

信息安全漏洞周报

2014 年 11 月 24 日-2014 年 11 月 30 日

2014 年第 48 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 138 个，其中高危漏洞 47 个、中危漏洞 82 个、低危漏洞 9 个。上述漏洞中，可利用来实施远程攻击的漏洞有 123 个。本周收录的漏洞中，已有 100 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“Hikvision DVR DS-7204 RTSP 请求头处理远程缓冲区溢出漏洞”、“WebsiteBaker 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 138 个漏洞。报送情况如表 1 所示。其中，天融信、恒安嘉新、绿盟科技、安天实验室等单位报送数量较多。此外，CNCERT 各分中心、北京数字认证股份有限公司、北京安信天行科技有限公司、High-Tech Bridge Security Research Lab 及白帽子向 CNVD 提交了 58 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	131	0
恒安嘉新	119	0
绿盟科技	102	0
安天实验室	88	0
启明星辰	74	0
奇虎 360	3	3

北京数字认证股份有限公司	1	1
北京安信天行科技有限公司	6	6
High-Tech Bridge Security Research Lab	1	1
CNCERT 江西分中心	10	10
CNCERT 山西分中心	8	8
CNCERT 福建分中心	6	6
CNCERT 陕西分中心	6	6
CNCERT 甘肃分中心	5	5
CNCERT 河北分中心	3	3
CNCERT 四川分中心	2	2
个人	7	7
报送总计	572	58
录入总计	138（去重）	58

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 WordPress、Drupal、Asterisk 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	WordPress	19	14%
2	Drupal	10	7%
3	Asterisk	8	6%
4	Cisco	5	4%
5	IBM	4	3%
6	phpMyAdmin	4	3%
7	Google	3	2%
8	Linux	3	2%
9	Apple	2	1%
10	其他	80	58%

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 138 个漏洞。其中应用程序漏洞 69 个，WEB 应用漏洞 45 个，网络设备漏洞 13 个，操作系统漏洞 9 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	69
WEB 应用漏洞	45
网络设备漏洞	13
操作系统漏洞	9
安全产品漏洞	2

表 3 漏洞按影响类型统计表

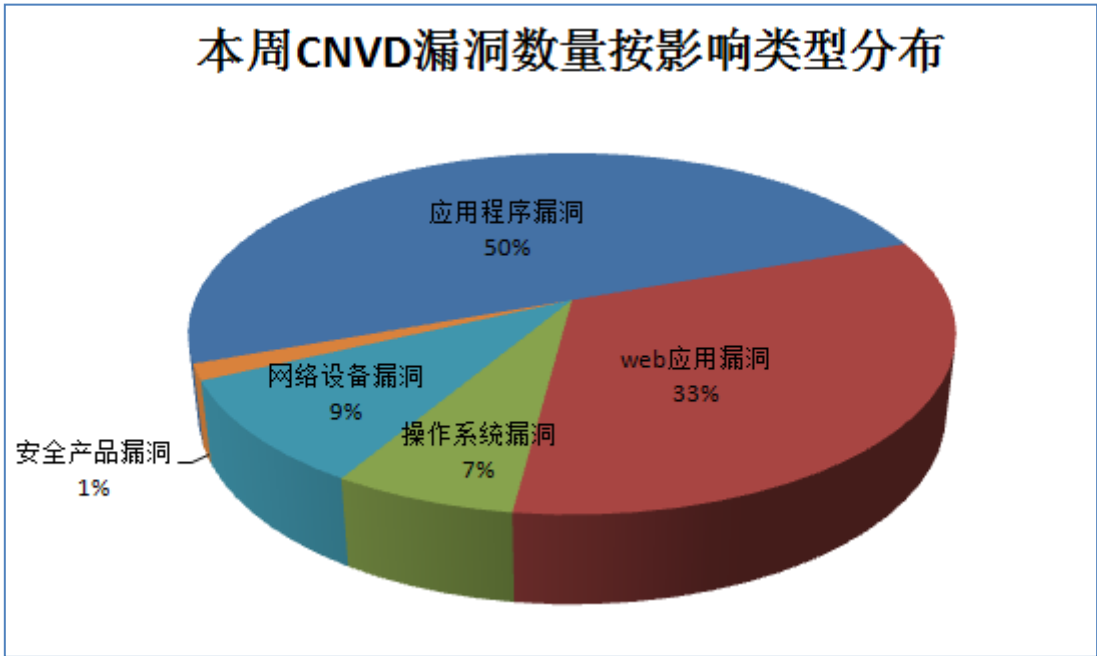


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 12 个电信行业漏洞，5 个移动互联网漏洞，1 个工控系统行业漏洞（如下图表所示）。其中，“多个 Asterisk 产品 ConfBridge Dialplan Functions 远程权限提升漏洞、多个 Asterisk 产品'funcs/func_db.c'远程权限提升漏洞、Google Android Settings 应用权限提升漏洞、Google Android WAPPushManager 模块 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-2014-08492	多个 Asterisk 产品 ConfBridge Dialplan	高	是

		Functions 远程权限提升漏洞		
电信	CNVD-2014-08493	多个 Asterisk 产品'funcs/func_db.c'远程权限提升漏洞	高	是
电信	CNVD-2014-08494	Asterisk Open Source PJSIP 通道驱动拒绝服务漏洞	中	是
电信	CNVD-2014-08489	Asterisk 'res_pjsip_refer'模块拒绝服务漏洞	中	是
电信	CNVD-2014-08490	多个 Asterisk 产品 ConfBridge 拒绝服务漏洞	中	是
电信	CNVD-2014-08491	多个 Asterisk 产品访问控制列表安全绕过漏洞	中	是
电信	CNVD-2014-08495	Asterisk Open Source 'res_pjsip_acl'模块安全绕过漏洞	中	是
电信	CNVD-2014-08515	Cisco IOS XR Software LISP TCP 会话拒绝服务漏洞	中	是
电信	CNVD-2014-08509	TP-Link TL-WR740N 'PingIframeRpm.htm'拒绝服务漏洞	中	否
电信	CNVD-2014-08521	Asterisk Open Source PJSIP 通道驱动拒绝服务漏洞	中	是
电信	CNVD-2014-08544	Cisco IOS XR Software TCP 会话拒绝服务漏洞	中	是
电信	CNVD-2014-08551	IBM WebSphere Portal 跨站脚本漏洞(CNVD-2014-08551)	低	是
移动互联网	CNVD-2014-08458	Apple iOS 和 TV 本地代码执行漏洞	中	是
移动互联网	CNVD-2014-08482	Apple iPhone 沙盒安全绕过漏洞	中	否
移动互联网	CNVD-2014-08533	Google Android 'handleSmsSent()'函数信息泄露漏洞	中	是
移动互联网	CNVD-2014-08534	Google Android Settings 应用权限提升漏洞	高	是
移动互联网	CNVD-2014-08535	Google Android WAPPushManager 模块 SQL 注入漏洞	高	是
工控系统	CNVD-2014-08577	MatrikonOPC DNP3 OPC Server 拒绝服务漏洞	中	是

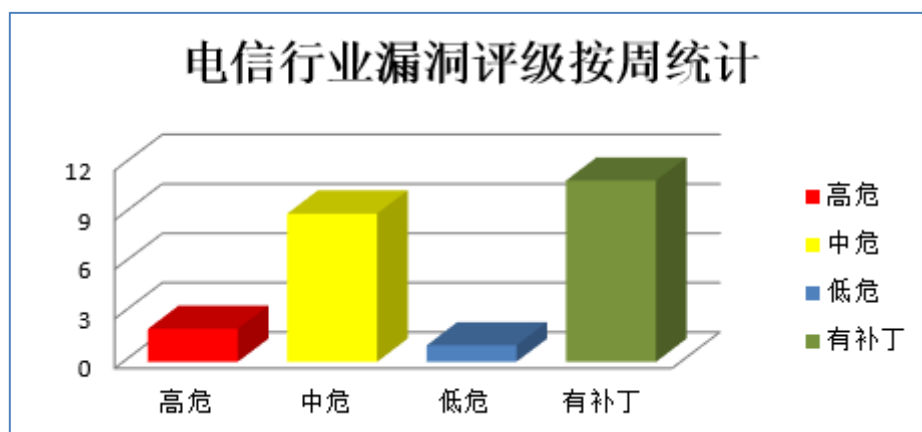


图 1 电信行业漏洞统计

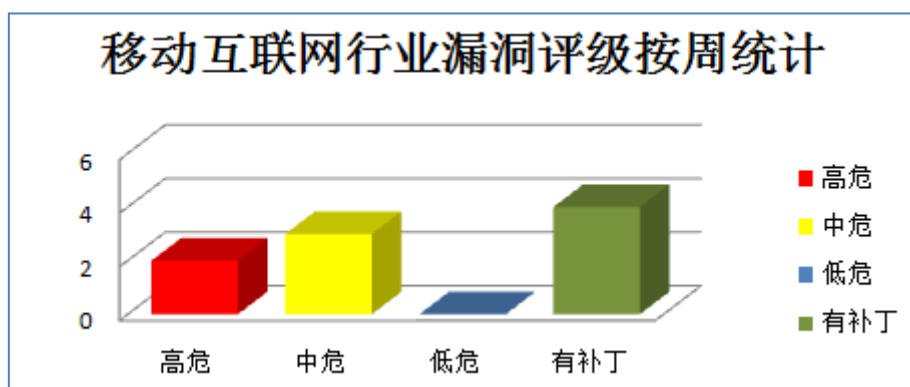


图 2 移动互联网行业漏洞统计

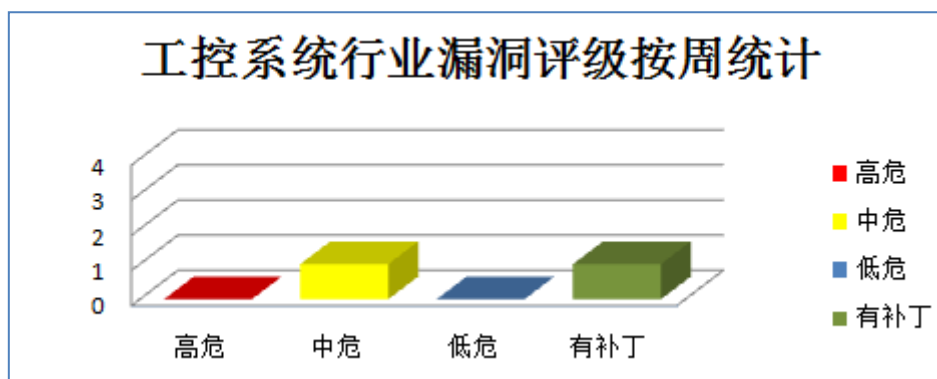


图 3 工控系统行业漏洞统计

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 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 OpenH264 是美国思科（Cisco）公司的一款开源的 H.264（视频编解码技术）编码和解码器。Cisco IOS XR 是美国思科（Cisco）公司的 IOS 软件系列中的

一套完全模块化、分布式的网络操作系统。本周，上述产品被披露存在内存错误引用漏洞、缓冲区溢出和拒绝服务漏洞，攻击者可利用漏洞发起拒绝服务或执行任意代码。

CNVD 收录的相关漏洞包括：Cisco Adaptive Security Appliance (ASA) Software 拒绝服务漏洞（CNVD-2014-08558）、Cisco OpenH264 'decode_slice.cpp'内存错误引用漏洞、Cisco OpenH264 'decode.cpp'缓冲区溢出漏洞、Cisco IOS XR Software TCP 会话拒绝服务漏洞、Cisco IOS XR Software LISP TCP 会话拒绝服务漏洞。其中“Cisco OpenH264 'decode_slice.cpp'内存错误引用漏洞、Cisco OpenH264 'decode.cpp'缓冲区溢出漏洞”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-2014-08558>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08556>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08555>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08544>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08515>

2、Drupal 产品安全漏洞

Drupal 是一套用 PHP 语言开发的免费、开源的内容管理系统。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、执行未授权操作、进行跨站脚本攻击或发起拒绝服务。

CNVD 收录的相关漏洞包括：Drupal Commerce 模块信息泄露漏洞、Drupal Ubercart 模块信息泄露漏洞、Drupal Protected Pages 模块安全绕过漏洞、Drupal Secure Password Hashes 模块拒绝服务漏洞、Drupal Node Field 模块跨站脚本漏洞、Drupal Form Builder 模块跨站脚本漏洞、Drupal Commerce Authorize.Net SIM/DPM Payment Methods 访问绕过漏洞、Drupal Tournament 模块存在 HTML 注入漏洞。其中“Drupal Secure Password Hashes 模块拒绝服务漏洞”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-2014-08470>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08471>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08443>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08444>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08445>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08446>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08447>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08448>

3、WordPress 产品安全漏洞

WordPress 是一种使用 PHP 语言开发的博客平台,用户可以在支持 PHP 和 MySQL 数据库的服务器上架设自己的网志。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、执行任意代码或进行跨站脚本攻击。

CNVD 收录的相关漏洞包括: WordPress 插件 Google Doc Embedder 'google-document-embedder/view.php' SQL 注入漏洞、WordPress 插件 wpDataTables 存在多个文件上传漏洞、WordPress 插件 wpDataTables 'wpdatatables.php' SQL 注入漏洞、WordPress 插件 SP Project & Document Manager 'ajax.php'存在多个 SQL 注入漏洞、WordPress 插件 CM Download Manager 远程 PHP 代码执行漏洞、WordPress 插件 DukaPress 路径泄露漏洞、WordPress media-playlists 功能跨站脚本漏洞、WordPress 跨站脚本漏洞 (CNVD-2014-08553)。其中,除“WordPress 插件 DukaPress 路径泄露漏洞、WordPress media-playlists 功能跨站脚本漏洞、WordPress 跨站脚本漏洞 (CNVD-2014-08553)”外,其余漏洞的综合评级为“高危”。目前,厂商已经发布了修补程序。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-2014-08564>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08548>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08529>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08525>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08442>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08554>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08552>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08553>

4、Google 产品安全漏洞

Android 是基于 Linux 开放性内核的操作系统,是 Google 公司在 2007 年 11 月 5 日公布的手机操作系统。本周,上述产品被披露存在 SQL 注入、信息泄露和权限提升漏洞,攻击者可利用漏洞获取敏感信息或提升权限。

CNVD 收录的相关漏洞包括: Google Android WAPPushManager 模块 SQL 注入漏洞、Google Android Settings 应用权限提升漏洞、Google Android 'handleSmsSent()'函数信息泄露漏洞。其中“Google Android WAPPushManager 模块 SQL 注入漏洞、Google Android Settings 应用权限提升漏洞”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-2014-08535>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08534>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08533>

5、GNU patch 'pch.c'整数溢出漏洞

GNU 核心工具 (Coreutils) 是 GNU 操作系统所使用的基本文件、shell 和文本操控工具。本周,GNU patch 被披露存在综合评级为“高危”的整数溢出漏洞。攻击者可利

用漏洞在应用程序上下文中执行任意代码。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-2014-08563>

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-2014-08441	PCRE 'pcre_exec.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://vcs.pcre.org
CNVD-2014-08469	Lantronix xPrintServer 任意命令执行漏洞	高	暂无
CNVD-2014-08466	VldPersonals 存在多个 SQL 注入漏洞	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.vldpersonals.com/blog/maintenance-update-2-7-1-964/
CNVD-2014-08478	Zoph 存在多个漏洞	高	暂无
CNVD-2014-08479	Proticaret E-Commerce Script 'code'参数 SQL 注入漏洞	高	暂无
CNVD-2014-08481	Amazon Fire Phone 存在多个未明漏洞	高	暂无
CNVD-2014-08518	Wibu-Systems CodeMeter 本地权限提升漏洞	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.wibu.com/en/codemeter.html
CNVD-2014-08513	Mozilla Firefox WEBM 文件处理整数溢出漏洞	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://www.mozilla.org/en-US/
CNVD-2014-08510	RobotStats 'profile.php' 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： http://www.robotstats.com/en/
CNVD-2014-08508	FluxBB 'profile.php' 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： http://www.fluxbb.org

表 3 部分高危漏洞列表

小结：本周，Cisco 产品被批露存在内存错误引用、缓冲区溢出和拒绝服务漏洞，攻击者可利用漏洞发起拒绝服务攻击或执行任意代码。此外，Drupal、WordPress、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获取敏感信息、执行任意代码、发起拒绝服务、执行未经授权操作或者植入跨站脚本。另外，GNU patch 被披露存在一个高危零日漏洞。攻击者可利用漏洞在应用程序上下文中执行任意代码。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、Linux 修补 Kernel 产品漏洞

Linux Kernel 是 Linux 操作系统的内核。

本周，Linux 修补了上述产品存在的拒绝服务和安全绕过漏洞，避免攻击者利用漏洞发起拒绝服务攻击或绕过某些安全限制，执行未经授权的操作。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/52139>

<http://www.cnvd.org.cn/patchInfo/show/52140>

本周要闻速递

1. Adobe 紧急发布 Flash 播放器计划外安全更新

据安全厂商 F-Secure 称，在 10 月 14 日 Flash 发布补丁修复之后，黑客利用 Windows、Mac、和 Linux 系统上的 Flash 播放器高危漏洞（CVE-2014-8439）进行攻击的形势有所缓和，但没过多久法国的研究员 Kafeine 又在该恶意软件中发现了 Flash 播放器的最新漏洞利用程序。由于 Flash 在处理内存指示器的过程中存在可以被攻击的弱点，所以攻击者可以利用该漏洞在受害者机器上执行任意的代码。

参考链接：<http://www.freebuf.com/news/52953.html>

2. WordPress 4.0 以下版本存在跨站脚本漏洞

WordPress 是著名的开源 CMS（内容管理）系统。近日，在 4.0 版本以下的 Wordpress 被发现存在跨站脚本漏洞（XSS），新版本的 Wordpress 已经修复了这些问题。据调查得知全球有 86% 的 Wordpress 网站都感染了这一漏洞，为了安全起见，建议尽早更新到 WP 新版本。

参考链接：<http://www.freebuf.com/news/52895.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