

信息安全漏洞周报

2014 年 12 月 08 日-2014 年 12 月 14 日

2014 年第 50 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 148 个，其中高危漏洞 69 个、中危漏洞 77 个、低危漏洞 2 个。上述漏洞中，可利用来实施远程攻击的漏洞有 144 个。本周收录的漏洞中，已有 112 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“Technicolor ADSL2+ Router 'ping'远程命令注入漏洞”、“Microsoft Internet Explorer 远程代码执行漏洞（CNVD-2014-08768）”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、各分中心及个人报送了本周收录的全部 148 个漏洞。报送情况如表 1 所示。其中，奇虎 360、天融信、启明星辰、安天实验室、恒安嘉新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 1137 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	1125	1125
天融信	184	0
启明星辰	136	0
安天实验室	125	0
恒安嘉新	107	0

绿盟科技	49	0
CNCERT 河南分中心	5	5
CNCERT 福建分中心	1	1
个人	6	6
报送总计	1738	1137
录入总计	148（去重）	1137

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Adobe、Microsoft、Zenoss 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	Adobe	26	18%
2	Microsoft	21	14%
3	Zenoss	18	12%
4	X.Org	13	9%
5	WebKit	6	4%
6	WordPress	5	3%
7	Apache	3	2%
8	Technicolor	3	2%
9	IBM	2	1%
10	其他	51	35%

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 148 个漏洞。其中应用程序漏洞 118 个，WEB 应用漏洞 19 个，网络设备漏洞 6 个，操作系统漏洞 4 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	118
WEB 应用漏洞	19
网络设备漏洞	6
操作系统漏洞	4
数据库漏洞	1

表 3 漏洞按影响类型统计表

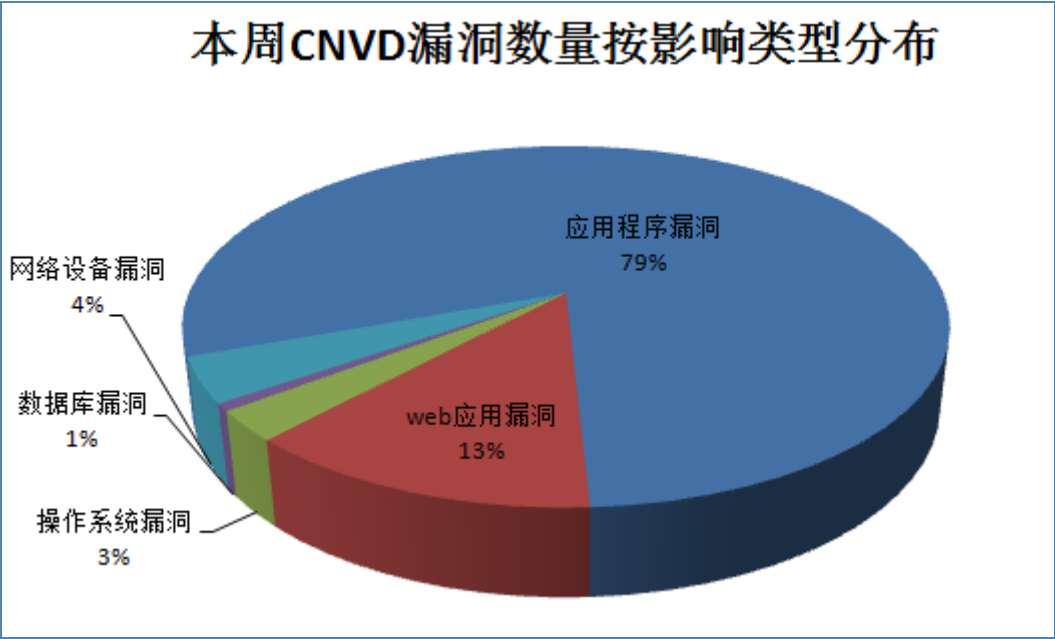


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 3 个电信行业漏洞， 1 个工控系统行业漏洞（如下图表所示）。其中，“Trihedral VTScada 畸形请求拒绝服务漏洞”的综合评级为“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-2014-08782	Technicolor ADSL2+ Router 'failrefer' 参数重定向漏洞	中	否
电信	CNVD-2014-08781	Technicolor ADSL2+ Router 'failrefer' 参数跨站脚本漏洞	中	否
电信	CNVD-2014-08783	Technicolor ADSL2+ Router 'ping'远程命令注入漏洞	高	否
工控系统	CNVD-2014-08874	Trihedral VTScada 畸形请求拒绝服务漏洞	高	是

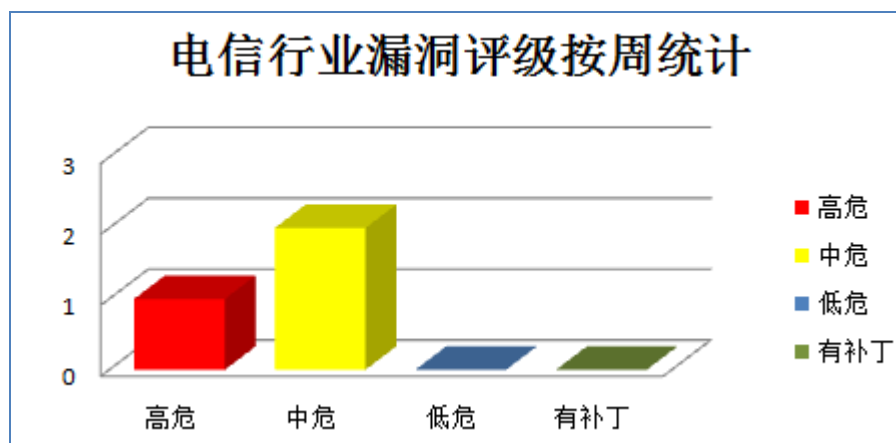


图 1 电信行业漏洞统计

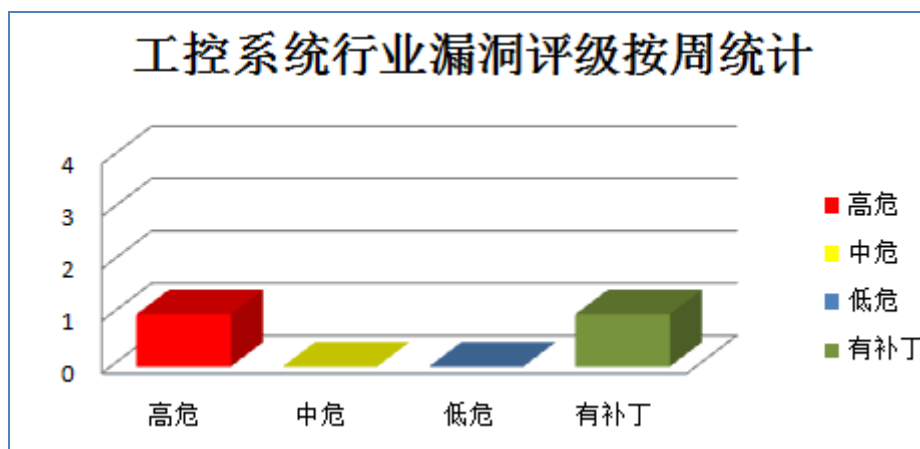


图 2 工控系统行业漏洞统计

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、Microsoft 产品安全漏洞

12 月 9 日，微软发布了 2014 年 12 月份的月度例行安全公告，共含 7 项更新，修复了 Microsoft Windows、Internet Explorer、Office 和 Exchange 中存在的 25 个安全漏洞。其中，Internet Explorer、Word、VBScript 3 项漏洞的更新综合评级为最高级“严重”级别，成功利用此漏洞的攻击者均可通过执行远程代码，获得与当前用户相同的用户权限，如果当前用户拥有最高权限，则攻击者可完全控制受影响的系统。综合利用上述漏洞，攻击者可以远程执行代码，提升权限，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-2014-08882、CNVD-2014-08883、CNVD-2014-08884、CNVD-2014-08885、CNVD-2014-08886、CNVD-2014-08887、CNVD-2014-08888）、Microsoft Internet Explorer 存在未明内存破坏漏洞（CNVD-2014-08889）。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/webinfo/show/3547>

2、ISC BIND 产品安全漏洞

本周，CNVD 收录了域名解析系统软件 BIND 9 存在的一个远程拒绝服务漏洞（CNVD-2014-08772，对应 CVE-2014-8500），允许攻击者利用变更管理 BIND 9 影响区域委派的相关配置，这使得其他 BIND 服务器跟随区域委派的配置进行无限制次数查询，导致域名解析服务崩溃。

CNVD 收录的相关漏洞包括：BIND GeoIP 功能拒绝服务漏洞、BIND 拒绝服务漏洞。其中“BIND 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-2014-08786>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08772>

3、F5 TLS 产品安全漏洞

12 月 10 日，CNVD 收录了安全传输层协议 TLS 1.2 存在的一个中间人攻击漏洞（CNVD-2014-08824，对应 CVE-2014-8730），该漏洞与此前披露 SSL V3 “POODLE”（中文名：贵宾犬）漏洞攻击原理相同，允许攻击者利用中间人攻击方法绕过传输层加密机制，窃取用户的敏感信息，例如 cookies 信息，帐号信息等。

CNVD 收录的相关漏洞包括：TLS 填充中间人攻击漏洞。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-2014-08824>

4、Adobe 产品安全漏洞

Adobe Reader/Acrobat 是一款流行的处理 PDF 文件的应用程序。本周，上述产品被披露存在未明内存破坏漏洞，攻击者可利用漏洞执行任意代码或发起拒绝服务。

CNVD 收录的相关漏洞包括：Adobe Reader/Acrobat 存在未明内存破坏漏洞（CNVD-2014-08844、CNVD-2014-08845、CNVD-2014-08846、CNVD-2014-08847、CNVD-2014-08848、CNVD-2014-08849、CNVD-2014-08850、CNVD-2014-08851）。上述漏洞的综合评级均为“高危”。目前，厂商已经发布了该漏洞的修补程序。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-2014-08844>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08845>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08846>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08847>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08848>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08849>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08850>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08851>

5、phpTrafficA 'Php/Functions/log_function.php' SQL 注入漏洞

phpTrafficA 是一个统计工具用于网站流量分析。本周，phpTrafficA 被披露存在综合评级为“高危”的 SQL 注入漏洞。攻击者可利用漏洞提交特制的 SQL 查询，操作或获取数据库数据。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-2014-08876>

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-2014-08763	MediaWiki PHP 代码注入漏洞	高	用户可以联系供应商获得补丁信息： http://www.mediawiki.org/wiki/MediaWiki
CNVD-2014-08760	PBBoard 'email'参数 SQL 注入漏洞	高	用户可以联系供应商获得补丁信息： http://www.pbboard.com/
CNVD-2014-08759	Tcpdump 缓冲区溢出漏洞	高	用户可以联系供应商获得补丁信息： http://cvs.tcpdump.org/
CNVD-2014-08752	WebKit 存在未明内存破坏漏洞（CNVD-2014-08752）	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页： http://www.webkit.org/
CNVD-2014-08754	WebKit 存在未明内存破坏漏洞（CNVD-2014-08754）	高	用户可以联系供应商获得补丁信息： http://www.webkit.org/
CNVD-2014-08753	WebKit 存在未明内存破坏漏洞（CNVD-2014-08753）	高	用户可以联系供应商获得补丁信息： http://www.webkit.org/
CNVD-2014-08771	Samsung SmartViewer 'STWConfig' ActiveX 远程代码执行漏洞	高	目前厂商已经发布升级补丁/版本以修复这个安全问题，请用户及时下载更新： http://www.samsungsecurity.com/product/product_view.asp?idx=6275
CNVD-2014-08770	JasPer 'jpc_dec.c'存在多个远程缓冲区溢出漏洞	高	用户可以联系供应商获得补丁信息： http://www.ece.uvic.ca/~frodo/software.html

CNVD-2014-08775	WordPress 插件 Cart66 Lite 'Cart66ModelAbstract.php' SQL 注入漏洞	高	用户可以联系供应商获得补丁信息： https://wordpress.org/
CNVD-2014-08774	UnRTF RTF 文件处理越界内存破坏漏洞	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.gnu.org/software/unrtf/unrtf.html

表 3 部分高危漏洞列表

小结：本周，微软发布了 2014 年 12 月份的月度例行安全公告，共含 7 项更新，修复了 Microsoft Windows、Internet Explorer、Office 和 Exchange 中存在的 25 个安全漏洞。其中，Internet Explorer、Word、VBScript 3 项漏洞的更新综合评级为最高级“严重”级别，综合利用上述漏洞，攻击者可以远程执行代码，提升权限，获得敏感信息。本周，CNVD 收录了域名解析系统软件 BIND 9 存在的一个远程拒绝服务漏洞及安全传输层协议 TLS 1.2 存在的一个中间人攻击漏洞。同时，Adobe 多款产品被批露存在未明内存破坏漏洞，允许攻击者利用漏洞执行任意代码或发起拒绝服务。此外，phpTrafficA 被批露存在一个高危零日漏洞。攻击者可利用漏洞提交特制的 SQL 查询，操作或获取数据库数据。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、IBM 修补 Tivoli Endpoint Manager/Operational Decision 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。IBM Operational Decision Manager 是一个运营决策管理平台。

本周，IBM 修补了上述产品存在的任意代码执行和 XML 外部实体注入漏洞，避免攻击者利用漏洞执行任意代码或获取敏感信息。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/52684>

<http://www.cnvd.org.cn/patchInfo/show/52601>

本周要闻速递

1. 阿里巴巴速卖通曝安全漏洞

据国外媒体报道，阿里巴巴全球速卖通的网站上曝出安全漏洞，可能影响全球的数百万用户。攻击者可以在不知道用户账户密码的情况下，利用该漏洞窃取到全球数百万

用户的个人信息。不过，12月9日，据官方反馈，阿里巴巴安全团队已在第一时间修复该漏洞。

参考链接：<http://www.freebuf.com/news/53785.html>

2. 巴西知名 SCADA 曝严重拒绝服务漏洞

巴西知名 SCADA（数据采集与监视控制系统）Elipse SCADA 近日曝出一个严重的拒绝服务漏洞，这个漏洞出现在 Elipse SCADA 部署的 DNP3 协议上。漏洞版本号为 CVE-2014-5429，它允许攻击者提交包含格式错误的报文，消耗系统资源，而造成拒绝服务攻击。并且该漏洞的表现形式随着 SCADA 部署的不同而变化：在 Elipse E3 中，服务会中断；在 Elipse 动力系统中，大概会产生 30 秒左右的停顿；而 Elipse SCADA 则会直接宕机。该漏洞还可以被远程利用，虽然现在还没有发现真实案例。目前其官方 Elipse 已修复此漏洞。

参考链接：<http://www.freebuf.com/news/53704.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