国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2015 年 03 月 23 日-2015 年 03 月 29 日 **2015 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**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 130 个，其中高危漏洞 37 个、中危漏洞 82 个、低危漏洞 11 个。上述漏洞中，可利用来实施远程攻击的漏洞有 120 个。本周收录的漏洞中，已有 86 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。其中互联网上出现“PHP KIT SQL 注入漏洞”、“Joomla! 'com_tpjobs'组件'id_c[]'参数 SQL 注入漏洞”等零日攻击代码，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、合作伙伴及个人报送了本周收录的全部 130 个漏洞。报送情况如表 1 所示。其中，奇虎 360、安天实验室、恒安嘉新、绿盟科技、天融信等单位报送数量较多。此外，补天平台、CNCERT 各分中心、High-Tech Bridge Security Research Lab、卓望数码技术（深圳）有限公司、江苏国瑞信安科技有限公司、安徽讯成创安科技有限公司及白帽子向 CNVD 提交了 677 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
奇虎 360	276	276
安天实验室	134	0
恒安嘉新	125	0
绿盟科技	85	0
天融信	75	11

启明星辰	75	0
东软	2	0
乌云	345	345
漏洞盒子	18	18
High-Tech Bridge Security Research Lab	2	2
CNCERT 福建分中心	4	4
卓望数码技术（深圳）有限公司	5	5
江苏国瑞信安科技有限公司	1	1
安徽讯成创安科技有限公司	1	1
个人	14	14
报送总计	1162	677
录入总计	130（去重）	677

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、OpenSSL、PHP 等多家厂商的产品，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	16	12%
2	OpenSSL	13	10%
3	PHP	4	3%
4	LBL	4	3%
5	Cisco	4	3%
6	Drupal	4	3%
7	X.Org	3	2%
8	MetalGenix	3	2%
9	WordPress	2	2%
10	其他	77	60%

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 130 个漏洞。其中应用程序漏洞 87 个，WEB 应用漏洞 33 个，网络设备漏洞 4 个，操作系统漏洞 3 个，安全产品 3 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	87
WEB 应用漏洞	33
网络设备漏洞	4
操作系统漏洞	3
安全产品漏洞	3

表 3 漏洞按影响类型统计表

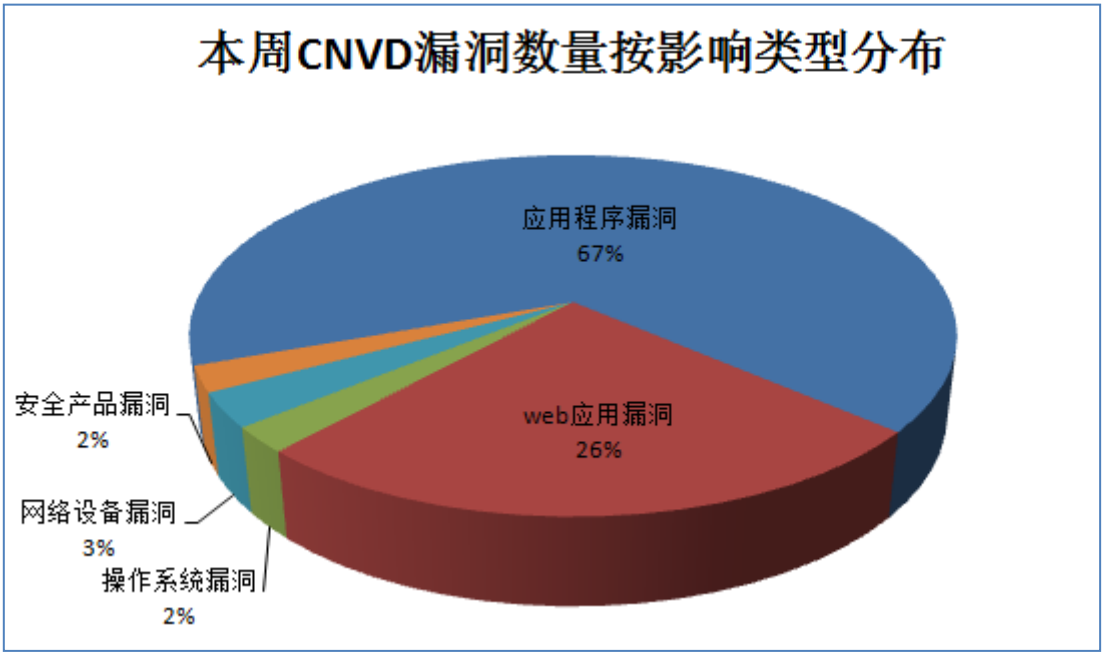

图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 7 个电信行业漏洞，1 个移动互联网行业漏洞，1 个工控系统行业漏洞（如下图表所示）。其中，“Google Android 'get_option()'函数远程代码执行漏洞”的综合评级均为“高危”。相关厂商已经发布了上述漏洞的修补程序。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2015-01883	Cisco WebEx Meetings Server 跨站脚本漏洞（CNVD-2015-01883）	中	是
电信	CNVD-2015-01946	IBM Business Process Manager 跨站脚	中	是

		本漏洞（CNVD-2015-01946）		
电信	CNVD-2015-01955	Asus RT-G32 路由器跨站脚本漏洞	中	否
电信	CNVD-2015-01969	ASUS RT-G32 跨站请求伪造漏洞	中	否
电信	CNVD-2015-02011	IBM Tivoli Directory Server (ITDS) FREAK 降级攻击漏洞	中	是
电信	CNVD-2015-02029	pfSense 存在多个跨站脚本漏洞	低	是
电信	CNVD-2015-02028	pfSense 跨站请求伪造漏洞	中	是
移动互联网	CNVD-2015-01961	Google Android 'get_option()'函数远程代码执行漏洞	高	是
工控系统	CNVD-2015-02027	多个 Rockwell Automation 产品 DLL 加载存在多个本地代码执行漏洞	中	是

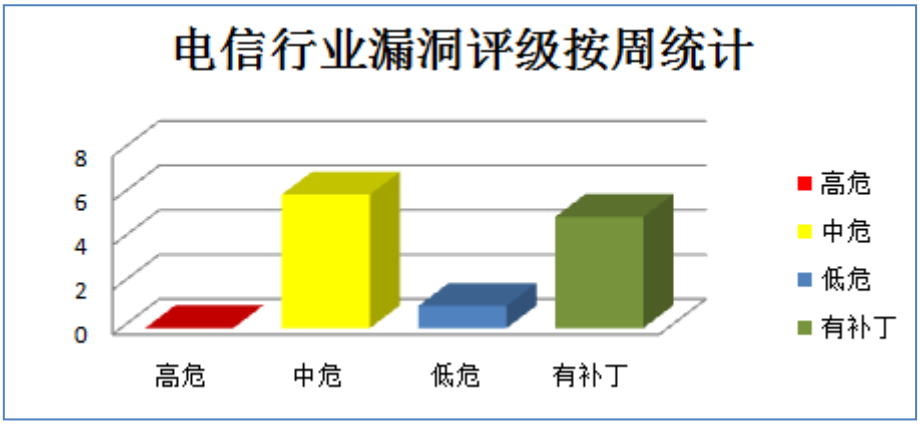

图 1 电信行业漏洞统计

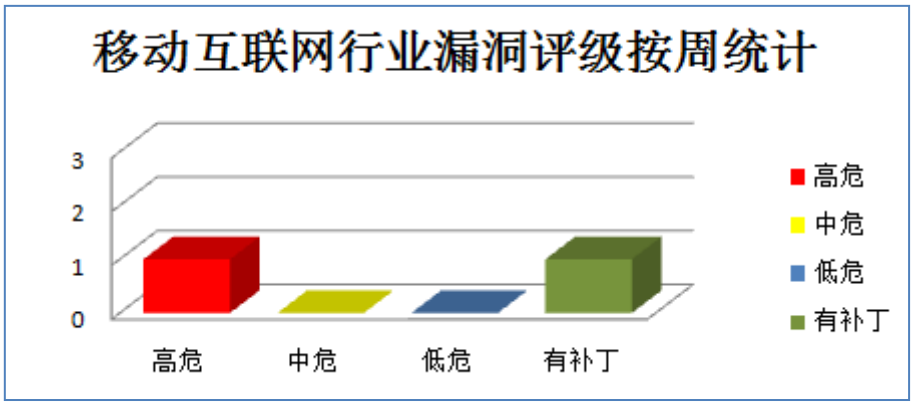

图 2 移动互联网行业漏洞统计

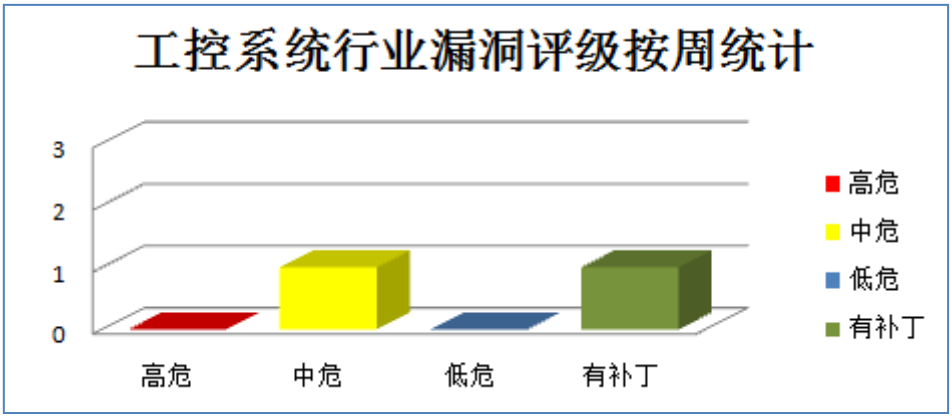

图 3 工控系统行业漏洞统计

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、 OpenSSL 产品安全漏洞

OpenSSL 是一种开放源码的 SSL 实现，用来实现网络通信的高强度加密，现在被广泛地用于各种网络应用程序中。本周，上述产品被披露存在拒绝服务漏洞，攻击者可利用漏洞发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：OpenSSL 'EVP_DecodeUpdate'拒绝服务漏洞、OpenSSL ClientHello sigalgs 拒绝服务漏洞、OpenSSL 'multi-block'功能拒绝服务漏洞、OpenSSL 'dtls1_listen'函数拒绝服务漏洞、OpenSSL 'ASN1_TYPE_cmp'函数拒绝服务漏洞、OpenSSL ASN.1 signature-verification 拒绝服务漏洞、OpenSSL 'ASN1_item_ex_d2i'函数拒绝服务漏洞、OpenSSL PKCS#7 拒绝服务漏洞。其中，“OpenSSL 'EVP_DecodeUpdate'拒绝服务漏洞”的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒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-2015-01894

http://www.cnvd.org.cn/flaw/show/CNVD-2015-01887

http://www.cnvd.org.cn/flaw/show/CNVD-2015-01888

http://www.cnvd.org.cn/flaw/show/CNVD-2015-01889

http://www.cnvd.org.cn/flaw/show/CNVD-2015-01890

http://www.cnvd.org.cn/flaw/show/CNVD-2015-01891

http://www.cnvd.org.cn/flaw/show/CNVD-2015-01892

http://www.cnvd.org.cn/flaw/show/CNVD-2015-01893

2、 IBM 产品安全漏洞

IBM Rational ClearCase 是美国 IBM 公司的一套软件配置管理解决方案。IBM Rational Focal Point 是 IBM Rational 基于 Web 的产品管理系统，内置了面向客户和市场的产品管理流程，提供产品管理过程中的工作流自动化、信息相关性分析、信息统计分析以及信息的优先级分析功能。IBM General Parallel File System 是一套共享文件系统，起源于 IBM SP 系统上使用的虚拟共享磁盘技术。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞获取敏感信息、绕过安全限制、进行跨站攻击、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：IBM General Parallel File System ROOT 权限执行漏洞、IBM General Parallel File System 绕过验证执行代码漏洞、IBM General Parallel File System mmfslinux 内核模块拒绝服务漏洞、IBM Rational ClearCase 信息泄露漏洞、IBM Rational ClearQuest 跨站请求伪造漏洞（CNVD-2015-01981）、IBM Rational Focal Point HTML 注入漏洞（CNVD-2015-01907）、IBM Rational Focal Point 跨站脚本漏洞（CNVD-2015-01906）、IBM Rational Focal Point 安全绕过漏洞。其中，“IBM General Parallel File System ROOT 权限执行漏洞、IBM General Parallel File System 绕过验证执行代码漏洞”的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒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-2015-01960

http://www.cnvd.org.cn/flaw/show/CNVD-2015-01959

http://www.cnvd.org.cn/flaw/show/CNVD-2015-01958

http://www.cnvd.org.cn/flaw/show/CNVD-2015-01983

http://www.cnvd.org.cn/flaw/show/CNVD-2015-01981

http://www.cnvd.org.cn/flaw/show/CNVD-2015-01907

http://www.cnvd.org.cn/flaw/show/CNVD-2015-01906

http://www.cnvd.org.cn/flaw/show/CNVD-2015-01905

3、 Cisco 产品安全漏洞

Cisco Small Business IP phones SPA 300 和 SPA 500 是美国思科（Cisco）公司的 SPA 300 和 SPA 500 系列 IP 网络电话产品。Cisco IOS 是美国思科（Cisco）公司为其网络设备开发的操作系统。Cisco WebEx Meetings 是网络会议解决方案。本周，上述产品被披露存在信息泄露、跨站脚本和拒绝服务漏洞，攻击者可利用漏洞获取敏感信息、进行跨站攻击或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco Small Business IP phones SPA 300 和 SPA 500 信息泄露漏洞、Cisco IOS Autonomic Networking Infrastructure 拒绝服务漏洞、Cisco Videoscape Distribution Suite for Internet Streaming 拒绝服务漏洞、Cisco WebEx Meetings Server 跨站脚本漏洞（CNVD-2015-01883）。目前，厂商已经发布了除“Cisco S

mall Business IP phones SPA 300 和 SPA 500 信息泄露漏洞”外，其余漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，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-2015-01923

http://www.cnvd.org.cn/flaw/show/CNVD-2015-01924

http://www.cnvd.org.cn/flaw/show/CNVD-2015-01884

http://www.cnvd.org.cn/flaw/show/CNVD-2015-01883

4、Drupal 产品安全漏洞

Drupal 是一个基于 PHP 语言编写的开发型 CMF(内容管理框架)。本周，上述产品被披露存在跨站脚本漏洞，攻击者可利用漏洞进行跨站脚本攻击。

CNVD 收录的相关漏洞包括：Drupal Webform 模块存在多个跨站脚本漏洞、Drupal OG tabs 模块存在多个跨站脚本漏洞、Drupal Image Title 模块存在多个跨站脚本漏洞、Drupal Site Documentation 模块存在多个跨站脚本漏洞。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，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-2015-02023

http://www.cnvd.org.cn/flaw/show/CNVD-2015-02022

http://www.cnvd.org.cn/flaw/show/CNVD-2015-02021

http://www.cnvd.org.cn/flaw/show/CNVD-2015-02020

5、Drumbeat CMS SQL 注入漏洞

Drumbeat CMS 是澳大利亚 Drumbeat 公司的一套中小企业托管内容管理系统（CMS）。本周，Drumbeat CMS 被披露存在综合评级为“高危”的 SQL 注入漏洞。攻击者可利用该漏洞控制应用程序，访问或修改数据库数据。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-2015-02016

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-2015-01916	MyBB cache handler 漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞：http://blog.mybb.com/2015/02/15/mybb-1-8-4-released-feature-update-security-maintenance-release/
CNVD-2015-01917	Fortinet Single Sign On collector agent.exe 栈缓冲区溢出漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞：http://www.fortiguard.com/advisory/FG-IR-15-006/

CNVD-2015-01918	Futomi CGI Cafe MP Form Mail CGI eCommerce 任意代码执行漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：http://www.futomi.com/library/info/2015/20150319.html
CNVD-2015-01922	X.Org libXfont bitmap/bdfread.c 拒绝服务漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：http://www.x.org/wiki/Development/Security/Advisory-2015-03-17/
CNVD-2015-01925	X.Org libXfont bitmap/bdfread.c 空指针引用拒绝服务漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：http://www.x.org/wiki/Development/Security/Advisory-2015-03-17/
CNVD-2015-01926	X.Org libXfont bitmap/bdfread.c 越界写拒绝服务漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：http://www.x.org/wiki/Development/Security/Advisory-2015-03-17/
CNVD-2015-01941	PHP DateInterval unserialize()函数内存错误引用漏洞	高	暂无
CNVD-2015-01942	PHP SoapClient 类型混淆代码执行漏洞	高	暂无
CNVD-2015-01954	MetalGenix GeniXCMS SQL 注入漏洞	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：https://github.com/semplon/GeniXCMS/commit/698245488343396185b1b49e7482ee5b25541815
CNVD-2015-01963	PHP '/ext/enchant/enchant.c' 堆缓冲区溢出漏洞	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://www.php.net/downloads.php

表 3 部分高危漏洞列表

小结：本周，OpenSSL 被披露存在拒绝服务漏洞，攻击者可利用漏洞发起拒绝服务攻击。此外，IBM、Cisco、Drupal 多款产品被批露存在多个安全漏洞，允许攻击者利用漏洞获取敏感信息、绕过安全限制、进行跨站攻击、执行任意代码或发起拒绝服务攻击。另外，Drumbeat CMS 被披露存在一个高危零日漏洞，攻击者可利用该漏洞控制应用程序，访问或修改数据库数据。建议相关用户应随时关注上述厂商主页，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、EMC 修补 2 款产品漏洞

EMC Documentum xCelerated Management System（xMS）是美国易安信（EMC）公司的一个用于简化和加速 Documentum（内容管理系统）部署到基于 VMware 的私有云环境中的技术。EMC Secure Remote Services Virtual Edition（ESRS VE）是美国易安信（EMC）公司的一套用于在 EMC 客户服务和终端用户的 EMC 产品及解决方案之间提供双向远程连接的远程服务虚拟版软件。

本周，EMC 修补了上述产品存在的信息泄露和命令注入漏洞，避免攻击者利用漏洞获取敏感信息或执行任意代码。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网络安全事件。

补丁下载链接：http://www.cnvd.org.cn/patchInfo/show/56608

http://www.cnvd.org.cn/patchInfo/show/56578

本周要闻速递

1. SSL/TLS 又曝新漏洞，可明文读取传输数据

SL/TLS 协议是一个被广泛使用的加密协议，而研究人员近日了曝出一个名为“受诫礼”的新型攻击手段，能够窃取通过 SSL 和 TLS 协议传输的机密数据， 诸如银行卡号码，密码和其他敏感信息。这种攻击利用了一个 RC4 加密算法中的一个长达 13 年的漏洞。众所周知 RC4 算法不怎么安全，但事实互联网上 30% 的 TLS 流量加密使用的都是 RC4 算法。受诫礼(Bar Mitzvah)攻击实际上是利用了"不变性漏洞"，这是 RC4 算法中的一个缺陷，它能够在某些情况下泄露 SSL/TLS 加密流量中的密文，从而将账户用 户名密码，信用卡数据和其他敏感信息泄露给黑客。

参考链接：http://www.freebuf.com/news/62301.html

2. Cisco IP 电话暴高危漏洞可致远程窃听

Cisco 小型商业电话的固件暴高危漏洞，攻击者可通过该漏洞监听私人电话以及进行远程拨打电话，而且这一系列恶意行为都不需要任何身份验证。该漏洞（CVE-2015-0670）的存在实际上是由于某些 Cisco IP 电话的默认配置中含有了一些不恰当的设置。它允许攻击者通过向受影响的设备发送特殊的 XML 请求来控制该设备。此外，该漏洞可以被黑客利用来进行远程拨打电话，利用收集到的音频信息对目标进行一系列的其他攻击。该漏洞影响到 Cisco 小型商业 SPA300 以及 SPA500 IP 电话且运行的固件版本为 7.5.5。然而，Cisco 发出警告称在 7.5.5 后的版本也可能会受到该漏洞影响。

参考链接：http://www.freebuf.com/news/61719.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

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，为非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心协调机构。

作为国家级应急中心，CNCERT 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82990999