国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报会 员 版

2015 年 03 月 30 日-2015 年 04 月 05 日　　2015 年第 14 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 131 个，其中高危漏洞 43 个、中危漏洞 82 个、低危漏洞 6 个。上述漏洞中，可利用来实施远程攻击的漏洞有 126 个。本周收录的漏洞中，已有 119 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“pbm2120 30 缓冲区溢出漏洞”、“724CMS 存在多个信息泄露漏洞”等零日漏洞，请使用相关产品的用户注意加强防范。

重要漏洞处置情况

本周，CNVD 重点协调处置了涉及西安三才科技实业有限公司、深圳市河辰通讯技术有限公司、北京易龙天网科技有限公司、南京南软科技有限公司、中国铁建股份有限公司、上海泛微网络科技股份有限公司、迅雷公司、深圳市图美电子技术有限公司、湖南中科博华科技有限公司、华平信息技术股份有限公司、微软(中国)有限公司、上海斐讯数据通信技术有限公司、深圳市友信君德科技有限公司、深圳市惠尔顿信息技术有限公司、沈阳东软系统集成工程有限公司、浙江大华技术股份有限公司、药监局、全峰快递集团、中国国家博物馆、北京市建华实验学校、中国国际广播电台、国家超级计算天津中心、全国音乐等级考试服务平台、首旅集团网站、中国智慧城市网、中国科学技术协会、法治中国法治观察网、中国工业网、北京省际客运信息网等单位软件产品或网站信息系统存在的信息泄露、弱口令、SQL 注入、未授权访问、任意文件上传和下载、远程代码执行等漏洞。攻击者利用上述漏洞可获取用户敏感信息，上传和下载任意文件，进行未授权操作或执行任意代码。

成员单位报送漏洞统计

本周，共 4 家成员单位、合作伙伴及个人报送了本周收录的全部 131 个漏洞。报送情况如表 1 所示。其中，天融信、启明星辰、恒安嘉新等单位报送数量较多。此外，CNCERT 各分中心、乌云、漏洞盒子及白帽子向 CNVD 提交了 401 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
天融信	180	27
启明星辰	115	0
恒安嘉新	71	0
安天实验室	65	0
乌云	331	331
漏洞盒子	20	20
CNCERT 福建分中心	6	6
CNCERT 甘肃分中心	4	4
CNCERT 宁夏分中心	1	1
CNCERT 河南分中心	1	1
个人	11	11
报送总计	805	401
录入总计	131（去重）	401

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、Websense、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	Cisco	21	16%
2	Websense	21	16%
3	PHP	7	5%
4	Drupal	7	5%

5	Inductive Automation	6	5%
6	McAfee	4	3%
7	Schneider	4	3%
8	Hospira	4	3%
9	Mozilla	4	3%
10	其他	53	41%

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 131 个漏洞。其中应用程序漏洞 84 个，WEB 应用漏洞 21 个，网络设备漏洞 19 个，安全产品 5 个，操作系统漏洞 1 个，数据库漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	84
WEB 应用漏洞	21
网络设备漏洞	19
安全产品漏洞	5
操作系统漏洞	1
数据库漏洞	1

表 3 漏洞按影响类型统计表

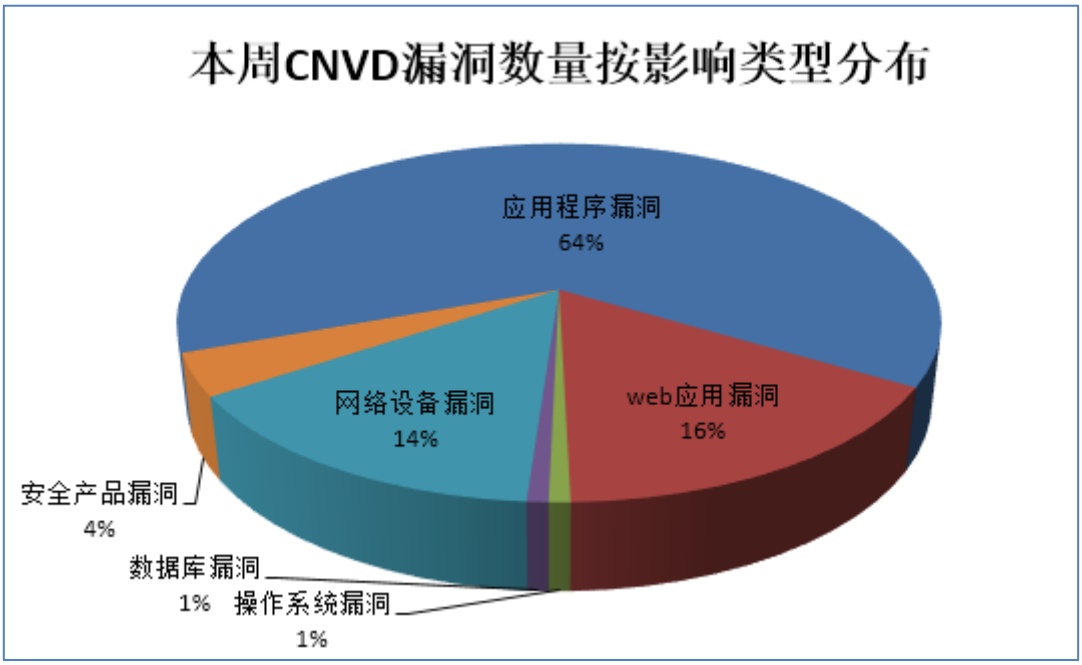

图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 21 个电信行业漏洞，2 个移动互联网行业漏洞，11 个工控系统行业漏洞（如下图表所示）。其中，“IBM DB2 Universal Database DAS 缓冲区溢出漏洞、Cisco IOS XE high-speed logging (HSL) 超大 IP 报文处理拒绝服务漏洞、Cisco IOS/IOS XE 畸形 AN 消息处理拒绝服务漏洞(CNVD-2015-02086、CNVD-2015-02085)、Cisco IOS/IOS XE 畸形 ANRA 应答报文限制绕过拒绝服务漏洞、Cisco IOS Service Discovery Gateway 拒绝服务漏洞、Cisco IOS TCP 报文拒绝服务漏洞、Cisco IOS 内存泄露拒绝服务漏洞、Cisco IOS CIP UDP 拒绝服务漏洞、Cisco IOS TCP 输入模块拒绝服务漏洞、Cisco IOS XE Layer 4 Redirect (L4R)拒绝服务漏洞、Cisco IOS XE App Nav 拒绝服务漏洞、Cisco IOS XE IPv6 报文处理拒绝服务漏洞、Cisco IOS XE Common Flow Table (CFT)畸形 IPv6 报文处理拒绝服务漏洞、Cisco IOS 畸形 IKEv2 报文处理拒绝服务漏洞(CNVD-2015-02088、CNVD-2015-02087)、Cisco IOS ICMPv4 报文拒绝服务漏洞、Google Android Bluetooth Forced Pairing 远程代码执行漏洞、Inductive Automation Ignition 暴力破解漏洞”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-2015-02041	IBM DB2 Universal Database DAS 缓冲区溢出漏洞	高	是
电信	CNVD-2015-02055	Cisco IOS XE high-speed logging (HSL) 超大 IP 报文处理拒绝服务漏洞	高	是
电信	CNVD-2015-02086	Cisco IOS/IOS XE 畸形 AN 消息处理拒绝服务漏洞(CNVD-2015-02086)	高	是
电信	CNVD-2015-02085	Cisco IOS/IOS XE 畸形 AN 消息处理拒绝服务漏洞（CNVD-2015-02085）	高	是
电信	CNVD-2015-02084	Cisco IOS/IOS XE 畸形 ANRA 应答报文限制绕过拒绝服务漏洞	高	是
电信	CNVD-2015-02082	Cisco IOS Service Discovery Gateway 拒绝服务漏洞	高	是
电信	CNVD-2015-02081	Cisco IOS XR DHCPv4 服务器拒绝服务漏洞	中	是
电信	CNVD-2015-02076	Cisco NX-OS PowerOn Auto Provisioning (POAP)任意命令执行漏洞	中	是
电信	CNVD-2015-02075	Cisco Unified Call Manager 任意文件读取漏洞	中	是
电信	CNVD-2015-02074	Cisco Wireless LAN Controller WEB 验证拒绝服务漏洞	中	是
电信	CNVD-2015-02100	Cisco IOS TCP 报文拒绝服务漏洞	高	是
电信	CNVD-2015-02099	Cisco IOS 内存泄露拒绝服务漏洞	高	是
电信	CNVD-2015-02098	Cisco IOS CIP UDP 拒绝服务漏洞	高	是
电信	CNVD-2015-02097	Cisco IOS TCP 输入模块拒绝服务漏洞	高	是

电信	CNVD-2015-02096	Cisco IOS XE Layer 4 Redirect (L4R) 拒绝服务漏洞	高	是
电信	CNVD-2015-02091	Cisco IOS XE AppNav 拒绝服务漏洞	高	是
电信	CNVD-2015-02090	Cisco IOS XE IPv6 报文处理拒绝服务漏洞	高	是
电信	CNVD-2015-02089	Cisco IOS XE Common Flow Table (CFT)畸形 IPv6 报文处理拒绝服务漏洞	高	是
电信	CNVD-2015-02088	Cisco IOS 畸形 IKEv2 报文处理拒绝服务漏洞(CNVD-2015-02088)	高	是
电信	CNVD-2015-02083	Cisco IOS ICMPv4 报文拒绝服务漏洞	高	是
电信	CNVD-2015-02087	Cisco IOS 畸形 IKEv2 报文处理拒绝服务漏洞（CNVD-2015-02087）	高	是
移动互联网	CNVD-2015-02033	Google Android Bluetooth Forced Pairing 远程代码执行漏洞	高	是
移动互联网	CNVD-2015-02034	Dropbox SDK for Android 安全绕过漏洞	中	是
工控系统	CNVD-2015-02056	Schneider Electric InduSoft Web Studio 和 InTouch Machine Edition 信息泄露漏洞（CNVD-2015-02056）	低	是
工控系统	CNVD-2015-02057	Schneider Electric InduSoft Web Studio 和 InTouch Machine Edition 信息泄露漏洞（CNVD-2015-02057）	低	是
工控系统	CNVD-2015-02058	Schneider Electric InduSoft Web Studio 和 InTouch Machine Edition 信息泄露漏洞（CNVD-2015-02058）	中	是
工控系统	CNVD-2015-02059	Schneider Electric InduSoft Web Studio 和 InTouch Machine Edition 信息泄露漏洞（CNVD-2015-02059）	低	是
工控系统	CNVD-2015-02153	Inductive Automation Ignition 跨站脚本漏洞	中	是
工控系统	CNVD-2015-02154	Inductive Automation Ignition 信息泄露漏洞（CNVD-2015-02154）	中	是
工控系统	CNVD-2015-02155	Inductive Automation Ignition 信息泄露漏洞（CNVD-2015-02155）	中	是
工控系统	CNVD-2015-02156	Inductive Automation Ignition 无效会话过期漏洞	中	是
工控系统	CNVD-2015-02157	Inductive Automation Ignition 安全绕过漏洞	中	是
工控系统	CNVD-2015-02158	Inductive Automation Ignition 暴力破解漏洞	高	是
工控系统	CNVD-2015-02165	Ecava IntegraXor DLL 漏洞	中	是

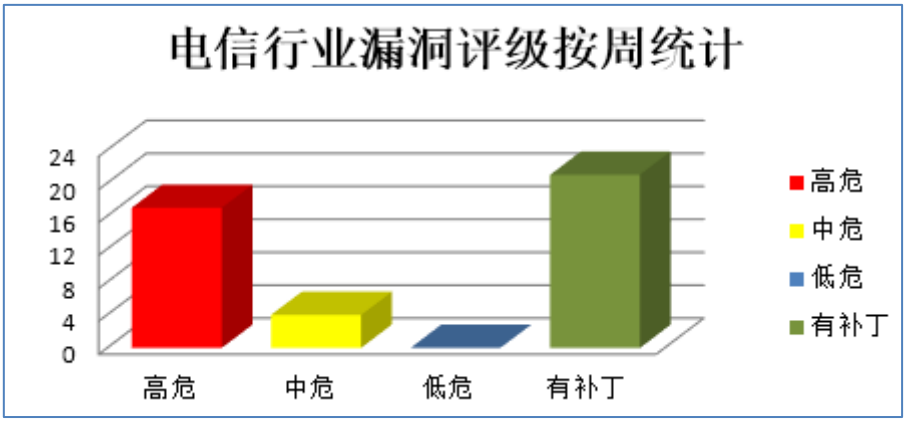

图 1 电信行业漏洞统计

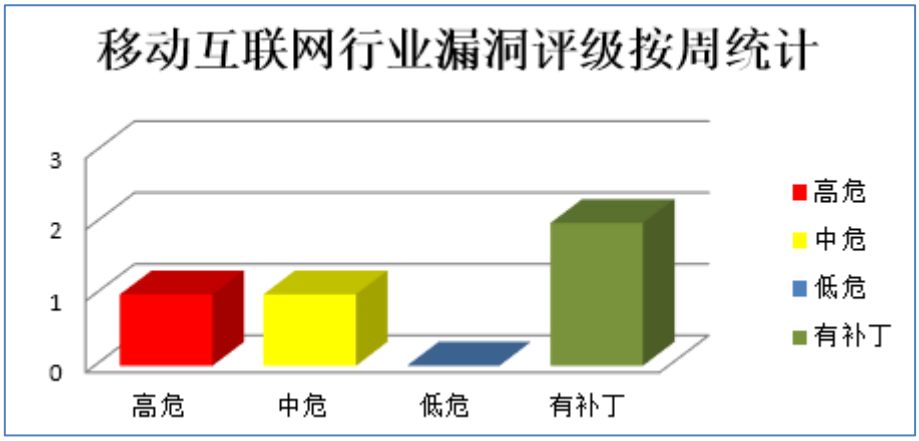

图 2 移动互联网行业漏洞统计

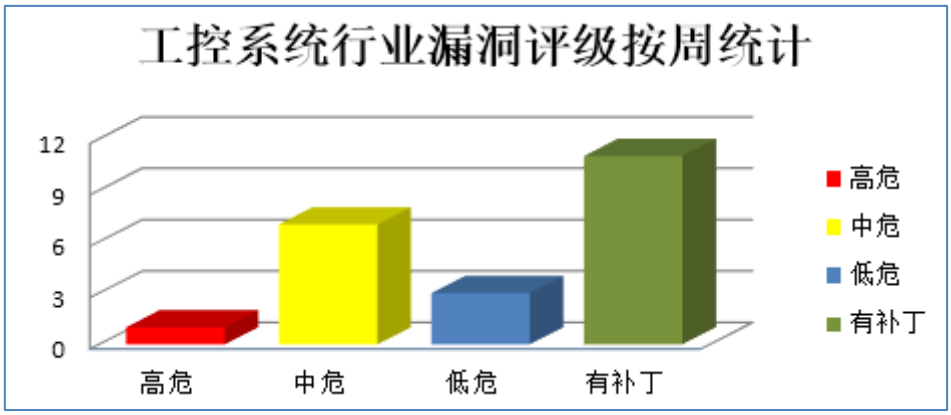

图 3 工控系统行业漏洞统计

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、Cisco 产品安全漏洞

Cisco IOS 是一款流行的 Internet 操作系统。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：Cisco IOS Service Discovery Gateway 拒绝服务漏洞、Cisco IOS XE AppNav 拒绝服务漏洞、Cisco IOS XE IPv6 报文处理拒绝服务漏洞、Cisco IOS TCP 报文拒绝服务漏洞、Cisco IOS 内存泄露拒绝服务漏洞、Cisco IOS CIP UDP 拒绝服务漏洞、Cisco IOS TCP 输入模块拒绝服务漏洞、Cisco IOS XE Layer 4 Redirect (L4R)拒绝服务漏洞。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-2015-02082
http://www.cnvd.org.cn/flaw/show/CNVD-2015-02091
http://www.cnvd.org.cn/flaw/show/CNVD-2015-02090
http://www.cnvd.org.cn/flaw/show/CNVD-2015-02091
http://www.cnvd.org.cn/flaw/show/CNVD-2015-02100
http://www.cnvd.org.cn/flaw/show/CNVD-2015-02099
http://www.cnvd.org.cn/flaw/show/CNVD-2015-02098
http://www.cnvd.org.cn/flaw/show/CNVD-2015-02097
http://www.cnvd.org.cn/flaw/show/CNVD-2015-02096

2、 Websese 产品安全漏洞

Websense TRITON 是统一内容架构保护数据安全。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、进行跨站攻击或执行未授权操作。

CNVD 收录的相关漏洞包括：Websense TRITON AP-EMAIL 存在未明漏洞、Websense TRITON AP-EMAIL 存在未明信息泄露漏洞、Websense TRITON V-Series appliances SVM 任意文件上传漏洞、Websense TRITON AP-EMAIL 存在未明跨站脚本漏洞、Websense TRITON AP-EMAIL PEM 存在多个跨站请求伪造漏洞、Websense TRITON AP-EMAIL mail 服务器明文密码漏洞、Websense TRITON V-Series appliances 跨站请求伪造漏洞、Websense TRITON AP-DATA 存在多个跨站脚本漏洞。其中，“Websense TRITON AP-EMAIL 存在未明漏洞、Websense TRITON AP-EMAIL 存在未明信息泄露漏洞、Websense TRITON V-Series appliances SVM 任意文件上传漏洞”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-2015-02116
http://www.cnvd.org.cn/flaw/show/CNVD-2015-02125
http://www.cnvd.org.cn/flaw/show/CNVD-2015-02120
http://www.cnvd.org.cn/flaw/show/CNVD-2015-02124
http://www.cnvd.org.cn/flaw/show/CNVD-2015-02123
http://www.cnvd.org.cn/flaw/show/CNVD-2015-02122

http://www.cnvd.org.cn/flaw/show/CNVD-2015-02121

http://www.cnvd.org.cn/flaw/show/CNVD-2015-02119

3、McAfee 产品安全漏洞

McAfee Data Loss Prevention Endpoint(DLPe)是美国迈克菲(McAfee)公司的一套集成式终端数据保护解决方案。本周，上述产品被披露存在信息泄露、跨站脚本漏洞、跨站请求伪造和拒绝服务漏洞。攻击者可利用漏洞获取敏感信息、进行跨站脚本或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：McAfee Data Loss Prevention Endpoint EPO 扩展跨站脚本漏洞、McAfee Data Loss Prevention Endpoint EPO 扩展信息泄露漏洞、McAfee Data Loss Prevention Endpoint EPO 扩展跨站请求伪造漏洞、McAfee Data Loss Prevention Endpoint EPO 扩展拒绝服务漏洞。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-2015-02077

http://www.cnvd.org.cn/flaw/show/CNVD-2015-02078

http://www.cnvd.org.cn/flaw/show/CNVD-2015-02079

http://www.cnvd.org.cn/flaw/show/CNVD-2015-02080

4、Schneider Electric 产品安全漏洞

Schneider Electric InduSoft Web Studio 和 InTouch Machine Edition 都是法国施耐德电气（Schneider Electric）公司的一个嵌入式 HMI 软件包。本周，上述产品被披露存在信息泄露漏洞。攻击者可利用漏洞获取敏感信息。

CNVD 收录的相关漏洞包括：Schneider Electric InduSoft Web Studio 和 InTouch Machine Edition 信息泄露漏洞（CNVD-2015-02059、CNVD-2015-02058、CNVD-2015-02057、CNVD-2015-02056）。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-2015-02059

http://www.cnvd.org.cn/flaw/show/CNVD-2015-02058

http://www.cnvd.org.cn/flaw/show/CNVD-2015-02057

http://www.cnvd.org.cn/flaw/show/CNVD-2015-02056

5、pbm212030 缓冲区溢出漏洞

pbm212030 是一套便携式位图格式（PBM）图像处理工具。本周，pbm212030 被披露存在综合评级为“高危”的缓冲区溢出漏洞。攻击者利用该漏洞可借助特制的 PBM 图像造成拒绝服务（崩溃），或执行任意代码。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-2015-02066

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-2015-02048	Citrix Command Center 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这个安全问题，请到厂商的主页下载：http://support.citrix.com/article/CTX200584
CNVD-2015-02067	MyBB 存在未明漏洞（CNVD-2015-02067）	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://blog.mybb.com/2015/02/15/mybb-1-8-4-released-feature-update-security-maintenance-release/
CNVD-2015-02115	Byzanz GIF 编码拒绝服务漏洞	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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=778261
CNVD-2015-02114	PHP ZIP 扩展_zip_cdir_new 函数整数溢出漏洞	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://git.php.net/?p=php-src.git;a=commit;h=ef8fc4b53d92fbfcd8ef1abbd6f2f5fe2c4a11e5
CNVD-2015-02112	PHP phar_rename_archive 函数内存错误引用漏洞	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://git.php.net/?p=php-src.git;a=commit;h=b2cf3f064b8f5efef89bb084521b61318c71781b
CNVD-2015-02111	PHP calendar 扩展整数溢出漏洞	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：https://github.com/MegaManSec/php-src/commit/a538d2f5605798422f2746636ecdc300f8ebcaa1
CNVD-2015-02128	PHP process_nested_data 函数内存错误引用漏洞	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://gist.github.com/smalyshev/eea9eafc7c88a4a6d10d
CNVD-2015-02133	setroubleshoot 任意命令执行漏洞	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：https://fedorahosted.org/setroubleshoot/wiki/SETroubleShoot%20Overvie

			w
CNVD-2015-02142	Dulwich 缓冲区溢出漏洞	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：https://pypi.python.org/packages/source/d/dulwich/dulwich-0.9.9.tar.gz
CNVD-2015-02137	HP Operations Orchestration 安全绕过漏洞	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：https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01389709?lang=en&cc=us&hpappid=OSP

表 3 部分高危漏洞列表

小结：本周，Cisco 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，Websense、McAfee、Schneider Electric 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、进行跨站攻击、执行未授权操作或发起拒绝服务攻击。另外，pbm212030 被披露存在一个高危零日漏洞，攻击者利用该漏洞可借助特制的 PBM 图像造成拒绝服务（崩溃），或执行任意代码。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、Apache 修补 Subversion 产品漏洞

Subversion 是一款开源多用户版本控制系统，支持非 ASCII 文本和二进制数据。

本周，Apache 修补了上述产品存在的 svn:author 属性值欺骗和拒绝服务漏洞，避免攻击者利用漏洞修改 svn:author 属性值或发起拒绝服务攻击。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网络安全事件。

补丁下载链接：http://www.cnvd.org.cn/patchInfo/show/56910

http://www.cnvd.org.cn/patchInfo/show/56914

本周重要漏洞验证信息

本周，CNVD 核实和发布以下重要漏洞验证信息。

1、Fiyo CMS 存在多个 SQL 注入漏洞

验证描述

Fiyo CMS 是小型的商务电话服务及移动合作工具。

Fiyo CMS 存在多个 SQL 注入漏洞。攻击者可利用漏洞获取数据库敏感信息。

验证信息

http://192.168.248.132/fiyo/dapur/index.php?app=user&act=edit&id=1[sqli]

信息提供者

恒安嘉新（北京）科技有限公司

2、WordPress 插件 WPML 存在未明漏洞

验证描述

WordPress 是 WordPress 软件基金会的一套使用 PHP 语言开发的博客平台，该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。WPML 是其中的一个多语言插件。

WordPress WPML 插件 3.1.9 之前版本中存在安全漏洞，该漏洞源于程序未能正确处理请求中的多个操作。远程攻击者可通过发送特制的请求利用该漏洞绕过随机数检查，执行任意操作。

验证信息

<form method=POST action=" https://YOUR.WORDPRESS.BLOG/?icl_ajx_action=toggle-subscription_10&nonce=1234567890 "> <input type=hidden name="icl_ajx_action" value="icl_save_language_negotiation_type"> <input type=hidden name="_icl_nonce" value="(ignored)"> <input type=hidden name="icl_language_negotiation_type" value="1"> <input type=hidden name="use_directory" value="1"> <input type=hidden name="show_on_root" value="html_file"> <input type=hidden name="root_html_file_path" value="/etc/passwd"> <input type=submit> </form>

信息提供者

恒安嘉新（北京）科技有限公司

注：以上验证信息(方法)可能带有攻击性，仅供安全研究之用。请广大用户加强对漏洞的防范工作，尽快下载相关补丁。

本周要闻速递

1. 白帽子发现 YouTube 任意视频删除漏洞

俄罗斯安全研究员 Kamil Hismatullin 近日在寻找 YouTube 造物主工作室跨站点脚本（XSS）及跨站点请求伪造（CSRF）漏洞的时候，偶然发现了一个可以删除任何视频的逻辑漏洞，攻击者只需针对任一会话令牌发送一条任何视频的识别代码就可以删除这一视频。也就是说，攻击者可以利用该漏洞轻松地删除任何 YouTube 视频。

参考链接：http://www.freebuf.com/news/62933.html

2. Java 官网曝本地文件包含（LFI）漏洞

意大利安全研究人员 Christian Galeone 最近发现 Java JDK7 网站上存在目录浏览（Path Traversal）/本地文件包含（Local File Inclusion）漏洞。研究人员测试，通过漏洞可读取服务器端敏感数据（Important Sensible Server-Side Data）也包含在内。如果该漏洞被攻击者利用的话，不仅会泄露 web 服务器敏感信息，还可以读取应用程序源码。

参考链接：http://www.freebuf.com/news/62764.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