

信息安全漏洞周报

2014 年 8 月 4 日-2014 年 8 月 10 日

2014 年第 32 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 121 个，其中高危漏洞 33 个、中危漏洞 80 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 110 个。本周收录的漏洞中，已有 75 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“Hybrid Auth 'install.php'远程代码执行漏洞”、“TP-Link TL-WR740N 命令注入漏洞”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 8 家成员单位及个人报送了本周收录的全部 121 个漏洞。报送情况如表 1 所示。其中，奇虎 360、安天实验室、恒安嘉新、启明星辰、天融信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 359 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	324	324
安天实验室	95	0
恒安嘉新	85	0
启明星辰	49	0
天融信	47	0
绿盟科技	44	0

知道创宇	2	0
东软	1	1
CNCERT 江西分中心	20	20
CNCERT 山西分中心	7	7
CNCERT 上海分中心	1	1
CNCERT 福建分中心	1	1
CNCERT 河北分中心	1	1
个人	4	4
报送总计	681	359
录入总计	121（去重）	359

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、OpenSSL 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	14	12%
2	Wordpress	12	10%
3	OpenSSL	9	7%
4	Wireshark	5	4%
5	Lian Li Co. Ltd	5	4%
6	Cisco	4	3%
7	HP	4	3%
8	Drupal	3	2%
9	Microsoft	3	2%
10	其他	62	53%

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 121 个漏洞。其中应用程序漏洞 82 个，WEB 应用漏洞 22 个，网络设备漏洞 10 个，操作系统漏洞 5 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	82
WEB 应用漏洞	22

网络设备漏洞	10
操作系统漏洞	5
安全产品漏洞	2

表 3 漏洞按影响类型统计表

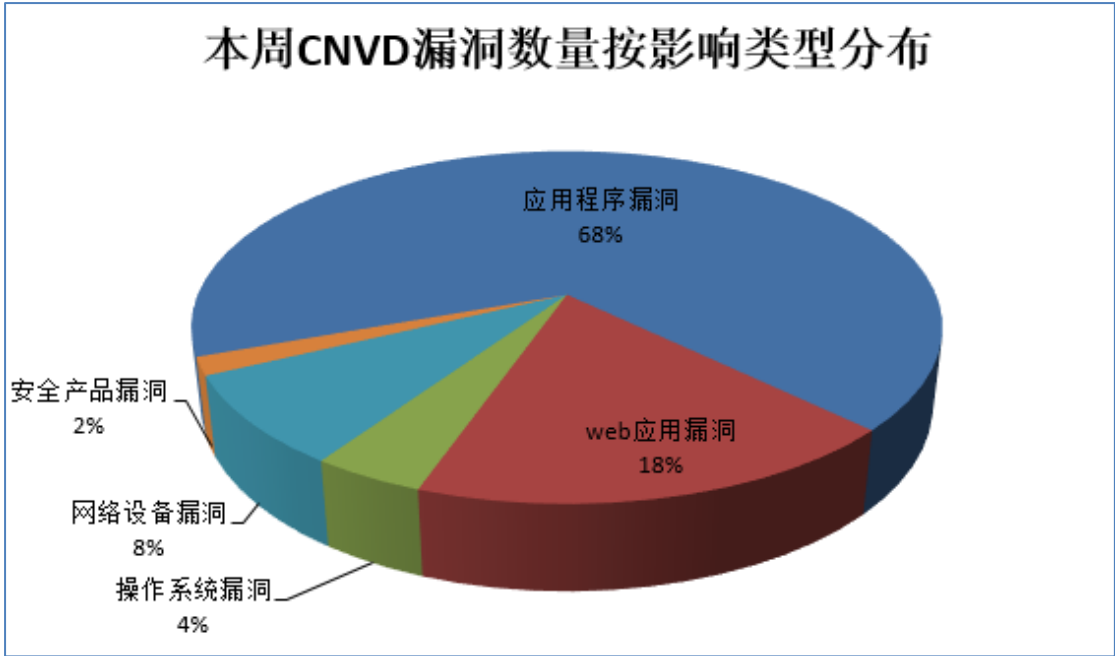


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 11 个电信行业漏洞，8 个移动互联网漏洞，1 个工控系统漏洞（如下图表所示）。其中，“Cisco IOS 和 IOS XE Software 拒绝服务漏洞、Android AP P FakeID 签名漏洞”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-2014-04787	Wireshark GTP 和 GSM Management 拒绝服务漏洞	中	是
电信	CNVD-2014-04795	TP-Link TL-WR740N 命令注入漏洞	高	否
电信	CNVD-2014-04824	IBM WebSphere Portal 存在未明跨站脚本漏洞（CNVD-2014-04824）	中	是
电信	CNVD-2014-04823	IBM WebSphere Portal 信息泄露漏洞(CNVD-2014-04823)	中	是
电信	CNVD-2014-04822	IBM WebSphere Portal 存在未明跨站脚本漏洞（CNVD-2014-04822）	中	是
电信	CNVD-2014-04820	IBM WebSphere Portal 开放重定向漏洞（CNVD-2014-04820）	中	是
电信	CNVD-2014-04841	Cisco IOS 内存泄露漏洞（CNVD-2014-	中	是

		04841)		
电信	CNVD-2014-04850	Cisco Nexus 9000 Series Switches 安全绕过漏洞	中	是
电信	CNVD-2014-04854	Cisco Unified Communications Manager 并发登陆安全绕过漏洞	中	否
电信	CNVD-2014-04856	Cisco IOS 和 IOS XE Software 拒绝服务漏洞	高	是
电信	CNVD-2014-04858	Aerohive HiveOS 存在多个漏洞	中	是
移动互联网	CNVD-2014-04764	Android APP FakeID 签名漏洞	高	是
移动互联网	CNVD-2014-04778	Google Android Certificate Chain Validation 安全绕过漏洞	中	是
移动互联网	CNVD-2014-04804	Android for MSM Project 本地权限提升漏洞	中	是
移动互联网	CNVD-2014-04826	Apache Cordova For Android 安全绕过漏洞 (CNVD-2014-04826)	中	是
移动互联网	CNVD-2014-04825	Apache Cordova For Android 安全绕过漏洞 (CNVD-2014-04825)	中	是
移动互联网	CNVD-2014-04821	Apache Cordova For Android 信息泄露漏洞	中	是
移动互联网	CNVD-2014-04875	Photo WiFi Transfer 'path'参数目录遍历漏洞	中	否
移动互联网	CNVD-2014-04872	Evernote For Android 存在多个信息泄露漏洞	中	是
工控系统	CNVD-2014-04877	SubSTATION Server 存在多个缓冲区溢出漏洞	高	否

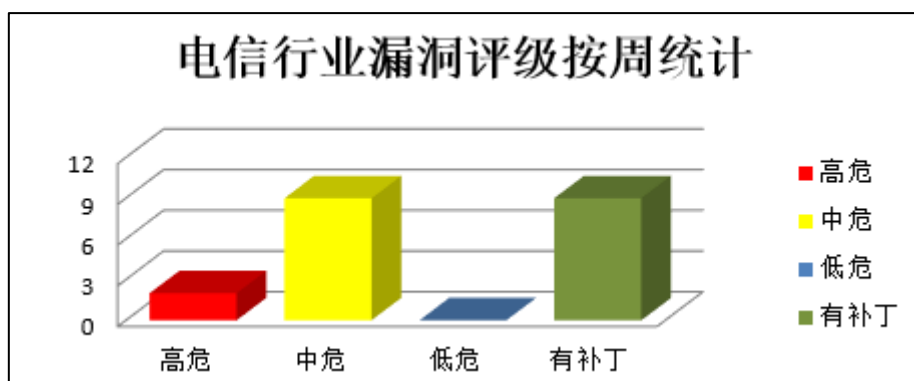


图 1 电信行业漏洞统计

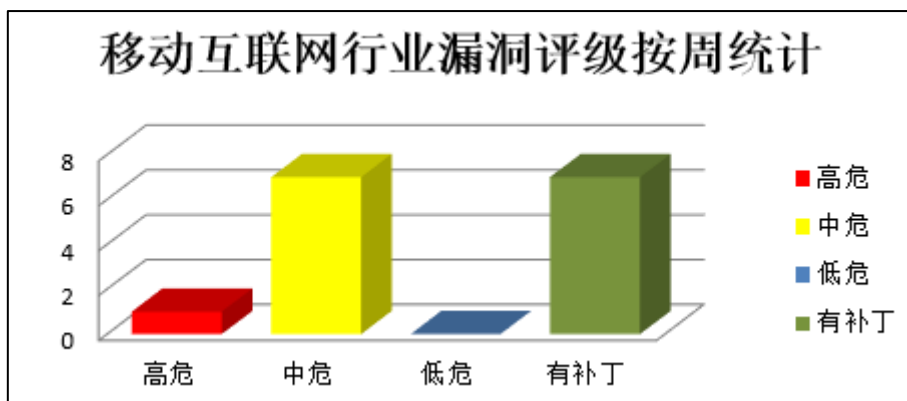


图 2 移动互联网行业漏洞统计

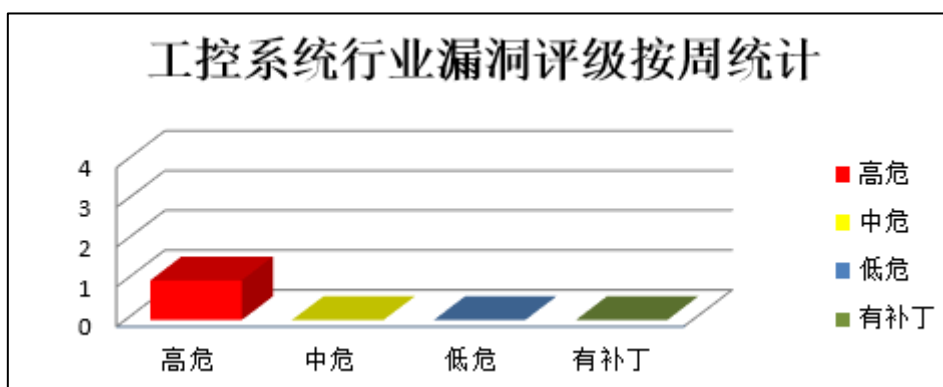


图 3 工控系统行业漏洞统计

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、OpenSSL 产品安全漏洞

2014 年 8 月 6 日，OpenSSL 发布了 2014 年 8 月份安全公告，修复了 OpenSSL 产品存在的 9 个安全漏洞，涉及 SSL/TLS 和 DTLS 两种协议。允许攻击者利用漏洞获取敏感信息或者发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：OpenSSL 远程拒绝服务漏洞、OpenSSL SRP 远程拒绝服务漏洞、OpenSSL 中间人安全绕过漏洞、OpenSSL 空指针引用本地拒绝服务漏洞、OpenSSL 信息泄露漏洞、OpenSSL DTLS 远程拒绝服务漏洞（CNVD-2014-04832、CNVD-2014-04833、CNVD-2014-04835、CNVD-2014-04837）。其中“OpenSSL 远程拒绝服务漏洞、OpenSSL DTLS 远程拒绝服务漏洞（CNVD-2014-04832、CNVD-2014-04833、CNVD-2014-04837）”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/webinfo/show/3482>

2、IBM 产品安全漏洞

IBM Security AppScan Source 可以检测并修复 Web 和移动应用内的漏洞。IBM InfoSphere BigInsights 是 IBM 推出的用于储存和分析“大数据”的软件平台。IBM WebSphere Portal 提供了一个组合应用程序或业务 mashup 框架，并且提供了一种高级工具来构造灵活的，基于 SOA 的解决方案。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任意脚本代码。

CNVD 收录的相关漏洞包括：IBM Security AppScan Source 本地权限提升漏洞、IBM Security Access Manager for Mobile 存在未明跨站脚本漏洞、IBM InfoSphere BigInsights 信息泄露漏洞、IBM InfoSphere Optim Data Grow Solutions 存在多个信息泄露漏洞、IBM WebSphere Portal 开放重定向漏洞（CNVD-2014-04820）、IBM WebSphere Portal 存在未明跨站脚本漏洞（CNVD-2014-04822、CNVD-2014-04824）、IBM WebSphere Portal 信息泄露漏洞（CNVD-2014-04823）。其中“IBM Security AppScan Source 本地权限提升漏洞”的综合评级为“高危”。目前，除“IBM InfoSphere BigInsights 信息泄露漏洞”外，厂商已经发布其余漏洞的修补程序。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-2014-04807>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04827>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04855>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04851>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04820>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04822>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04824>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04823>

3、Cisco 产品安全漏洞

Cisco Nexus 系列交换机是数据中心级交换机。采用 Cisco Nexus OS 操作系统。Cisco Unified Communications Manager 是一款 Cisco IP 电话解决方案中的呼叫处理组件。Cisco IOS 是多数思科系统路由器和网络交换机上使用的互联网络操作系统。本周，上述产品被披露存在拒绝服务和安全绕过漏洞，攻击者可利用漏洞绕过安全限制执行未经授权操作或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco IOS 和 IOS XE Software 拒绝服务漏洞、Cisco IOS 内存泄露漏洞（CNVD-2014-04841）、Cisco Nexus 9000 Series Switches 安全绕过漏洞、Cisco Unified Communications Manager 并发登陆安全绕过漏洞。其中“Cisco IOS 和 IOS XE Software 拒绝服务漏洞”的综合评级为“高危”。目前，除“Cisco Unified Communications Manager 并发登陆安全绕过漏洞”外，厂商已经发布其余漏洞的修补程序。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-2014-04856>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04841>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04850>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04854>

4、Apache 产品安全漏洞

Apache Cordova 是用 HTML、CSS、JavaScript 构建本地移动应用程序的平台。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,上述产品被披露存在多个安全漏洞,攻击者可利用漏洞获得敏感信息或执行未授权操作。

CNVD 收录的相关漏洞包括:Apache Cordova For Android 信息泄露漏洞、Apache Cordova For Android 安全绕过漏洞(CNVD-2014-04825、CNVD-2014-04826)、Apache Subversion 不安全身份验证漏洞。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-2014-04821>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04825>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04826>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04794>

5、GNU glibc '__gconv_translit_find()'函数内存破坏漏洞

glibc 是绝大多数 Linux 操作系统中 C 库的实现。本周,GNU 被披露存在综合评级为“高危”的内存破坏漏洞。攻击者可利用漏洞在受影响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-2014-04771>

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-2014-04770	Sphider 'admin.php'存在多个输入验证漏洞	高	暂无
CNVD-2014-04766	Sphider 'admin.php'存在多个 SQL 注入漏洞	高	用户可以联系供应商获得补丁信息: http://www.sphider.eu/
CNVD-2014-04777	CMSimple 存在多个漏洞	高	暂无
CNVD-2014-04773	Drupal Storage API 模块任意代码执行漏洞	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: https://www.drupal.org/

CNVD-2014-04790	AlienVault OSSIM 'ws_data'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://forums.alienvault.com/discussion/2559/security-advisory-multiple-vulnerabilities
CNVD-2014-04791	Samba nmbd NetBIOS 名称服务远程代码执行漏洞	高	Samba 已经为此发布了一个安全公告（CVE-2014-3560）以及相应补丁： http://samba.org/samba/patches/
CNVD-2014-04793	AlienVault 命令注入漏洞	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.alienvault.com/
CNVD-2014-04796	AlienVault OSSIM 存在多个远程代码执行漏洞	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://forums.alienvault.com/discussion/2559/security-advisory-multiple-vulnerabilities
CNVD-2014-04814	Kunena 存在多个漏洞	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.kunena.org
CNVD-2014-04813	HP Enterprise Maps 存在未明信息泄露漏洞	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://h20564.www2.hp.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04390793

表 3 部分高危漏洞列表

小结：本周，OpenSSL 多款产品披露存在多个安全漏洞，允许攻击者可以利用漏洞获取敏感信息或者发起拒绝服务攻击。此外，IBM、Cisco、Apache 多款产品被披露存在多个漏洞，攻击者利用漏洞可执行任意代码，获取敏感信息或发起拒绝服务攻击。另外，GNU 被披露存在一个高危零日漏洞。攻击者可利用漏洞在受影响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、Google 修补 Android 产品漏洞

Google Android 是美国谷歌（Google）公司和开放手持设备联盟（简称 OHA）共同开发的一套以 Linux 为基础的开源操作系统。

本周，Google 修补了上述产品存在的安全绕过漏洞，避免攻击者可利用漏洞实施中间人攻击或冒充受信任的应用程序，实施进一步攻击。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/48150>



本周要闻速递

1. 苹果承认 iOS 存“后门”

日前，在“黑客大会”上，知名 iOS 黑客、早期 iOS 越狱开发团队成员乔纳森·扎德斯基对外披露了 iOS 中存在的若干“后门”，并展示了在特定的情况下如何利用这些“后门”获取到用户的个人信息。事实面前，苹果公司也不得不承认，该公司员工确实可以通过一项未曾公开的技术获取 iPhone 用户的短信、通讯录和照片等个人数据。虽然苹果公司辩称称，这个技术是为诊断功能服务的，只是为了向企业信息部门、开发者和苹果公司提供故障信息，不会对用户隐私和安全带来影响。但乔纳森随后指出，利用 iOS 中的“后门”，美国执法机构或者其他恶意组织完全可以在用户不知情的情况下，通过无线网络监测用户的信息。

参考链接：http://news.xinhuanet.com/finance/2014-08/05/c_126832843.htm

2. WordPress 和 Drupal 站点存在 DDoS 风险

近日白帽子 Nir goldshlager 发现了 WordPress 和 Drupal 存在 DDoS 攻击风险，受影响的版本为 WordPress 3.5 - 3.9 和 Drupal 6.x - 7.x，根据为维基百科的数据，使用 WordPress 的站点可能超过 6 千万，更有超过 100 万的 Drupal 网站。

参考链接：<http://www.freebuf.com/news/40284.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