

表 3 漏洞按影响类型统计表

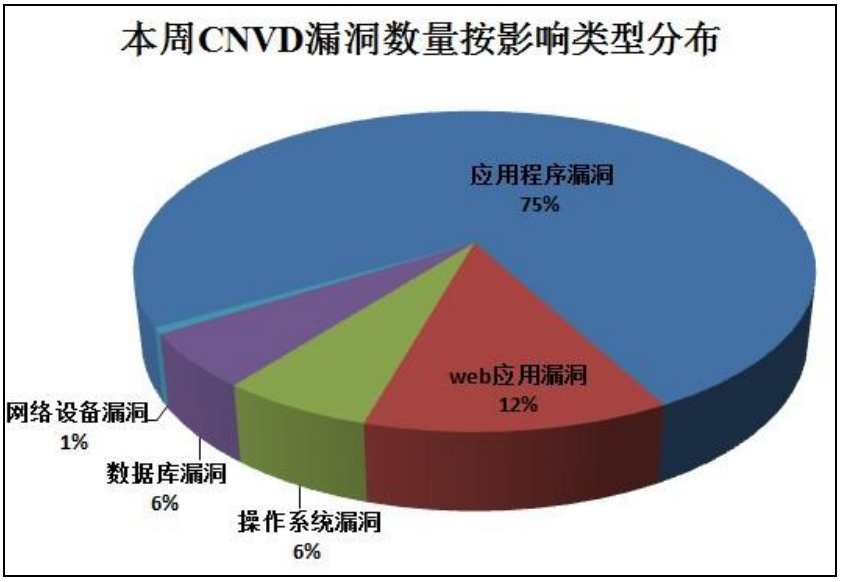

图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 1 个网络设备漏洞：Cisco Linksys Routers 未验证 root 访问漏洞，该漏洞的综合评级为“高危”。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。

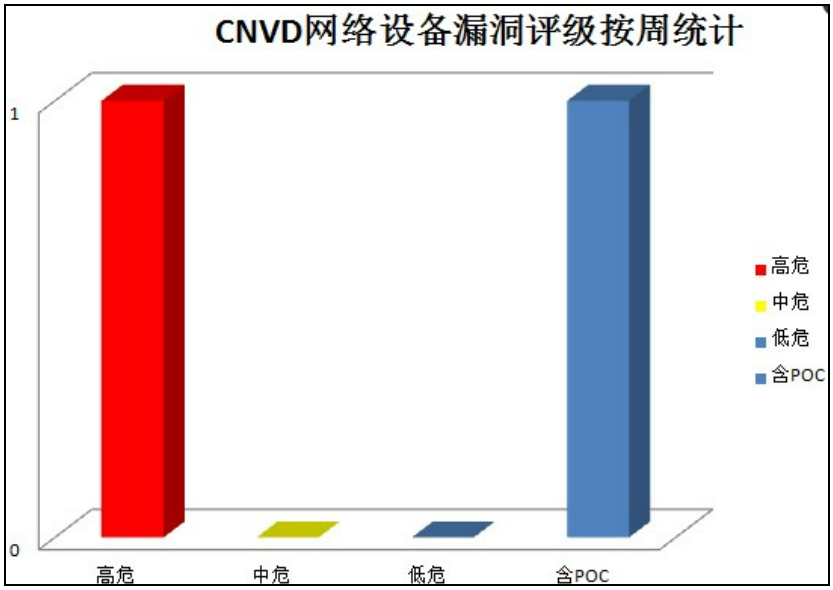

图 2 网络设备漏洞统计

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

本周，微软发布了安全更新，修复了 Microsoft Windows，Office，.NET Framework，开发工具和 Server 软件中存在的 12 个安全漏洞。其中，2 项更新为“严重”级别（微软定义的威胁最高级别），其余 5 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、绕过安全认证或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Microsoft XML Core Services XSLT 解析漏洞、Microsoft XML Core Services 整数溢出漏洞、Microsoft Windows Print Spooler 打印作业处理漏洞、Microsoft Windows SSLv3/TLS 协议安全功能绕过漏洞、Microsoft System Center Operations Manager 跨站脚本漏洞（CNVD-2013-19143）、Microsoft Windows win32k.sys 不正确消息处理漏洞、Microsoft .NET Framework 绘图信息泄露漏洞、Microsoft .NET Framework 双重构造漏洞等。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/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19130

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19132

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19153

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19143

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19147

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19148

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19152

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19129

2、Adobe 产品安全漏洞

本周，Adobe 发布了安全更新，修复了 Adobe Flash Player、Acrobat、Reader 产品存在的 28 个安全漏洞，相关产品运行在 Windows、Macintosh、Android、Linux 多个平台。利用上述漏洞，攻击者可以构建恶意文件，诱使用户解析，以应用程序上下文执行任意代码，严重的可危及用户操作系统主机安全。

CNVD 收录的相关漏洞包括：Adobe Acrobat/Reader 内存破坏漏洞（CNVD-2013-19182）、Adobe Acrobat/Reader 堆溢出漏洞（CNVD-2013-19188）、Adobe Acrobat/Reader 缓冲区溢出漏洞（CNVD-2013-19192）、Adobe Acrobat/Reader 逻辑错误代码执行漏洞（CNVD-2013-19193）、Adobe Acrobat/Reader 整数溢出漏洞（CNVD-2013-19196）、Adobe Acrobat/Reader 栈溢出漏洞（CNVD-2013-19197）、Adobe Acrobat/Reader 逻辑错误代码执行漏洞（CNVD-2013-19199）、Adobe Acrobat/Reader 安全绕过漏洞（CNVD-2013-19210）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-2013-19210
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19199
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19197
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19196
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19193
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19193
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19188
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19182

3、Mozilla 产品安全漏洞

Mozilla Firefox/SeaMonkey/Thunderbird 是 Mozilla 所发布的 WEB 浏览器/新闻组客户端/邮件客户端。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：Mozilla Firefox/Thunderbird/SeaMonkey nsHTMLEditRules 内存错误引用漏洞、Mozilla Firefox/Thunderbird/SeaMonkey 内存破坏漏洞（CNVD-2013-19183）、Mozilla Firefox/Thunderbird/SeaMonkey AutoWrapperChanger 代码执行漏洞、Mozilla Firefox/Thunderbird/SeaMonkey serializeToStream 内存错误引用漏洞、Mozilla Firefox/Thunderbird/SeaMonkey nsSVGPathElement::GetPathLengthScale 越界读漏洞、Mozilla Firefox/Thunderbird/SeaMonkey ListenerManager 内存错误引用漏洞、Mozilla Firefox/Thunderbird/SeaMonkey Vibrate 内存错误引用漏洞、Mozilla Firefox/Thunderbird/SeaMonkey Javascript 代理对象内存错误引用漏洞等。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-2013-19179
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19183
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19180
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19157
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19165
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19166
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19167
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19168

4、Sybase 产品安全漏洞

Sybase Adaptive Server Enterprise 是一款关系数据库管理软件。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可绕过安全限制，提升权限，获取敏感信息或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Sybase Adaptive Server Enterprise 安全绕过漏洞、Sybase Adaptive Server Enterprise 堆缓冲区溢出漏洞、Sybase Adaptive Server Enterprise 缓冲区溢出漏洞、Sybase Adaptive Server Enterprise ASE 插件安全绕过漏洞、Sybase Adaptive Server Enterprise SQL 注入漏洞、Sybase Adaptive Server Enterprise 信息泄露漏洞、Sybase Adaptive Server Enterprise 拒绝服务漏洞、Sybase Adaptive Server Enterprise 文件破坏漏洞等。其中，“Sybase Adaptive Server Enterprise 安全绕过漏洞”和“Sybase Adaptive Server Enterprise 堆缓冲区溢出漏洞”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-2013-19131

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19140

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19137

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19133

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19134

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19135

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19138

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19141

5、Java 7 存在远程代码执行零日漏洞

Oracle Java 7（1.7, 1.7.0）是 Oracle 公司发布的为 Java 应用程序提供运行环境的产品，相关产品包括：Java SE 7、JDK 7、JRE 7，并支持当前主流浏览器插件扩展。本周，该产品被披露存在一个综合评级为“高危”的远程代码执行漏洞。由于 Java 7 对代码执行权限机制存在处理异常，一些未经信任的 Java 程序通过调用 setSecurityManager（）函数可以实现权限提升，进而执行任意代码。攻击者利用漏洞通常可以构建挂马页面，诱使用户解析，在用户主机上执行木马程序，取得用户主机操作系统的控制权。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-2013-19216

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-2013-19189	Ruby on Rails 存在多个漏洞	高	Ruby on Rails 3.2.11, 3.1.10, 3.0.19, 2.3.15 已经修复此漏洞，建议用户下载

			使用： http://www.rubyonrails.com/
CNVD-2013-19117	Firefox Foxit Reader 插件 'npFoxitReaderPlugin.dll'栈缓冲区溢出漏洞	高	暂无
CNVD-2013-19154	EMC NetWorker 'nsrindexd' RPC 服务缓冲区溢出漏洞	高	EMC NetWorker 7.6.5，8.0.0.6 和 8.0.1 及之后版本已经修复此漏洞，建议用户下载使用： http://www.emc.com
CNVD-2013-19126	E SMS 脚本存在多个 SQL 注入漏洞	高	暂无
CNVD-2013-19108	Coppermine Photo Gallery 'index.php'脚本 SQL 注入漏洞	高	暂无
CNVD-2013-19109	pfSense 命令执行漏洞	高	pfSense 2.0.2 版本已修复此漏洞，建议用户下载使用：http://www.pfsense.org/
CNVD-2013-19105	ICEstate SQL 注入漏洞	高	暂无
CNVD-2013-19104	php MBB SQL 注入漏洞	高	暂无
CNVD-2013-19139	Website Baker Concert Calendar Add-on 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://addons.websitebaker2.org/pages/en/browse-add-ons.php?id=0E8BC37
CNVD-2013-19113	VANA CMS 'index.php'脚本 SQL 注入漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，微软和 Adobe 均发布了月度例行安全更新，修复其多个产品存在的多个漏洞，相关操作系统、浏览器软件以及应用软件用户需及时更新。Mozilla 多个产品和 Sybase Adaptive Server Enterprise 也被披露存在多个漏洞，攻击者利用漏洞可使应用程序崩溃或执行任意代码。

本周，CNVD 收录了 Java 7 存在的一个远程代码执行零日漏洞，目前互联网上已经出现了针对该漏洞的网页挂马攻击，在漏洞补丁发布之前，建议用户暂时禁用 Java 运行环境功能或浏览器插件，同时不要随意打开不明来源的页面，，。

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、Red Hat 发布升级程序，修补多款产品漏洞

Red Hat 是一款基于 linux 内核的发行版本。OpenShift 是 redhat 推出的开发框架。SquirrelMail 是一款基于 PHP 的 WEB 邮件服务程序。本周，Red Hat 修补了多款产品存在的漏洞。攻击者可以利用漏洞重定向用户到任意 WEB 页、执行任意命令，或使系统拒绝服务。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=28811

http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=28791

http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=28812

http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=28771

本周要闻速递

1. Oracle 发布 Java7 补丁修补安全漏洞

在宣布修正 Java 严重 0day 漏洞的消息发出一天后，甲骨文公布了 Java SE 7u11 更新，它包含了安全漏洞 CVE-2013-0422 的补丁，同时也改变了默认的 Java 安全级别设置，任何未签名的 Java Applet 或 Java Web Start 应用程序运行时总是会被提示，这样可以防止恶意应用被下载，对用户来说这可能会带来的影响是需要多确认一下。

参考链接：http://digi.tech.qq.com/a/20130114/000654.htm

2. 微软发布 2013 年首批补丁 暂未修复 IE 漏洞

北京时间 1 月 9 日凌晨，微软发布 2013 年首次安全补丁更新，涉及 Windows、Office、开发者工具、Server 软件等 12 个漏洞，但尚未修复 2012 年底曝出的 IE 浏览器 0day 漏洞(CVE-2012-4792)。值得关注的是，Win8 以及 Win8 RT(平板电脑)用户也需要打补丁，修复 Windows 内核漏洞、SSL/TLS 漏洞以及 XML 服务。此外，系统常用组件.NET Framework 以及微软云服务 System Center Operations Manager(SCOM)都在此次漏洞修复之列。

参考链接：

http://www.chinadaily.com.cn/micro-reading/dzh/2013-01-10/content_7993740.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