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 25 日-2013 年 03 月 31 日 **2013 年第 13 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 160 个，其中高危漏洞 50 个、中危漏洞 96 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 148 个。本周收录的漏洞中，已有 109 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“Clip Share 'gid'参数 SQL 注入漏洞”、“PsychoStats 'awards.php'脚本 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及个人报送了本周收录的全部 160 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、安天实验室和天融信等单位报送数量较多。此外，奇虎公司、High-Tech Bridge Security Research Lab 以及个人报送者向 CNVD 提交了 7 个原创漏洞。本周，CNVD 补充收录了此前中国电信系统集成公司报送的涉及某国产 CMS 软件产品的两个漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
启明星辰	110	0
绿盟科技	88	0
安天实验室	49	0
天融信	50	0
恒安嘉新	17	0
中国电信系统集成公司	2	2
High-Tech Bridge	2	2

Security Research Lab		
奇虎 360	2	2
个人	3	3
报送总计	323	9
录入总计	160（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 IBM、Google、Cisco、Moodle 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	IBM	21	13%
2	Google	12	8%
3	Cisco	9	6%
4	Moodle	8	5%
5	Microsoft	7	4%
6	Siemens	5	3%
7	Drupal	4	3%
8	Linux	3	2%
9	ISC	2	1%
10	Novell	2	1%
11	其它	87	54%

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 160 个漏洞。其中应用程序漏洞 107 个，WEB 应用漏洞 33 个，操作系统漏洞 12 个，网络设备漏洞 5 个，数据库漏洞 3 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	107
WEB 应用漏洞	33
网络设备漏洞	5
操作系统漏洞	12
数据库漏洞	3
安全产品漏洞	0

表 3 漏洞按影响类型统计表

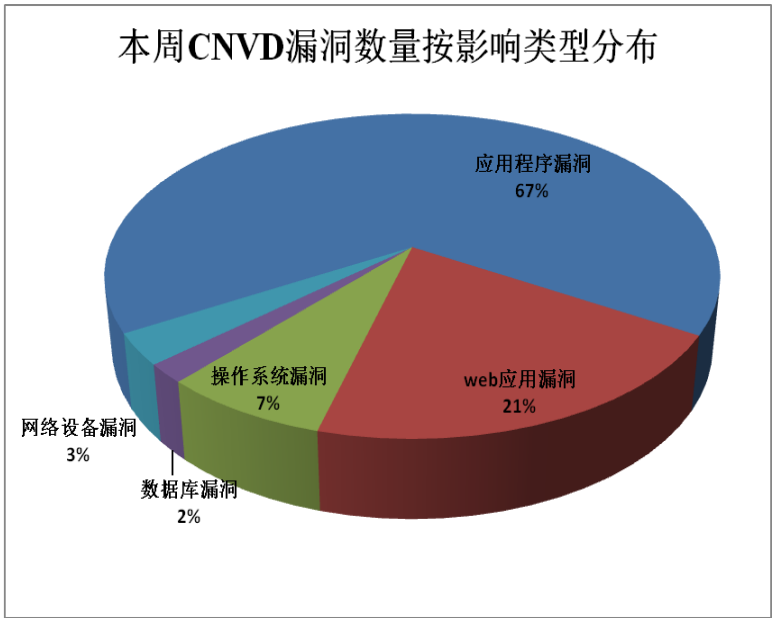

图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 5 个网络设备漏洞：Polycom HDX 系列 SQL 注入漏洞（CNVD-2013-21178）、Rosewill RSVA11001/RSVA12001 NTP 主机操作远程命令执行漏洞、Cisco IOS XR TE 报文拒绝服务漏洞、HP ProCurve Switches 跨站请求伪造漏洞、PowerHawk 6320 Smart Meter 信息泄露漏洞。其中“Polycom HDX 系列 SQL 注入漏洞（CNVD-2013-21178）、Rosewill RSVA11001/RSVA12001 NTP 主机操作远程命令执行漏洞”的综合评级均为“高危”，相关厂商已经发布了漏洞修补程序。

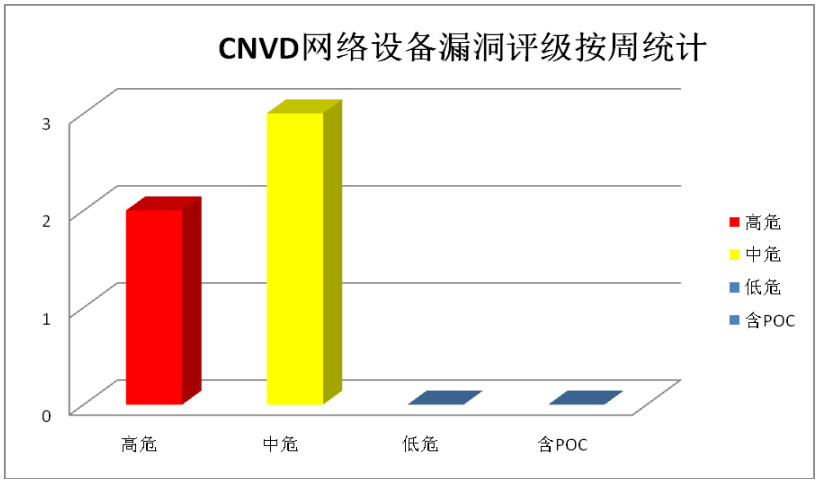

图 2 网络设备漏洞统计

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、Microsoft 产品安全漏洞

Microsoft Internet Explorer 是一款网页浏览器；Microsoft Windows 是一款操作系统。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可绕过安全限制，提升权限，发起拒绝服务攻击或远程执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer 存在未明远程代码执行漏洞（CNVD-2013-21183、CNVD-2013-21186）、Microsoft Internet Explorer 沙盒保护机制内存破坏漏洞、Microsoft Windows ASLR 安全绕过漏洞、Microsoft Windows 存在未明本地权限提升漏洞、Microsoft Windows 安全绕过漏洞等。上述漏洞的综合评级均为“高危”。目前，厂商尚未发布上述漏洞的修补程序。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-2013-21183
http://www.cnvd.org.cn/flaw/show/CNVD-2013-21186
http://www.cnvd.org.cn/flaw/show/CNVD-2013-21187
http://www.cnvd.org.cn/flaw/show/CNVD-2013-21191
http://www.cnvd.org.cn/flaw/show/CNVD-2013-21175
http://www.cnvd.org.cn/flaw/show/CNVD-2013-21177

2、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，攻击者利用漏洞可绕过安全限制，发起拒绝服务攻击或远程执行任意代码。

CNVD 收录的相关漏洞包括：Google Chrome 内存错误引用漏洞（CNVD-2013-21283、CNVD-2013-21286、CNVD-2013-21289）、Google Chrome 存在漏洞（CNVD-2013-21290、CNVD-2013-21291、CNVD-2013-21295）、Google Chrome 文件权限漏洞（CNVD-2013-21293）、Google Chrome 越界读取漏洞（CNVD-2013-21284）等。上述漏洞中“Google Chrome 内存错误引用漏洞（CNVD-2013-21283）、Google Chrome 存在漏洞（CNVD-2013-21290）、Google Chrome 文件权限漏洞（CNVD-2013-21293）”的综合评级均为“高危”。谷歌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-2013-21283
http://www.cnvd.org.cn/flaw/show/CNVD-2013-21290
http://www.cnvd.org.cn/flaw/show/CNVD-2013-21293
http://www.cnvd.org.cn/flaw/show/CNVD-2013-21286
http://www.cnvd.org.cn/flaw/show/CNVD-2013-21289
http://www.cnvd.org.cn/flaw/show/CNVD-2013-21291

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21295

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21284

3、IBM 产品安全漏洞

IBM Lotus Notes 是一款桌面客户端软件，为用户提供了单点访问功能；IBM Rational Policy Tester 是一款为了自动化测试网页内容是否符合标准化规范而推出的解决方案；IBM Rational AppScan 是一款 Web 应用安全测试工具；IBM Lotus Domino 服务器是一款基于 WEB 合作的应用程序架构；IBM Rational Team Concert for System z 是企业级跨平台合作开发环境；IBM Sterling B2B Integrator 集成了重要的 B2B 流程、交易和关系，支持与不同的合作伙伴社区之间实现复杂的 B2B 流程的安全集成。本周，上述 IBM 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，提升权限，使应用程序崩溃，执行任意代码。

CNVD 收录的相关漏洞包括：IBM Lotus Notes Autonomy KeyView 文件解析程序缓冲区溢出漏洞、多个 IBM 产品本地权限提升漏洞、IBM Lotus Domino 验证绕过漏洞、IBM Rational Team Concert for System z 缓冲区溢出漏洞、IBM Lotus Domino 拒绝服务漏洞、IBM Sterling B2B Integrator 不正确输入验证漏洞、IBM Sterling B2B Integrator 信息泄露漏洞（CNVD-2013-21181、CNVD-2013-21185）等。上述漏洞中“IBM Lotus Notes Autonomy KeyView 文件解析程序缓冲区溢出漏洞、多个 IBM 产品本地权限提升漏洞、IBM Lotus Domino 验证绕过漏洞、IBM Rational Team Concert for System z 缓冲区溢出漏洞”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-2013-21202

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21221

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21159

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21165

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21156

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21184

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21181

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21185

4、Siemens 工控相关产品安全漏洞

Siemens CP 1616 和 1604 是工业以太网通讯卡，用于连接桌面工作站和 PCI-104 系统至 PROFINET 接口；Siemens SIMATIC WinCC 是监测控制和数据采集 SCADA 及人机界面 HMI 系统；Siemens SIMATIC PCS 是流程控制系统。本周，上述西门子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，发起拒绝服务攻击或远程执行执行任意代码。

CNVD 收录的相关漏洞包括： Siemens CP 1616 和 CP 1604 访问安全绕过漏洞、Siemens SIMATIC WinCC 和 PCS 7 存在信息泄露、目录穿越、缓冲区溢出等多个漏洞、

Siemens WinCC CCEServer 缓冲区溢出漏洞、Siemens WinCC RegReader ActiveX 控件缓冲区溢出漏洞。其中，“Siemens CP 1616 和 CP 1604 访问安全绕过漏洞、Siemens SIMATIC WinCC 和 PCS 7 存在信息泄露、目录穿越、缓冲区溢出等多个漏洞”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-2013-21278

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21189

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21180

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21161

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21157

5、ClipShare 'gid'参数 SQL 注入漏洞

ClipShare 是一款视频共享应用程序。本周，该产品被披露存在一个综合评级为“高危”的 SQL 注入漏洞。由于 ClipShare gmembers.php 脚本未能正确过滤用户提交的'gid'参数，远程攻击者利用漏洞可进行 SQL 注入攻击，获得数据库信息。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-2013-21236

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-2013-21268	EMC Smarts Network Configuration Manager 验证绕过漏洞	高	厂商已经修复此漏洞，建议用户下载更新：https://support.emc.com/products/6259_Smarts-Network-Configuration-Manager/Downloads/
CNVD-2013-21275	MongoDB engine_spidermonkey.cpp nativeHelper.apply 函数任意代码执行漏洞	高	MongoDB 2.4.1 已经修复此漏洞，建议用户下载更新：http://www.mongodb.org
CNVD-2013-21266	Rosewill RSVA11001/RSVA12001 NTP 主机操作远程命令执行漏洞	高	暂无
CNVD-2013-21277	RubyGems 'thumbshooter'远程命令执行漏洞	高	暂无
CNVD-2013-21280	SynConnect 'loginid'参数 SQL 注入漏洞	高	用户可联系厂商获得最新版本的应用程序：http://www.synchroweb.com/prod_syn.php

CNVD-2013-21233	Airtime 任意 shell 命令执行漏洞	高	Airtime 2.3.1 已经修复此漏洞，建议用户下载更新：https://github.com/sourcefabric/Airtime/blob/master/changelog
CNVD-2013-21236	ClipShare 'gid'参数 SQL 注入漏洞	高	暂无
CNVD-2013-21213	Free Hosting Manager 存在多个 SQL 注入漏洞	高	暂无
CNVD-2013-21169	CA SiteMinder 产品 SAML 声明签名验证漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID={53E50CBD-6F6A-4B3A-85FF-36E44AB
CNVD-2013-21241	IconCool MP3 WAV Converter '.mp3'文件栈缓冲区溢出漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，Google Chrome、微软 IE 浏览器以及 windows 系统被披露存在多个安全漏洞，攻击者利用漏洞有可能发起大规模网页挂马攻击，建议服务器和桌面操作系统用户及时更新。可用于工业控制的多款西门子产品以及用于企业业务管理的 IBM 多款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，提升权限，使应用程序崩溃，远程执行任意代码。此外，ClipShare 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、ISC 发布升级程序，修补 BIND 安全漏洞

ISC BIND 是一款 DNS 协议的实现。本周，ISC 发布升级程序，修补了 BIND 存在的漏洞。远程攻击者可利用漏洞进行拒绝服务攻击。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/33087

http://www.cnvd.org.cn/patchInfo/show/33072

本周要闻速递

1. 苹果 iOS 有漏洞或致 iMessage 意外崩溃

来自国外科技网站 appleinsider 的消息称，最近一些苹果开发人员的 iMessage 应用遭到了攻击，向 ios 设备发送 iMessage 信息发现，iMessage 中的容量和速率等都没有限制。因为苹果不限制 iMessage 信息的发送间隔时间，所以攻击者很容易在短时间内发送上千条 iMessage 信息，受攻击 iOS 设备则会不停收到信息。iOS 设备不能及时处理信息，还会导致崩溃。万一受到这种攻击，用户可以关闭 iMessage 服务，但目前还有有什么可以预防的措施，苹果也没有提出解决方案。

参考链接：http://iphone.265g.com/news/131982.html

2. 支付宝被曝重大漏洞

有网友在微博上爆出，使用谷歌搜索输入“site：shenghuo.alipay.com 转账付款”即可看到各种转账信息，包括账户姓名、手机号等个人信息（如下图，网络图片）。昨日凌晨，支付宝官方微博回应称，极少量用户将自己付款结果页面分享到公共区域，造成某些搜索引擎可抓取。记者在搜索到的信息中随意选出若干条进行核实，结果发现，几乎所有的信息都可以对得上号。对此，支付宝方面回应，目前搜索到的只是网页快照，他们正在与搜索运营商沟通，“google 在处理过程中还有一些细则要遵循，因此需要一定的时间，请大家耐心等待。”

参考链接：http://news.sina.com.cn/c/2013-03-29/085026677602.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