

信息安全漏洞周报

2014 年 12 月 29 日-2015 年 01 月 04 日

2015 年第 1 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 85 个，其中高危漏洞 16 个、中危漏洞 61 个、低危漏洞 8 个。上述漏洞中，可利用来实施远程攻击的漏洞有 82 个。本周收录的漏洞中，已有 72 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“Notepad++ 存在未明缓冲区溢出漏洞”、“Info-ZIP UnZip 远程堆缓冲区溢出漏洞”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 5 家成员单位、各分中心及个人报送了本周收录的全部 85 个漏洞。报送情况如表 1 所示。其中，奇虎 360、天融信、绿盟科技、恒安嘉新、安天实验室等单位报送数量较多。此外，CNCERT 各分中心及白帽子向 CNVD 提交了 1232 个原创漏洞(注：奇虎 360 提交漏洞包含其“库带计划”中部分存量漏洞)。

报送单位或个人	漏洞报送数量	原创漏洞数量
奇虎 360	1220	1220
天融信	79	0
绿盟科技	48	0
恒安嘉新	38	0
安天实验室	13	0
CNCERT 甘肃分中心	5	5

CNCERT 河南分中心	1	1
CNCERT 上海分中心	1	1
CNCERT 宁夏分中心	1	1
CNCERT 福建分中心	1	1
个人	3	3
报送总计	1410	1232
录入总计	85（去重）	1232

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、WordPress、Cisco 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	26	31%
2	WordPress	9	11%
3	Cisco	5	6%
4	GnuPG	4	5%
5	Huawei	4	5%
6	OSClass	3	4%
7	Libsndfile	2	2%
8	NetIQ	2	2%
9	PHP	2	2%
10	其他	28	32%

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 85 个漏洞。其中应用程序漏洞 56 个，WEB 应用漏洞 17 个，网络设备漏洞 8 个，操作系统漏洞 2 个，安全产品漏洞 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	56
WEB 应用漏洞	17
网络设备漏洞	8

操作系统漏洞	2
安全产品漏洞	1
数据库漏洞	1

表 3 漏洞按影响类型统计表

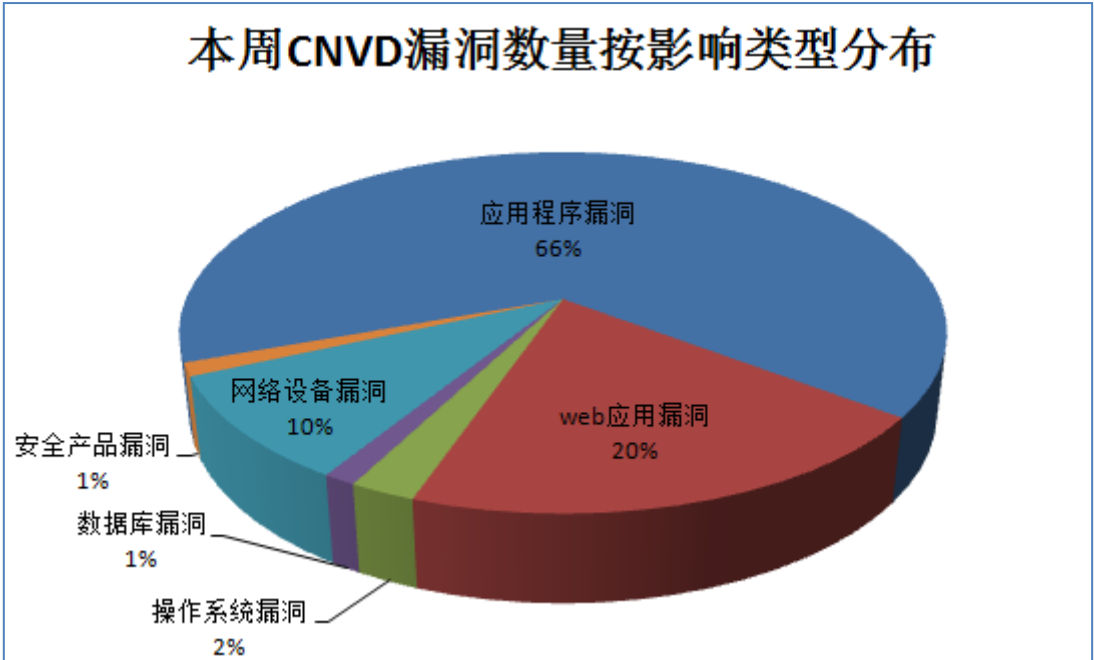


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 9 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）。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2014-09184	IBM WebSphere Application Server 点击劫持漏洞	中	是
电信	CNVD-2014-09183	IBM WebSphere Application Server 跨站脚本漏洞（CNVD-2014-09183）	中	是
电信	CNVD-2014-09182	IBM WebSphere Application Server 目录遍历漏洞（CNVD-2014-09182）	中	是
电信	CNVD-2014-09181	IBM WebSphere Application Server 信息泄露漏洞（CNVD-2014-09181）	中	是
电信	CNVD-2014-09212	IBM WebSphere Portal 跨站脚本漏洞(CNVD-2014-09212)	中	是
电信	CNVD-2014-09209	IBM WebSphere Portal XML 注入漏洞	中	是
电信	CNVD-2014-09211	IBM WebSphere Portal 跨站脚本漏洞(CNVD-2014-09211)	中	是
电信	CNVD-2014-09225	Huawei WS318 预测随机数发生器漏洞	中	是
电信	CNVD-2015-00013	Netcore(Netis)路由器 53413/UDP 后门服	高	否

		务漏洞		
移动互联网	CNVD-2014-09220	TSUTAYA application 任意命令执行漏洞	中	是
工控系统	CNVD-2014-09234	Koha 存在多个跨站脚本漏洞	中	是

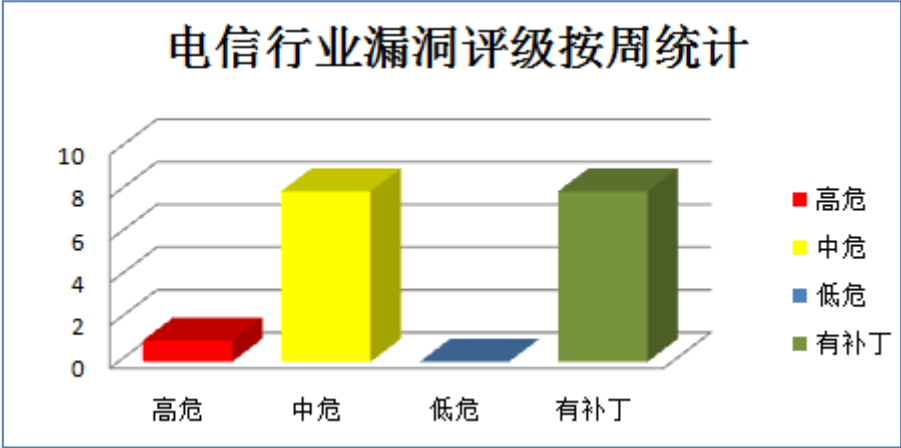


图 1 电信行业漏洞统计

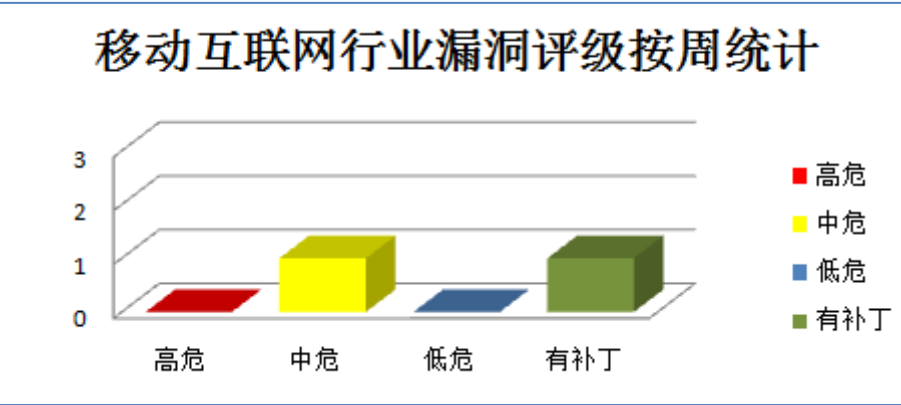


图 2 移动互联网行业漏洞统计

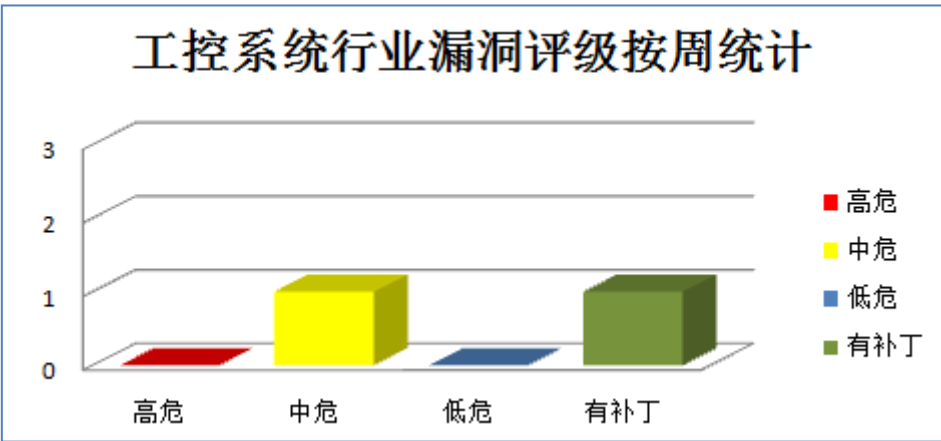


图 3 工控系统行业漏洞统计



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、IBM 产品安全漏洞

IBM Security Access Manager 软件是高度可扩展的用户认证、授权和 Web SSO 解决方案，用于在各种 Web 和应用资源上实施安全策略，集中管理在线门户网站。本周，上述产品被披露存在信息泄露、拒绝服务和安全绕过漏洞，攻击者可利用漏洞获取敏感信息、发起拒绝服务和绕过安全机制获得访问权限。

CNVD 收录的相关漏洞包括：IBM Security Access Manager 信息泄露漏洞（CNVD-2014-09200、CNVD-2014-09198、CNVD-2014-09199、CNVD-2014-09194、CNVD-2014-09196）、IBM Security Access Manager 拒绝服务漏洞（CNVD-2014-09201、CNVD-2014-09193）、IBM Security Access Manager 安全机制绕过漏洞。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-2014-09200>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09198>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09199>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09194>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09196>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09201>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09193>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09203>

2、Cisco 产品安全漏洞

Cisco Meraki MS MRMX 是思科公司的云管理无线网络设备。Cisco IronPort Email Security Appliance 是架构多层邮件安全管理工具。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、执行任意命令或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco Meraki MS MRMX 信息泄露漏洞、Cisco Meraki MS MRMX 任意命令执行漏洞、Cisco Meraki MS MRMX 存在 shell 获取漏洞、Cisco Meraki MS MRMX 任意固件安装漏洞、Cisco IronPort Email Security Appliance 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-2014-09189>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09190>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09191>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09192>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09187>

3、Huawei 产品安全漏洞

Huawei USG9560/9520/9580 是高端 10Gb 防火墙产品。华为 WS318 是一款无线路由器。Tecal E9000 融合架构刀片服务器是华为公司推出的新一代功能强大的基础设施平台。Huawei Tecal RH Series 是机架式服务器产品。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、提升权限或执行任意代码。

CNVD 收录的相关漏洞包括：Huawei Tecal E9000 Chassis IPMICommand 处理权限提升漏洞、Huawei Tecal RH Series 存在多个漏洞、Huawei USG9560/9520/9580 Main Processing Unit (MPU)内存泄露漏洞、Huawei WS318 预测随机数发生器漏洞。其中“Huawei Tecal E9000 Chassis IPMICommand 处理权限提升漏洞、Huawei Tecal RH Series 存在多个漏洞”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-2014-09226>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09227>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09224>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-09225>

4、GnuPG 产品安全漏洞

GnuPG 是一个 Python 模块允许，从 Python 程序方便地使用 GnuPG 的密钥管理，加密和签名功能。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：Gnupg2 '/scd/command.c' Double Free 拒绝服务漏洞、Gnupg2 '/sm/minip12.c' Double Free 拒绝服务漏洞、Gnupg2 'dirmngr/ldapsrv.c' Double Free 拒绝服务漏洞、Gnupg2 'sm/gpgsm.c' Double Free 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-2015-00019>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00018>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00017>
<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00016>

5、Info-ZIP UnZip 远程堆缓冲区溢出漏洞

unzip 是在 Unix 下对.zip 文件格式进行解压的工具。本周，Info-ZIP UnZip 被披露存在综合评级为“高危”的堆缓冲区溢出漏洞。攻击者可以利用此漏洞在应用上下文中执行任意代码或发起拒绝服务。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-2014-09223>

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	漏洞名称	综合	修复方式
--------	------	----	------

号		评级	
CNVD-2014-09239	IBM Security AppScan Enterprise 任意命令执行漏洞	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://xforce.iss.net/xforce/xfdb/96723
CNVD-2014-09241	IBM Security AppScan Enterprise 任意代码执行漏洞	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-01.ibm.com/support/docview.wss?uid=swg21693035
CNVD-2014-09237	IDA Pro 存在多个漏洞（CNVD-2014-09237）	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.hex-rays.com/vulnfix.shtml
CNVD-2014-09232	libsndfile 'src/sd2.c'存在多个缓冲区溢出漏洞	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： https://www.kernel.org/
CNVD-2015-00014	libpng 'png_combine_row()'缓冲区溢出漏洞	高	用户可以联系供应商获得补丁信息： http://www.libpng.org/pub/png/libpng.html
CNVD-2015-00015	WordPress 插件 cformsII 'lib_nona_jax.php'任意文件上传漏洞	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.wordpress.org
CNVD-2015-00013	Netcore(Netis)路由器 53413/UDP 后门服务漏洞	高	暂无
CNVD-2015-00006	Osclass 'contact.php'任意文件上传漏洞	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://osclass.org/
CNVD-2015-00008	Osclass 'alert'参数 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://osclass.org/
CNVD-2014-09208	Ettercap 堆缓冲区溢出漏洞	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： https://www.obrela.com/home/security-labs/advisories/osi-advisory-osi-1402/

表 3 部分高危漏洞列表

小结：本周，IBM 产品被批露存在信息泄露、拒绝服务和安全绕过漏洞，攻击者可利用漏洞获取敏感信息、发起拒绝服务和绕过安全机制获得访问权限。Cisco、Huawei、GnuPG 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、提升权限、执行任意代码或发起拒绝服务攻击。此外，Info-ZIP UnZip 被批露存在一个高危零日漏洞。攻击者可以利用此漏洞在应用程序的上下文中执行任意代码或发起拒绝服务。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 HTTP Server 产品漏洞

Apache HTTP Server 是 Apache 软件基金会的一个开放源码的网页服务器。

本周，Apache 修补了上述产品存在的安全绕过漏洞，避免攻击者利用漏洞执行未授权访问。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/53531>

本周要闻速递

1. Google 公布 Windows 8.1 0day 漏洞验证程序（PoC）

Google 安全研究人员发现了一枚 Windows 8.1 权限提升漏洞，攻击者可以借此漏洞修改系统内容甚至完全控制受害者计算机。这个漏洞源于 Windows 8.1 一个用于确认当前用户是否为系统管理员（administrator）的系统内部函数（非公共 API）——AhcVerifyAdminContext。这个函数没有正确的检查调用其的用户身份模拟令牌（impersonation token），因而可能被非管理员权限的攻击者绕过。目前 Google 已经公布了漏洞验证程序（PoC）。

参考链接：<http://www.freebuf.com/news/55544.html>

2. 磊科（NetCore）全系列路由器中的“疑似后门”程序

磊科(NetCore)路由器中内置了一个叫做 IGDMPD 的程序，按照它的描述应该是 IGD MPT Interface daemon 1.0。该程序会随路由器启动，并在公网上开放端口，攻击者可以执行任意系统命令、上传下载文件，控制路由器。

参考链接：<http://www.freebuf.com/news/55300.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