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 04 日-2013 年 03 月 10 日 **2013 年第 10 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**低**。

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 113 个，其中高危漏洞 30 个、中危漏洞 70 个、低危漏洞 13 个。上述漏洞中，可利用来实施远程攻击的漏洞有 107 个。本周收录的漏洞中，已有 80 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“Sami FTP Server 'LIST'命令缓冲区溢出漏洞”、“Hiverr 存在多个 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 7 家成员单位和多个合作伙伴报送了本周收录的全部 113 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、恒安嘉新等单位报送数量较多。此外，奇虎公司、CNCERT 辽宁分中心和 High-Tech Bridge Security Research Lab 以及个人报送者向 CNVD 提交了 10 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	151	0
安天实验室	37	0
天融信	32	0
恒安嘉新	46	0
东软	4	0
High-Tech Bridge Security Research L	4	4
奇虎 360	3	3

CNCERT 辽宁分中心	2	2
个人报送者	1	1
报送总计	343	10
录入总计	113（去重）	10

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Wireshark、Google、IBM、WordPress、Apache 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	Wireshark	13	12%
2	Google	10	9%
3	IBM	10	9%
4	WordPress	7	6%
5	Apache	6	5%
6	RubyGems	6	5%
7	Oracle	4	4%
8	Cisco	3	3%
9	HP	1	1%
10	Linux	1	1%
11	其它	52	45%

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 113 个漏洞。其中应用程序漏洞 82 个，WEB 应用漏洞 21 个，操作系统漏洞 1 个，网络设备漏洞 9 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	82
WEB 应用漏洞	21
网络设备漏洞	9
操作系统漏洞	1
安全产品漏洞	0
数据库漏洞	0

表 3 漏洞按影响类型统计表

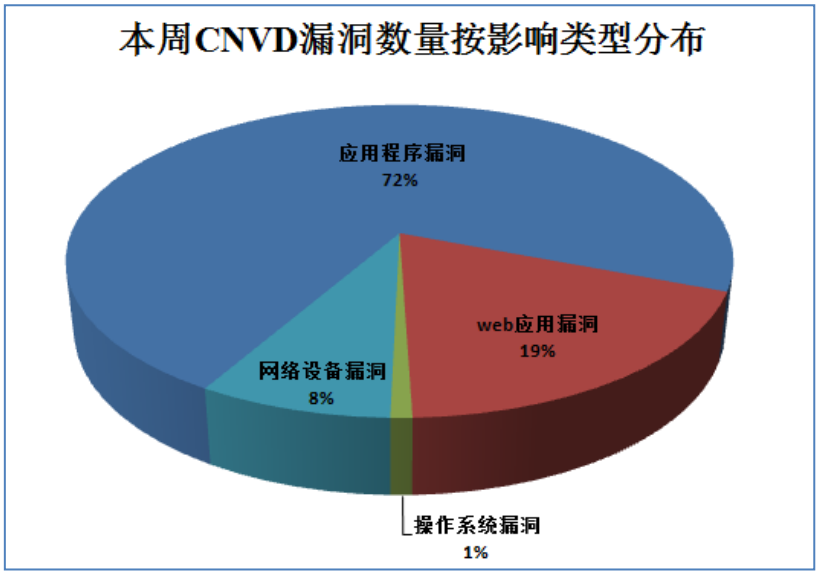

图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 9 个网络设备和移动智能终端的漏洞：Cisco Aironet Access Points 远程拒绝服务漏洞、D-Link DIR-645 路由器远程验证漏洞、Xerox 多个设备多协议未授权访问漏洞、Xerox Phaser 7800 多协议未授权访问漏洞、Foscam 路径遍历漏洞、D-Link DSL-2740B 远程验证绕过漏洞、Samsung Galaxy S3 锁屏安全绕过漏洞、Citrix Access Gateway 存在未明安全绕过漏洞、Cisco Small Business Switches 拒绝服务漏洞。其中，“Citrix Access Gateway 存在未明安全绕过漏洞”的综合评级为“高危”。

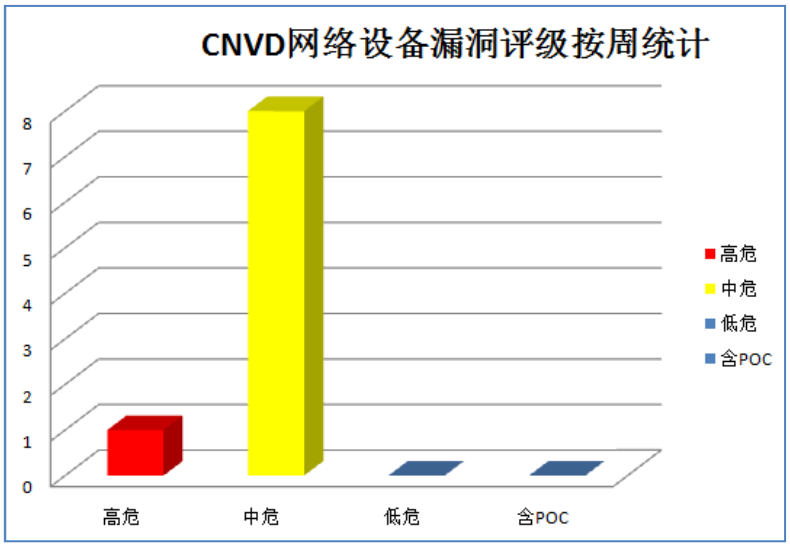

图 2 网络设备漏洞统计

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，攻击者利用漏洞可导致应用程序崩溃，执行任意代码。

CNVD 收录的相关漏洞包括：Google Chrome frame-loader 内存错误引用漏洞、Google Chrome 浏览器导航内存错误引用漏洞、Google Chrome Web Audio 内存破坏漏洞、Google Chrome SVG 动画媒介内存错误引用漏洞、Google Chrome IndexedDB 内存破坏漏洞、Google Chrome 媒体线程处理竞争条件漏洞、Google Chrome 扩展存在漏洞、Google Chrome 目录遍历漏洞等。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-2013-20646

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20647

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20648

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20650

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20652

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20654

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20655

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20658

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；Oracle Auto Service Request 是一种安全的、客户可安装的支持功能，可自动生成特定硬件故障的服务请求。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 Java Runtime Environment 存在多个未明远程代码执行漏洞（CNVD-2013-20641）、Oracle Java Runtime Environment 远程代码执行漏洞（CNVD-2013-20429）、Oracle Auto Service Request 不安全临时文件创建漏洞、Oracle Java SE 远程代码执行漏洞。其中，“Oracle Java SE 远程代码执行漏洞”和“Oracle Java Runtime Environment 远程代码执行漏洞（CNVD-2013-20429）”的综合评级均为“高危”。厂商已发布了“Oracle Java SE 远程代码执行漏洞”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-2013-20641

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20482

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20444

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20429

3、Cisco 产品安全漏洞

Cisco Aironet Access Points 是思科公司推出的无线接入点和网桥设备；Cisco Security Monitoring, Analysis, and Response System 是一款高性能、可扩展的威胁管理、监控和防御设备系列。本周，上述 Cisco 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，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco Aironet Access Points 远程拒绝服务漏洞、Cisco Security Monitoring, Analysis, Response System (MARS)信息泄露漏洞。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-2013-20424

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20642

4、IBM 产品安全漏洞

IBM Cognos Business Intelligence 是一款基于 Web 的集中式商务智能套件；IBM Rational Developer for System z 为 IBM 操作系统上运行的应用程序提供现代化的应用程序开发工具；IBM Tivoli Application Dependency Discovery Manager 提供业务应用和支持基础设施的完整详细的应用映射关系，包括跨层依赖性、运行时配置值和完全的变更历史记录。本周，上述 IBM 产品被披露存在多个安全漏洞，攻击者利用漏洞可注入任意 Web 脚本或 HTML，劫持用户通信，远程执行任意代码。

CNVD 收录的相关漏洞包括：IBM Cognos Business Intelligence 远程命令注入漏洞、IBM Rational Developer for System z 存在未明任意命令执行漏洞、IBM Cognos Business Intelligence XPath 注入漏洞（CNVD-2013-20638）、IBM Cognos Business Intelligence 存在未明跨站脚本漏洞（CNVD-2013-20639）、IBM Tivoli Application Dependency Discovery Manager 中间人攻击漏洞、IBM Cognos Business Intelligence 存在未明跨站脚本漏洞（CNVD-2013-20488）、IBM Cognos Business Intelligence 存在未明跨站脚本漏洞（CNVD-2013-20491）、IBM WebSphere Commerce Web 服务框架拒绝服务漏洞等。其中，“IBM Cognos Business Intelligence 远程命令注入漏洞”和“IBM Rational Developer for System z 存在未明任意命令执行漏洞”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-2013-20472

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20447

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20638

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20639

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20476

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20488

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20491

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20457

5、Sami FTP Server 'LIST'命令缓冲区溢出漏洞

KarjaSoft Sami FTP Server 是一款 FTP 服务程序。本周，该产品被披露存在一个综合评级为“高危”的缓冲区溢出漏洞。攻击者利用漏洞可执行任意代码。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-2013-20430

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-2013-20644	CosCMS 'index.php'远程命令注入漏洞	高	CosCms 1.822 已经修复此漏洞，建议用户下载更新：http://www.coscms.org/blog/view/4/Version-1.822
CNVD-2013-20645	TYPO3 'Extbase' SQL 注入漏洞	高	TYPO3 4.5.24, 4.6.17, 4.7.9 或 6.0.3 已经修复此漏洞，建议用户下载更新：http://typo3.org
CNVD-2013-20440	PloggerGallery SQL 注入漏洞	高	暂无
CNVD-2013-20480	OpenAFS 缓冲区溢出漏洞	高	OpenAFS servers 1.6.2 已经修复此漏洞，建议用户下载使用：http://www.openafs.org/release/latest.html OpenAFS servers 1.4.14.1 可采用如下厂商提供的补丁程序：http://www.openafs.org/pages/security/openafs-sa-2013-002-1_4_14_1.patch
CNVD-2013-20643	Citrix Access Gateway 存在未明安全绕过漏洞	高	用户可参考如下厂商提供的补丁以修复此漏洞：http://www.citrix.com/downloads/netscaler-access-gateway/product-software/access-gateway-504.html

CNVD-2013-20461	nconf handle_item.php SQL 注入漏洞	高	暂无
CNVD-2013-20484	mnoGoSearch 任意文件读取漏洞	高	最新版本已修复此漏洞，建议用户下载使用： http://www.mnogosearch.org/
CNVD-2013-20467	Hiverr 存在多个 SQL 注入漏洞	高	暂无
CNVD-2013-20469	Ruby extlib 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/extlib

表 3 部分高危漏洞列表

小结：本周， Google 和 Oracle 的多款产品被披露存在多个漏洞，攻击者利用漏洞可执行任意代码，影响涉及服务器及桌面终端用户，有可能诱发大规模的网页挂马或垃圾邮件攻击。Cisco 和 IBM 的多款产品也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，劫持用户通信，发起拒绝服务攻击，对企业用户构成较大威胁。此外，KarjaSoft Sami FTP Server 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、Linux 发布升级程序，修补 Kernel 漏洞

Linux 是一款开源的操作系统。本周，Linuxt 修补了 Kernel 存在的漏洞。攻击者可以利用漏洞导致系统破坏，造成拒绝服务攻击。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/sites/main/preview/bdgg_preview.htm?tid=32632

本周要闻速递

1. 苹果修复 App Store 安全漏洞

去年谷歌的安全性工程师 Elie Bursztein 曾经曝光苹果应用商店（App Store）出现了安全漏洞，通过这一漏洞黑客可以窃取用户密码等私密信息，从而进行不法活动。近日，根据国外媒体的报道，历经半年时间，苹果终于修复了这一漏洞。Elie Bursztein 发现的这个安全漏洞，用户一直在使用非加密 HTTP 协议与应用商店之间通信，也就是说用户在访问苹果应用商店的时候有可能遭到黑客窃取私密信息，比如密码等等。不过这个漏洞有个前提条件，就是用户与黑客必须处在相同的 WIFI 环境下。也就是说当你拿

着 iPad 或者 iPhone 在公共场所使用 WIFI 的时候就有可能被人拿到密码，并且恶意购买一些你完全不需要的程序。从去年七月份发现这个漏洞以后，直到今天苹果才修复，长达半年时间里没有给出明确解决方法，以至于在公共场所使用苹果设备的时候人心惶惶。国外媒体曾经针对该情况采访苹果，但是他们的发言人拒绝回答。

参考链接：http://it.sohu.com/20130311/n368377886.shtml

2. 三星 Note 2 再爆安全漏洞

前几日，三星 Galaxy Note 2 手机再曝安全漏洞。此漏洞是由安全研究人员 Terence Eden 发现，关于在该手机上可绕过解锁画面进入首页和程序的安全漏洞。在锁屏状态下，无需任何工具或手段，依次按下相应按键，就能看到 Home 首页会在一瞬间于屏幕上闪现。业内人士表示，这一情况与是否设置了 PIN 解锁、图形解锁、密码或是 Android 的脸部解锁都没有关系，甚至连第三方锁屏程序也不能避免该情况的发生。

参考链接：http://www.anqu.com/xinwen_486/34925/

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