国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2015 年 02 月 09 日-2015 年 02 月 15 日 **2015 年第 7 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 233 个，其中高危漏洞 105 个、中危漏洞 118 个、低危漏洞 10 个。上述漏洞中，可利用来实施远程攻击的漏洞有 209 个。本周收录的漏洞中，已有 205 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“Byzanz GIF Encoding 缓冲区溢出漏洞"、"Joomla! CMSJunkie J-ClassifiedsManager 组件 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 6 家成员单位、合作伙伴及个人报送了本周收录的全部 233 个漏洞。报送情况如表 1 所示。其中，奇虎 360、安天实验室、天融信、恒安嘉新、启明星辰等单位报送数量较多。此外，CNCERT 各分中心、High-Tech Bridge Security Research Lab、北京国舜科技有限公司及白帽子向 CNVD 提交了 1251 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	1228	1228
安天实验室	178	0
天融信	167	0
恒安嘉新	150	0
启明星辰	104	0
绿盟科技	93	0

High-Tech Bridge Security Research Lab	3	3
北京国舜科技有限公司	1	1
CNCERT 甘肃分中心	4	4
CNCERT 新疆分中心	3	3
CNCERT 河南分中心	2	2
CNCERT 江西分中心	2	2
CNCERT 福建分中心	1	1
CNCERT 宁夏分中心	1	1
个人	6	6
报送总计	1943	1251
录入总计	233（去重）	1251

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Microsoft、FreeType、Adobe 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	Microsoft	56	24%
2	FreeType	20	9%
3	Adobe	18	8%
4	Cisco	17	7%
5	Drupal	10	4%
6	Stuart Caie	8	3%
7	WordPress	6	3%
8	Fortinet	6	3%
9	Google	5	2%
10	其他	87	37%

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 233 个漏洞。其中应用程序漏洞 161 个，WEB 应用漏洞 38 个，操作系统漏洞 12 个，网络设备漏洞 11 个，安全产品漏洞 7 个，数据库漏洞 4 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	161
WEB 应用漏洞	38
操作系统漏洞	12
网络设备漏洞	11
安全产品漏洞	7
数据库漏洞	4

表 3 漏洞按影响类型统计表

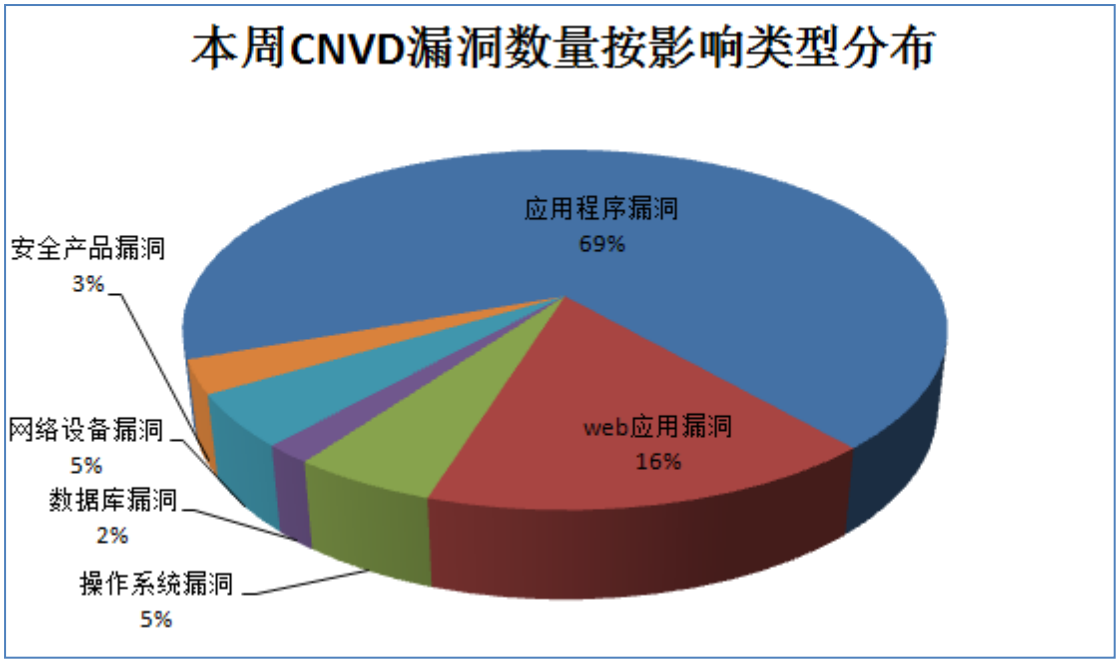

图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 15 个电信行业漏洞，7 个移动互联网行业漏洞（如下图表所示）。其中，“Cisco WebEx Meetings Server 命令注入漏洞、PostgreSQL 'to_char()' 函数缓冲区溢出漏洞、PostgreSQL 'pgcrypto'模块缓冲区溢出漏洞、Cisco IOS Software 拒绝服务漏洞（CNVD-2015-01122）、Cisco Secure Access Control System SQL 注入漏洞、Google Chrome for Android 内存错误引用漏洞、Google Chrome for Android 跨域绕过漏洞、Google Chrome for Android 特权提升漏洞、Google Chrome for Android 存在未明漏洞（CNVD-2015-00944）、FancyFon Software FAMOC SQL 注入漏洞”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-2015-00960	Cisco WebEx Meetings Server 命令注入漏洞	高	是
电信	CNVD-2015-01002	SIPhone Enterprise PBX SQL 注入漏洞	高	否
电信	CNVD-2015-01001	fli4l 跨站脚本漏洞	中	是
电信	CNVD-2015-01025	Apache Tomcat 全系报请求漏洞	中	是
电信	CNVD-2015-01038	PostgreSQL 'to_char()' 函数缓冲区溢出漏洞	高	是
电信	CNVD-2015-01039	PostgreSQL 'pgcrypto'模块缓冲区溢出漏洞	高	是
电信	CNVD-2015-01040	PostgreSQL 安全绕过漏洞（CNVD-2015-01040）	中	是
电信	CNVD-2015-01043	Cisco IOS Software 拒绝服务漏洞	中	是
电信	CNVD-2015-01121	IBM Tivoli Endpoint Manager HTML 注入漏洞	中	是
电信	CNVD-2015-01122	Cisco IOS Software 拒绝服务漏洞（CNVD-2015-01122）	高	是
电信	CNVD-2015-01123	Cisco IOS 安全绕过漏洞	中	是
电信	CNVD-2015-01137	Cisco Secure Access Control System SQL 注入漏洞	高	是
电信	CNVD-2015-01139	Cisco IOS Software 拒绝服务漏洞（CNVD-2015-01139）	中	是
电信	CNVD-2015-01142	Cisco IOS Software 本地拒绝服务漏洞	中	是
电信	CNVD-2015-01167	PostgreSQL 'constraint-violation'信息泄露漏洞	中	是
移动互联网	CNVD-2015-00943	Google Chrome for Android 内存错误引用漏洞	高	是
移动互联网	CNVD-2015-00945	Google Chrome for Android 跨域绕过漏洞	高	是
移动互联网	CNVD-2015-00946	Google Chrome for Android 特权提升漏洞	高	是
移动互联网	CNVD-2015-00944	Google Chrome for Android 存在未明漏洞（CNVD-2015-00944）	高	是
移动互联网	CNVD-2015-01006	FancyFon Software FAMOC SQL 注入漏洞	高	是
移动互联网	CNVD-2015-01147	Fortinet FortiClient 中间人攻击漏洞（CNVD-2015-01147）	中	否
移动互联网	CNVD-2015-01170	多个 Hitachi 产品 online help 系统跨站脚本漏洞	中	是

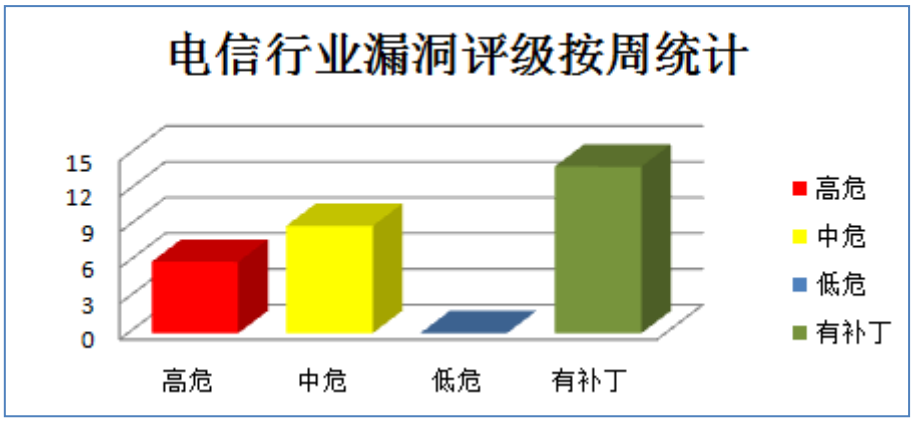

图 1 电信行业漏洞统计

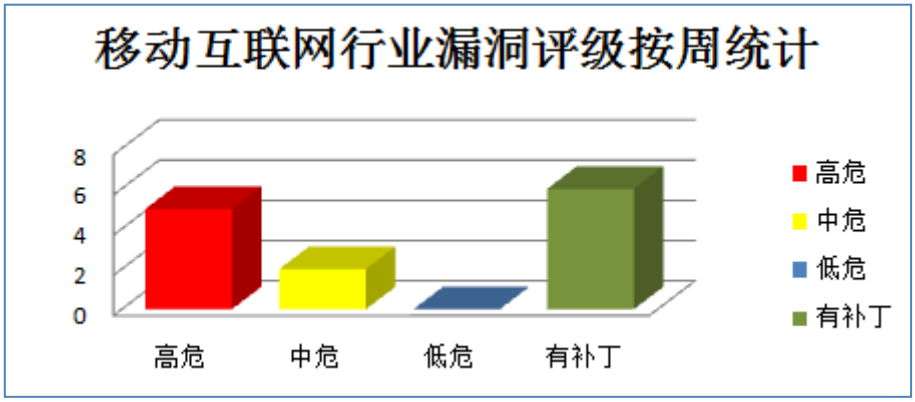

图 2 移动互联网行业漏洞统计

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

2 月 10 日，微软发布了 2015 年 2 月份的月度例行安全公告，共含 9 项更新，修复了 Microsoft Windows、Internet Explorer、Office 和 Server 软件中存在的 56 个安全漏洞。其中，3 项更新的综合评级为最高级“严重”级别。利用上述漏洞，攻击者可以执行远程代码，提升权限，绕过安全功能限制，获得敏感信息。

CNVD 收录的相关漏洞包括： Microsoft Internet Explorer 远程内存破坏漏洞（CNVD-2015-01068、CNVD-2015-01069、CNVD-2015-01055、CNVD-2015-01056、CNVD-2015-01057、CNVD-2015-01058、CNVD-2015-01059、CNVD-2015-01060）。上述漏洞的综合评级均为“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/webinfo/show/3581

2. FreeType 产品安全漏洞

FreeType 是 FreeType 团队开发的一个基于 C 语言的、高质量的且可移植的开源字体引擎库，它可用来将字符栅格化并映射成位图以及提供其他字体相关业务的支持。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：FreeType 'cff/cf2intrp.c'拒绝服务漏洞、FreeType'_bdf_parse_glyphs'函数拒绝服务漏洞、FreeType 'type42/t42parse.c'拒绝服务漏洞、FreeType 'cff/cf2ft.c'拒绝服务漏洞、FreeType 'tt_cmap4_validate'函数拒绝服务漏洞、FreeType 拒绝服务漏洞、FreeType 'Load_SBit_Png'函数拒绝服务漏洞、FreeType 'tt_sbit_decoder_init'函数拒绝服务漏洞。上述漏洞的综合评级均为“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-2015-01044

http://www.cnvd.org.cn/flaw/show/CNVD-2015-01051

http://www.cnvd.org.cn/flaw/show/CNVD-2015-01050

http://www.cnvd.org.cn/flaw/show/CNVD-2015-01049

http://www.cnvd.org.cn/flaw/show/CNVD-2015-01048

http://www.cnvd.org.cn/flaw/show/CNVD-2015-01047

http://www.cnvd.org.cn/flaw/show/CNVD-2015-01141

http://www.cnvd.org.cn/flaw/show/CNVD-2015-01046

3. Adobe 产品安全漏洞

Adobe Flash Player 是一款 Flash 文件处理程序。本周，上述产品被披露存在未明内存破坏和空指针引用漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括： Adobe Flash Player 存在未明内存破坏漏洞（CNVD-2015-00954、CNVD-2015-00963、CNVD-2015-00957、CNVD-2015-00961、CNVD-2015-00964、CNVD-2015-01030）、Adobe Flash Player 存在未明空指针引用漏洞（CNVD-2015-00949、CNVD-2015-00941）。上述漏洞的综合评级均为“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-2015-00954

http://www.cnvd.org.cn/flaw/show/CNVD-2015-00963

http://www.cnvd.org.cn/flaw/show/CNVD-2015-00957

http://www.cnvd.org.cn/flaw/show/CNVD-2015-00961

http://www.cnvd.org.cn/flaw/show/CNVD-2015-00964

http://www.cnvd.org.cn/flaw/show/CNVD-2015-01030

http://www.cnvd.org.cn/flaw/show/CNVD-2015-00949

http://www.cnvd.org.cn/flaw/show/CNVD-2015-00941

4、Google 产品安全漏洞

Google Chrome for Android 是一款基于安卓的浏览器。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞执行任意代码或提升权限。

CNVD 收录的相关漏洞包括：Google Chrome for Android 特权提升漏洞、Google Chrome for Android 存在未明漏洞（CNVD-2015-00944）、Google Chrome for Android 内存错误引用漏洞、Google Chrome for Android 跨域绕过漏洞。上述漏洞的综合评级为“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-2015-00946

http://www.cnvd.org.cn/flaw/show/CNVD-2015-00944

http://www.cnvd.org.cn/flaw/show/CNVD-2015-00943

http://www.cnvd.org.cn/flaw/show/CNVD-2015-00945

5、Pragyan CMS SQL 注入漏洞

Pragyan CMS 是一款内容管理系统。本周，Pragyan CMS 被披露存在综合评级为“高危”的 SQL 注入漏洞。攻击者可以利用漏洞发起 SQL 注入攻击。目前，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-2015-01020

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-2015-00968	file 'readelf.c'越界读取漏洞	高	用户可以联系供应商获得补丁信息：https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-9653
CNVD-2015-00998	ZOHO ManageEngine OpManager 和 IT360 SQL 注入漏洞	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.zoho.com/portal/manageengine/helpcenter/articles/vulnerabilities-in-failoverhelperservlet
CNVD-2015-01008	NetApp OnCommand Balance 权限控制漏洞	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://kb.netapp.com/support/index?page=content&id=9010020
CNVD-2015-01002	SIPhone Enterprise PBX SQL 注入漏洞	高	暂无
CNVD-2015-01017	AVG Internet Security 权限提升漏洞	高	用户可以联系供应商获得补丁信息：http://www.avg.com/cn-zh/china-home
CNVD-2015-01014	SerVision HVG Video Gateway devices with firmware 权限提升漏洞	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.kb.cert.org/vuls/id/522460
CNVD-2015-01018	BullGuard 多个产品存在任意写入权限提升漏洞	高	用户可以联系供应商获得补丁信息：http://www.bullguard.com/about/release-notes.aspx
CNVD-2015-01019	K7 Computing 多款产品存在任意写入权限提升漏洞	高	用户可以联系供应商获得补丁信息：http://www.k7computing.co.uk/
CNVD-2015-01020	Pragyan CMS SQL 注入漏洞	高	暂无
CNVD-2015-01026	powerpc-utils 远程代码执行漏洞	高	用户可以联系供应商获得补丁信息：http://sourceforge.net/projects/power

			pc-utils/

表 3 部分高危漏洞列表

小结：2 月 10 日，微软发布了 2015 年 2 月份的月度例行安全公告，共含 9 项更新，修复了 Microsoft Windows、Internet Explorer、Office 和 Server 软件中存在的 56 个安全漏洞。其中，3 项更新的综合评级为最高级“严重”级别。利用上述漏洞，攻击者可以执行远程代码，提升权限，绕过安全功能限制，获得敏感信息。此外，FreeType、Adobe、Google 多款产品被批露存在多个安全漏洞，允许攻击者利用漏洞提升权限、执行任意代码或发起拒绝服务攻击。另外，Pragyan CMS 被披露存在一个高危零日漏洞，攻击者可利用漏洞发起 SQL 注入攻击。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、IBM 修补 Tivoli Endpoint Manager 产品漏洞

IBM Tivoli Endpoint Manager 提供了统一、实时的可视化和实施方法来向所有端点部署和管理补丁。

本周，IBM 修补了上述产品存在 HTML 注入漏洞，避免攻击者利用漏洞注入恶意脚本或 HTML 代码，获取敏感信息或劫持用户会话。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/55385

本周要闻速递

1. Facebook 用户相册任意删除漏洞

印度安全研究人员 Laxman Muthiyah 在 Facebook Graph API 上发现一个安全漏洞，攻击者可以利用该漏洞删除任意用户 Facebook 相册。Facebook Graph API 可以理解为一个可以访问 Facebook 数据的 Web 服务。该 API 提供了对人员，相册，事件等等 Facebook 对象以及这些对象之间诸如朋友，标签，分享内容等等连接之间的访问。当输入一个 URL 后，会返回一个 Json 对象。Graph API 是开发人员读写用户数据的主要方式。目前所有的 Facebook 应用程序使用的都是 Graph API。

参考链接：http://www.freebuf.com/news/59011.html

2. LG 手机认证权限绕过漏洞，可远程控制手机

安全研究人员最近发现了 LG 手机一个非常严重的漏洞，攻击者可以在用户毫无察觉的情况下控制 LG 手机，只要跟目标在同一个局域网内，就可以实施攻击，比如连了

同一个 WIFI，完全不需要物理接触。该漏洞的主要问题出在 LG 手机使用的一种叫做 On Screen Phone 的协议上，攻击者可以绕过该协议的认证机制与手机端 On Screen Phone 协议客户端建立连接。这个漏洞的 CVE 编号为：CVE-2014-8757，由 SEARCH-LAB 的安全机构发现。

参考链接：http://www.freebuf.com/news/58653.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