国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2013 年 02 月 25 日-2013 年 03 月 03 日 **2013 年 第9 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 165 个，其中高危漏洞 47 个、中危漏洞 96 个、低危漏洞 22 个。上述漏洞中，可利用来实施远程攻击的漏洞有 136 个。本周收录的漏洞中，已有 108 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“Photodex ProShow Producer 存在多个 DLL 加载任意代码执行漏洞”、“Brewthology 'r' 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 165 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、天融信等单位报送数量较多。此外，上海交通大学和 High-Tech Bridge Security Research Lab 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	128	0
绿盟科技	89	0
安天实验室	58	0
天融信	36	0
恒安嘉新	9	0
东软	4	0
High-Tech Bridge Security Research Lab	3	3
上海交通大学	4	3

报送总计	331	6
录入总计	165（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 Google、Drupal、ownCloud、Linux 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	Google	22	13%
2	Drupal	10	6%
3	ownCloud	9	5%
4	Linux	8	5%
5	SAP	7	4%
6	Cisco	6	4%
7	IBM	6	4%
8	Adobe	3	2%
9	Red Hat	2	1%
10	Apache	2	1%
11	其它	90	55%

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 165 个漏洞。其中应用程序漏洞 116 个，WEB 应用漏洞 37 个，操作系统漏洞 8 个，网络设备漏洞 2 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	116
WEB 应用漏洞	37
网络设备漏洞	2
安全产品漏洞	2
操作系统漏洞	8

表 3 漏洞按影响类型统计表

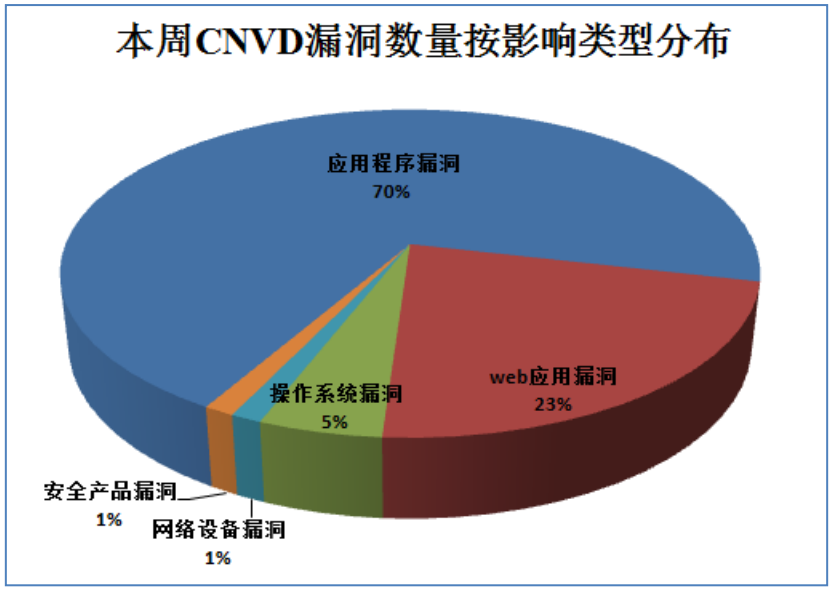

图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 1 个网络设备漏洞和 1 个移动互联网设备漏洞：Dell PowerConnect 6248P 拒绝服务漏洞、三星 Galaxy S III 紧急呼叫联系人 HOME 键密码锁绕过漏洞。其中，“Dell PowerConnect 6248P 拒绝服务漏洞”的综合评级为“高危”。

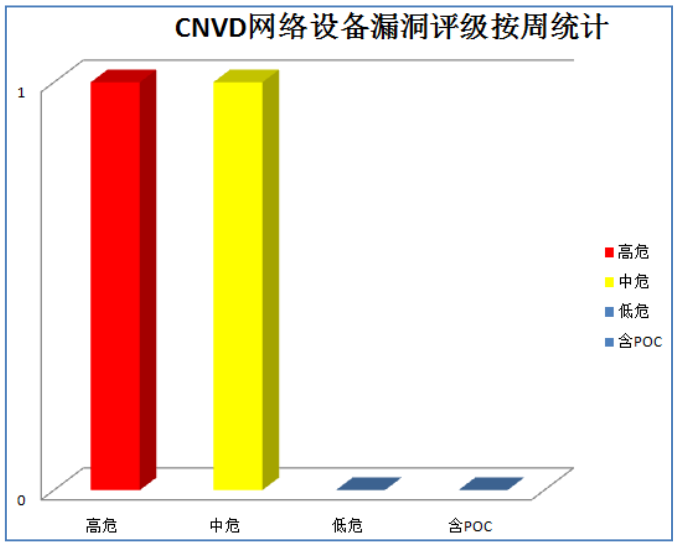

图 2 网络设备漏洞统计

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，攻击者利用漏洞可构建恶意 WEB 页，诱使用户解析，执行任意代码。

CNVD 收录的相关漏洞包括：Google Chrome 文件拷贝不正确路径处理漏洞、Google Chrome 媒体处理竞争条件漏洞、Google Chrome vorbis 解码缓冲区溢出漏洞、Google Chrome 不正确 API 权限授权漏洞、Google Chrome blob 处理整数溢出漏洞、Google Chrome SVG 参数处理内存访问漏洞、Google Chrome web 音频节点内存破坏漏洞、Google Chrome IPC 层处理内存漏洞等。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-2013-20278

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20275

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20277

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20261

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20271

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20256

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20250

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20269

2、Adobe 产品安全漏洞

Adobe Flash Player 是一款 Flash 文件处理程序。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Flash Player 'broker'缓冲区溢出漏洞、Adobe Flash Player 'ExternalInterface ActionScrip'远程代码执行漏洞、Adobe Flash Player 任意代码执行漏洞（CNVD-2013-20343）。其中，“Adobe Flash Player 'broker'缓冲区溢出漏洞”和“Adobe Flash Player 'ExternalInterface ActionScrip'远程代码执行漏洞”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-2013-20339

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20340

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20343

3、Cisco 产品安全漏洞

Cisco Cloud Portal 是一款思科公司推出的云应用解决方案；Cisco Adaptive Security Appliance 是一款自适应安全设备，提供 VPN 服务应用模块；Cisco Prime 是一款提

供，管理 LAN、WAN 与数据中心的解决方案；Cisco Unified Communications Manager 是一款 Cisco IP 电话解决方案中的呼叫处理组件；Cisco Unified Presence 是一款收集用户可用性和通信功能的信息，以提供统一用户在网状态的平台。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 Unified Presence Server 远程拒绝服务漏洞、Cisco Unified Communications Manager 缓存毒药漏洞、Cisco Unified Communications Manager 远程拒绝服务漏洞、Cisco Prime Central for HCS Assurance 远程拒绝服务漏洞、Cisco Adaptive Security Appliances 拒绝服务漏洞（CNVD-2013-20341）、Cisco Cloud Portal 信息泄露漏洞。其中，除“Cisco Adaptive Security Appliances 拒绝服务漏洞（CNVD-2013-20341）”和“Cisco Cloud Portal 信息泄露漏洞”外，其余漏洞的综合评级均为“高危”。厂商已发布了除上述两个漏洞外，其余漏洞的修补程序。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-2013-20383

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20381

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20379

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20376

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20341

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20346

4、IBM 产品安全漏洞

IBM HTTP Server 是一款基于 Apache 的 web 服务程序；IBM System Storage TS3500 磁带库为 IBM System z 和开放式系统备份与归档提供了可扩展的自动化磁带库；IBM Lotus Domino 服务器是一款基于 WEB 合作的应用程序架构；IBM InfoSphere Guardium 解决方案主要提供企业数据中心保障服务。本周，上述 IBM 产品被披露存在多个安全漏洞，攻击者利用漏洞可获得敏感信息或劫持用户会话，提升权限，发起跨站脚本攻击。

CNVD 收录的相关漏洞包括：IBM InfoSphere Guardium 权限提升漏洞、IBM Lotus Domino 存在未明开放重定向漏洞、IBM Lotus Domino 存在未明跨站脚本漏洞、IBM System Storage TS3500 磁带库安全绕过漏洞、IBM HTTP Server 模块跨站脚本漏洞、IBM HTTP Server 'mod_proxy_balance'模块跨站脚本漏洞。其中，“IBM InfoSphere Guardium 权限提升漏洞”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/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20395

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20323

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20324

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20364

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20304

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20305

5、Brewthology 'r'参数 SQL 注入漏洞

Brewthology 是一款基于 WEB 的应用程序。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 Brewthology beerxml.php 脚本未能正确过滤"r"参数，攻击者利用漏洞可进行 SQL 注入攻击，获得数据库敏感信息。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/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-20349

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-2013-20393	Poppler 内存破坏漏洞	高	用户可参考如下厂商提供的安全公告修复此漏洞：http://cgit.freedesktop.org/poppler/poppler/commit/?h=poppler-0.22
CNVD-2013-20338	Photodex ProShow Producer 存在多个 DLL 加载任意代码执行漏洞	高	暂无
CNVD-2013-20390	FFmpeg avcodec_decode_audio4 拒绝服务漏洞	高	用户可参考如下厂商提供的安全公告获得补丁信息：http://git.videolan.org/?p=ffmpeg.git;a=commit;h=8a6449167a6da8cb747cfe3502ae86ffaac2ed48
CNVD-2013-20350	Alt-N MDaemon STARTTLS 实现明文任意命令注入漏洞	高	MDaemon 13.0.4 已经修复此漏洞，建议用户下载使用：http://files.altn.com/MDaemon/release/relnotes_en.html
CNVD-2013-20315	Rix4Web 'dir_link'参数 SQL 注入漏洞	高	暂无
CNVD-2013-20359	SAP CCMS 代理代码注入漏洞	高	用户可参考如下厂商提供的 SAP Note 1758450 安全公告获得补丁信息：https://service.sap.com/sap/support/notes/1758450

CNVD-2013-20298	Dell PowerConnect 6248P 拒绝服务漏洞	高	暂无
CNVD-2013-20308	多个 VMware 产品内存破坏漏洞	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.vmware.com/security/advisories/VMSA-2013-0003.html
CNVD-2013-20316	CS-Cart 安全绕过漏洞	高	CS-Cart v3.0.6 已经修复此漏洞，建议用户下载使用：https://www.cs-cart.com/overview.html

表 3 部分高危漏洞列表

小结：本周，Adobe Flash Player、Google Chrome 被披露存在多个漏洞，攻击者利用漏洞可执行任意代码，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，发起拒绝服务或跨站脚本攻击。Brewthology 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、 Red Hat 发布升级程序，修补 OpenShift 漏洞

OpenShift 是由红帽推出的一款面向开源开发人员开放的云平台服务软件(PaaS)。本周，Red Hat 修补了 OpenShift 存在的漏洞。攻击者可以利用漏洞覆盖系统任意文件或者获取敏感信息。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=32374

http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=32373

本周要闻速递

1. HTML 5 漏洞可致硬盘遭垃圾数据填满

3 月 4 日消息，据国外媒体报道，最近有开发者发现，HTML 5 编码语言有一漏洞会使得网站产生数 GB 垃圾数据，在短时间内塞满硬盘，多款流行浏览器均受到该问题的影响。据本周发现这一问题的开发者法罗斯·阿布哈迪杰（Feross Aboukhadijeh）称，数据转储问题出现于大多数的网络浏览器上，其中包括苹果 Safari、谷歌 Chrome、微软 IE 和 Opera，Mozilla 的 Firefox 是唯一能够阻止数据转储的浏览器，Firefox 的存储上限是 5MB。该问题的根源在于 HTML 5 处理本地数据存储的方式有关。尽管每款浏览器的存储参数设置并不相同，但大多数都支持用户自定义上限，这使得存储在用户电脑的

空间上限至少达 2.5MB。在测试该漏洞时，采用固态硬盘的 MacBook Pro 每 16 秒钟就能够转储 1GB 数据。像 Chrome 这样的 32 位浏览器在硬盘存满之前可能会出现崩溃。阿布哈迪杰已经发布了代码来利用该漏洞，漏洞报告已经发给受影响浏览器的厂商，目前尚未发现其代码遭遇大范围的恶意使用行为。

参考链接：http://it.21cn.com/itnews/a/2013/0304/09/20526747.shtml

2. WinterBoard 更新:修复关键资源 vNode 漏洞

Saurik 日前发布了 Cydia 0.9.3911 版本更新，本次更新主要是修复一个漏洞，该漏洞会导致许多使用 Winterboard 的插件在加载时出现崩溃的问题。发现问题之后，Saurik 对这个问题进行研究，使用自制的 vNode 调试工具来进行测试，确定问题的根源就是 Winterboard，因此在 0.9.3911 版本中解决了该问题。目前 Winterboard 已经更新。

参考链接：http://tech.ifeng.com/digi/detail_2013_03/02/22662367_0.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