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 21 日-2013 年 01 月 27 日 **2013 年 第 4 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 148 个，其中高危漏洞 35 个、中危漏洞 99 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 137 个。本周收录的漏洞中，已有 115 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“NConf 'id'参数 SQL 注入漏洞”等漏洞的零日攻击代码，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 148 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。此外，广西网信和 High-Tech Bridge Security Research Lab 向 CNVD 提交了 3 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	135	0
绿盟科技	92	0
天融信	43	0
安天实验室	34	0
恒安嘉新	3	0
东软	3	0
High-Tech Bridge Security Research Lab	2	2
广西网信	1	1
报送总计	313	3
录入总计	148（去重）	3

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Cisco、Drupal、WordPress、Moodle、IBM 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	Cisco	17	11%
2	Drupal	11	7%
3	WordPress	10	7%
4	Moodle	10	7%
5	IBM	7	5%
6	Google	6	4%
7	SAP	5	3%
8	Barracuda Networks, Inc.	4	3%
9	EMC	3	2%
10	F5	2	1%
11	其它	73	50%

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 148 个漏洞。其中应用程序漏洞 93 个，WEB 应用漏洞 37 个，网络设备漏洞 12 个，安全产品漏洞 6 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	93
WEB 应用漏洞	37
网络设备漏洞	12
安全产品漏洞	6
数据库漏洞	0
操作系统漏洞	0

表 3 漏洞按影响类型统计表

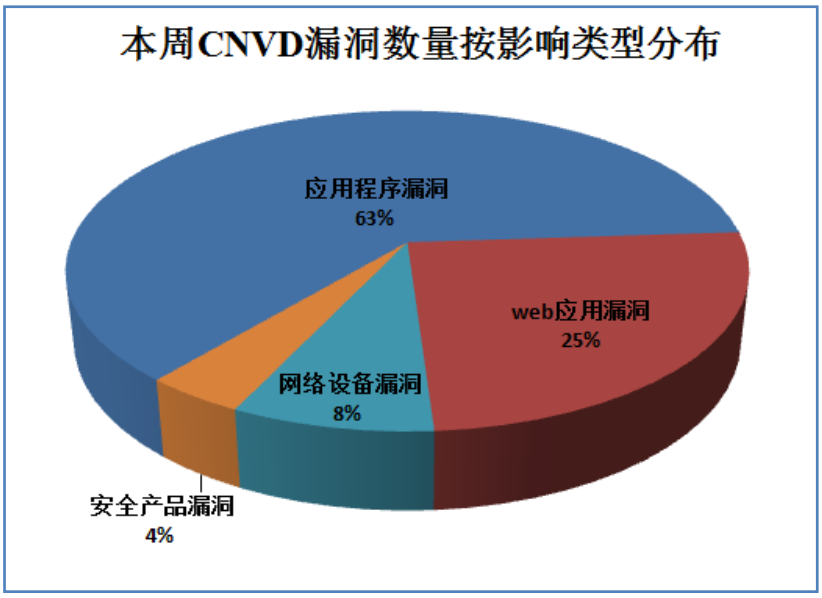

图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 12 个网络设备漏洞：Cisco Linksys WRT54GL Router 'wan_hostnam'令执行漏洞、Cisco Linksys WRT54GL Router 安全绕过漏洞、Cisco Linksys WRT54GL Router 跨站请求伪造漏洞、Cisco Linksys WRT54GL Router 跨站脚本漏洞、Cisco NX-OS on Nexus 7000 远程拒绝服务漏洞、F5 BIG-IP 'saveSettings.php' SQL 注入漏洞、F5 BIG-IP XML 外部实体注入漏洞、Sitecom WLM-2501 跨站请求伪造漏洞、Cisco Wireless LAN Controller 拒绝服务漏洞（CNVD-2013-19522）、Cisco Wireless LAN Controller 拒绝服务漏洞（CNVD-2013-19524）、Cisco Wireless LAN Controller 任意代码执行漏洞、Cisco Wireless LAN Controller SNMP 未验证访问漏洞。

其中，“Cisco Linksys WRT54GL Router 'wan_hostnam'令执行漏洞、F5 BIG-IP 'saveSettings.php' SQL 注入漏洞、Cisco Wireless LAN Controller 拒绝服务漏洞（CNVD-2013-19522）、Cisco Wireless LAN Controller 拒绝服务漏洞（CNVD-2013-19524）、Cisco Wireless LAN Controller 任意代码执行漏洞、Cisco Wireless LAN Controller SNMP 未验证访问漏洞”的综合评级均为“高危”。目前，互联网上已经出现了针对 F5、Cisco、Sitecom 等相关厂商产品的攻击代码，相关厂商已经发布了漏洞的修补程序。

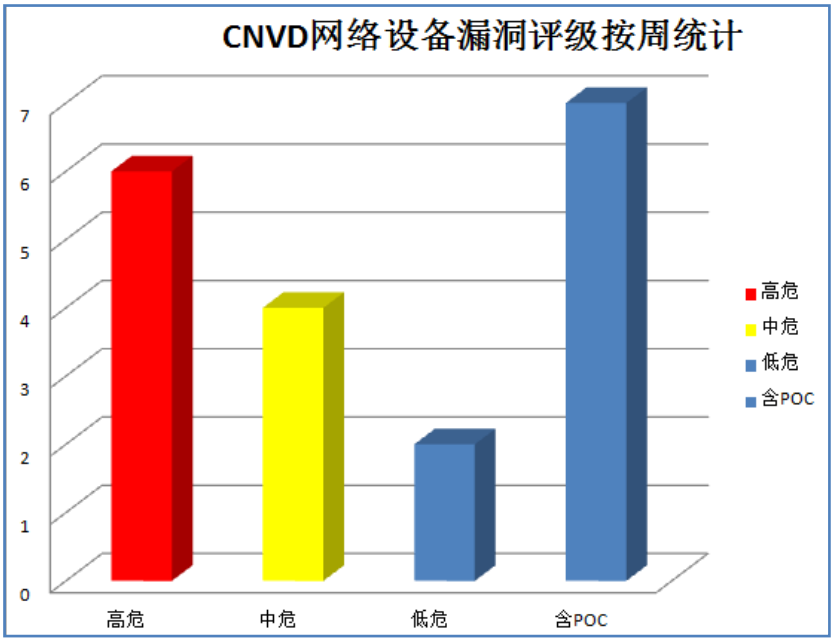

图 2 网络设备漏洞统计

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、Cisco 产品安全漏洞

Cisco Wireless LAN Controller 是一款用于使用轻量级接入点协议(LWAPP)管理 Cisco Aironet 接入点的应用设备。Cisco Linksys WRT54GL Router 是一款无线路由设备；Cisco WebEx Social 是一款思科公司推出的社交软件；Cisco Adaptive Security Appliance 是一款自适应安全设备，可提供安全和 VPN 服务的模块；Cisco VPN Client 是一款 VPN 客户端程序。本周，上述思科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，修改设备配置，发起拒绝服务攻击或执行任意代码。

CNVD 收录的相关漏洞包括：Cisco Wireless LAN Controller SNMP 未验证访问漏洞、Cisco Wireless LAN Controller 拒绝服务漏洞（CNVD-2013-19524、CNVD-2013-19522）、Cisco Wireless LAN Controller 任意代码执行漏洞、Cisco Linksys WRT54GL Router 'wan_hostnam'令执行漏洞、Cisco WebEx Socia 跨站脚本漏洞、Cisco Adaptive Security Appliances (ASA)拒绝服务漏洞（CNVD-2013-19432）、Windows Cisco VPN 客户端拒绝服务漏洞等。其中，“Cisco Wireless LAN Controller SNMP 未验证访问漏洞、Cisco Wireless LAN Controller 拒绝服务漏洞（CNVD-2013-19524、CNVD-2013-19522）、Cisco Wireless LAN Controller 任意代码执行漏洞、Cisco Linksys WRT54GL Router 'wan_hostnam'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-2013-19530

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19524

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19528

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19522

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19448

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19422

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19432

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19421

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，攻击者利用漏洞可获得敏感信息，执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Google Chrome canvas 字体内存错误引用漏洞、Google Chrome 内容拦截数组索引检查漏洞、Google Chrome 'RTC'拒绝服务漏洞、Google Chrome 跨站脚本过滤器安全绕过漏洞（CNVD-2013-19477）、Google Chrome 路径空字符处理漏洞。其中，“Google Chrome canvas 字体内存错误引用漏洞”和“Google Chrome 内容拦截数组索引检查漏洞”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-2013-19515

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19516

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19517

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19518

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19477

3、IBM 产品安全漏洞

IBM WebSphere Application Server (WAS)是一款由 IBM 开发并发行的应用服务器；Tivoli Federated Identity Manager 是 IBM 身份集成计划的软件套件。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。

CNVD 收录的相关漏洞包括：IBM WebSphere Application Server 跨站脚本漏洞（CNVD-2013-19548、CNVD-2013-19545、CNVD-2013-19546）、IBM WebSphere Application Server 'portlet'跨站请求伪造漏洞、IBM WebSphere Application Server 安全绕过漏洞（CNVD-2013-19550）、IBM Tivoli Federated Identity Manager OpenID 属性绕过漏洞、IBM Tivoli Federated Identity Manager 敏感信息泄露漏洞。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-2013-19548

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19545

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19546

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19547

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19550

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19444

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19443

4、SAP NetWeaver 安全漏洞

SAP NetWeaver 是一款集成化应用软件平台，用于系统应用整合。其组件包括门户、应用服务器、商务智能解决方案以及系统整合技术。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，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：SAP NetWeaver SDM 验证绕过漏洞、SAP NetWeaver SDM 拒绝服务漏洞、SAP NetWeaver SDM 信息泄露 SMBRelay 攻击漏洞、SAP NetWeaver SDM Admin 信息泄露漏洞、SAP NetWeaver SDM Admin 拒绝服务漏洞。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-2013-19527

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19529

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19531

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19532

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19534

5、F5 BIG-IP 安全漏洞

F5 BIG-IP 是一款应用交付前置网络设备。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恶意 SQL 查询，获得系统文件。

CNVD 收录的相关漏洞包括：F5 BIG-IP 'saveSettings.php' SQL 注入漏洞、F5 BIG-IP XML 外部实体注入漏洞。其中，“F5 BIG-IP 'saveSettings.php' SQL 注入漏洞”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-2013-19509

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=CNVD-2013-19510

6、NConf 'id'参数 SQL 注入漏洞

NConf 是一个用来配置 Nagios 监控软件的 Web 接口项目。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 NConf detail.php 和

detail_admin_items.php 未能正确过滤用户提交给'id'参数的数据，攻击者利用漏洞可进行 SQL 注入攻击，获得敏感信息或控制应用系统。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-2013-19497

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-2013-19521	NetArt Media Car Portal 文件上传漏洞	高	暂无
CNVD-2013-19538	DIY-CMS 'mod.php' SQL 注入漏洞	高	暂无
CNVD-2013-19493	Lenovo Bluetooth with Enhanced Data Rate Software DLL 加载任意代码执行漏洞	高	Lenovo 已经修复此漏洞，建议用户下载使用：http://download.lenovo.com/ibmdl/pub/pc/pccbbs/mobiles/g4wb10ww.txt
CNVD-2013-19487	Joomla! Collector 组件任意文件上传漏洞	高	暂无
CNVD-2013-19511	PDF-XChange Viewer PDF 文件处理堆缓冲区溢出漏洞	高	厂商已经修复此漏洞，建议用户下载更新：http://www.docu-track.com/home/prod_user/PDF-XChange_Tools/pdfx_viewer
CNVD-2013-19494	Movable Type 'mt-upgrade.cgi'输入验证漏洞	高	Movable Type 4.38 和 5.0 已经修复此漏洞，建议用户下载使用：http://www.movabletype.org
CNVD-2013-19445	IP.Gallery 'img'参数 SQL 注入漏洞	高	暂无
CNVD-2013-19502	ownCloud 'settings/personal.php'任意代码执行漏洞	高	ownCloud Server 4.5.6 或 4.0.11 已经修复此漏洞，建议用户下载使用：http://www.owncloud.org
CNVD-2013-19506	GE Proficy CIMPLICITY 命令执行漏洞	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.us-cert.gov/control_systems/pdf/ICSA-13-022-02.pdf
CNVD-2013-19446	php-Charts 'url.php'任意 PHP 代码执行漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，F5 BIG-IP 和 Cisco 多款产品被披露存在多个漏洞，攻击者利用漏洞可获取或修改设备配置信息，发起拒绝服务攻击或取得网络设备管理权限。Google 浏览器被披露存在多个漏洞，可能被用于挂马攻击。SAP NetWeaver 和 IBM 多款产品也被披露存在多个漏洞，攻击者利用漏洞可获得敏感信息，发起拒绝服务攻击。此外，NConf 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、F5 发布升级程序，修补 BIG-IP 漏洞

F5 BIG-IP 是一款应用交换机。本周，F5 修补了 BIG-IP 存在的漏洞。攻击者可以获得用户密码哈希值、访问系统文件。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=31171

http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=31151

本周要闻速递

1. IE 再曝零日漏洞

赛门铁克曾报道，一种新型 Internet Explorer 零日漏洞的利用正在迅速扩散。之后，微软发布了安全公告 2794220，证实 Microsoft Internet Explorer CdwnBindInfo Use-After-Free 远程代码执行漏洞(CVE-2012-4792)是影响 Internet Explorer 8、Internet Explorer 7 和 Internet Explorer 6 的零日漏洞。这些攻击中的网站均受到感染，并被用作水坑式攻击的一部分来为零日漏洞利用提供服务。水坑式攻击是一种锁定目标人群可能访问的网站的方法。攻击者会破坏此网站并植入 JavaScript 或 HTML，从而将受害者重新定向到其它恶意代码。在这种情况下，此新型 Internet Explorer 零日漏洞已成功破坏目标网站；当受害者访问目标网站时，JavaScript 会开始运行并执行大量检查，然后趁机攻击浏览器。

参考链接：http://tech.cnr.cn/list/201301/t20130127_511864954.html

2. Pod2g 发现新漏洞

对于 iOS 6 用户来说，最期待的无非就是它的完美越狱了。近日，越狱大神 Pod2g 更新了它的 Twitter，发布一条消息称，发现两个新的 iOS 6 系统漏洞。但从 Pod2g 的 Twitter 中可以看出，虽然发现了两个新的 iOS 6 系统漏洞，但由于源代码没有找到，所以完美越狱还不能正式放出。

参考链接：http://it.dbw.cn/system/2013/01/27/054548209.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