

信息安全漏洞周报

2014 年 8 月 11 日-2014 年 8 月 17 日

2014 年第 33 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 167 个，其中高危漏洞 81 个、中危漏洞 78 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 152 个。本周收录的漏洞中，已有 121 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“Pro Chat Rooms 存在多个漏洞”、“WordPress 插件 wpSS 'ss_handler.php' 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 6 家成员单位、合作伙伴及个人报送了本周收录的全部 167 个漏洞。报送情况如表 1 所示。其中，奇虎 360、恒安嘉新、天融信、安天实验室等单位报送数量较多。此外，CNCERT 各分中心、High-Tech Bridge Security Research、习科网络安全及白帽子向 CNVD 提交了 496 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	463	463
恒安嘉新	123	0
天融信	123	0
安天实验室	108	0
启明星辰	98	0
绿盟科技	42	0

习科网络安全	3	3
High-Tech Bridge Security Research	1	1
CNCERT 山西分中心	6	6
CNCERT 福建分中心	6	6
CNCERT 湖南分中心	2	2
CNCERT 江西分中心	2	2
个人	13	13
报送总计	990	496
录入总计	167（去重）	496

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Microsoft、WordPress、Adobe 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	Microsoft	40	24%
2	Wordpress	14	8%
3	Adobe	8	5%
4	Apple	7	4%
5	MyBB Group	5	3%
6	Cisco	5	3%
7	Google	4	2%
8	IBM	3	2%
9	Apache	2	1%
10	其他	79	48%

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 167 个漏洞。其中应用程序漏洞 110 个，WEB 应用漏洞 32 个，网络设备漏洞 13 个，操作系统漏洞 8 个，安全产品漏洞 4 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	110
WEB 应用漏洞	32
网络设备漏洞	13

操作系统漏洞	8
数据库漏洞	4

表 3 漏洞按影响类型统计表

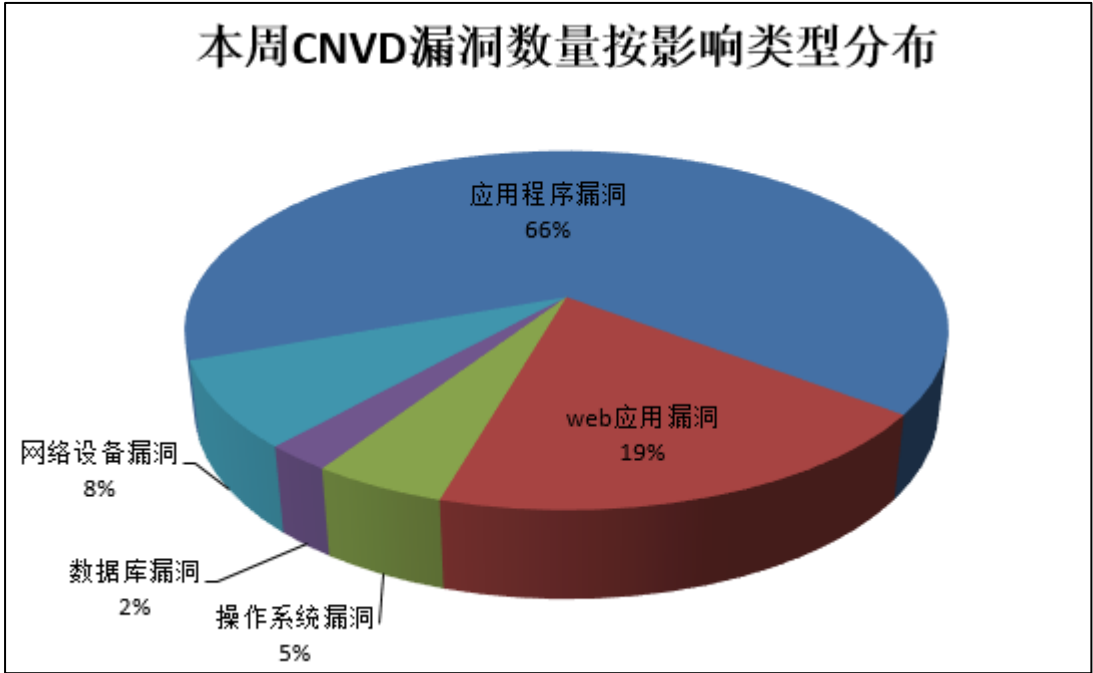


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 10 个电信行业漏洞，4 个移动互联网漏洞（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-2014-04895	Cisco Unity Connection 存在未明漏洞	中	是
电信	CNVD-2014-04925	Cisco Unity Connection SQL 注入漏洞	中	否
电信	CNVD-2014-04950	Cisco Unified Communications Manager 命令注入漏洞（CNVD-2014-04950）	中	否
电信	CNVD-2014-04949	Cisco Unified Communications Manager 拒绝服务漏洞（CNVD-2014-04949）	中	是
电信	CNVD-2014-04964	Iridium 多款产品身份验证绕过漏洞	中	否
电信	CNVD-2014-04993	Microsoft SQL Server 拒绝服务漏洞	中	是
电信	CNVD-2014-05001	Microsoft SQL Server master Data 服务跨站脚本漏洞	中	是
电信	CNVD-2014-05034	Iridium Pilot and OpenPort 内置账户信息泄露漏洞	高	否
电信	CNVD-2014-05030	Cisco Unified Communications Manager 和 Unified Presence Server SQL 注入漏洞	中	是
电信	CNVD-2014-05051	Raritan Japan KX2-101 switches 拒绝服	高	否

		务漏洞		
移动互联网	CNVD-2014-04898	Outlook.com for Android SSL 证书安全绕过漏洞	中	是
移动互联网	CNVD-2014-04914	Touchbyte GmbH PhotoSync for Apple iPhone/iPad/iPod touch 本地命令注入漏洞	中	否
移动互联网	CNVD-2014-05023	BlackBerry 10 OS 验证绕过漏洞	中	是
移动互联网	CNVD-2014-05021	BlackBerry Z10 验证绕过漏洞	中	是

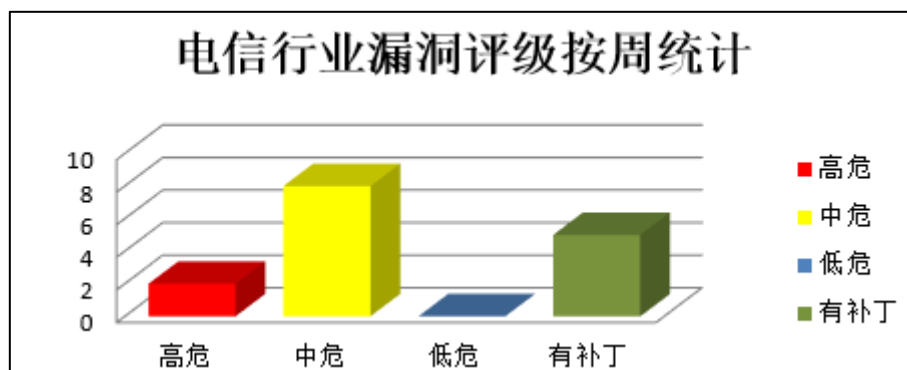


图 1 电信行业漏洞统计

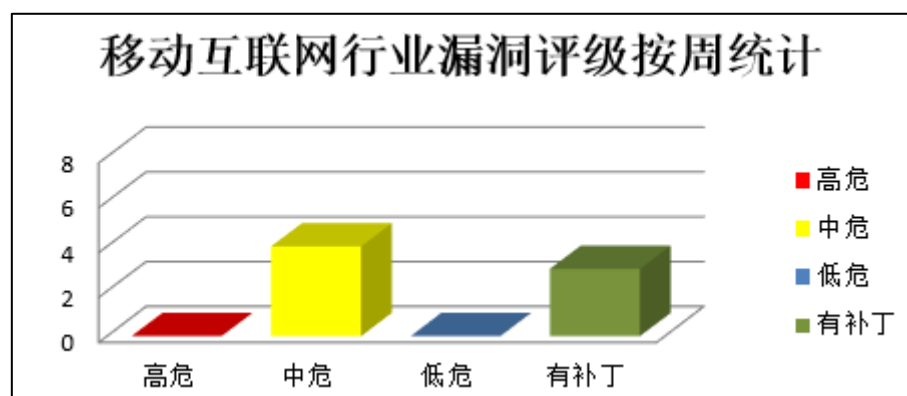


图 2 移动互联网行业漏洞统计

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

8 月 13 日，微软发布了 2014 年 8 月份的月度例行安全公告，共含 9 项更新，修复了 Microsoft Windows、Internet Explorer、Office、SQL Server 和 .NET Framework 中存在的 37 个安全漏洞。其中，2 项更新的综合评级为最高级“严重”级别。利用上述漏洞，攻击者可以执行远程代码，提升权限，绕过安全功能限制。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer 存在未明内存破坏漏洞（CNVD-2014-05027、CNVD-2014-05013、CNVD-2014-05011、CNVD-2014-05007、CNV

D-2014-05009、CNVD-2014-05008、CNVD-2014-05006、CNVD-2014-05005)。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/webinfo/show/3486>

2、Adobe 产品安全漏洞

Adobe Flash Player 是一款 Flash 文件处理程序。Adobe AIR 是 Adobe 公司出品的跨操作系统的运行时库，通过它开发者可利用现有的 Web 开发技术。Adobe Acrobat Professional/Adobe Reader 是 PDF 文件的处理程序。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞泄露内存信息、进行未经授权操作或执行任意脚本代码。

CNVD 收录的相关漏洞包括：Adobe Flash Player/AIR 内存错误引用漏洞（CNVD-2014-05017）、Adobe Flash Player/AIR 存在未明内存泄露漏洞（CNVD-2014-05010、CNVD-2014-05012、CNVD-2014-05000、CNVD-2014-05015、CNVD-2014-05016）、Adobe Acrobat/Reader 任意代码执行漏洞、Adobe Flash Player and AIR 存在未明安全绕过漏洞。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-2014-05017>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05010>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05012>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05000>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05015>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05016>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05014>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05003>

3、Cisco 产品安全漏洞

Cisco Unified Communications Manager 是一款 Cisco IP 电话解决方案中的呼叫处理组件。Cisco Unified Presence 是一款基于标准的平台，能够收集有关用户可用性和通信功能的信息，以提供统一用户在网状态。Cisco Unity Connection 是一个由语音、视频、数据和移动产品及应用组成的全面 IP 通信系统。本周，上述产品被披露存在 SQL 注入和拒绝服务漏洞，攻击者可利用漏洞访问或修改数据库数据或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco Unified Communications Manager 和 Unified Presence Server SQL 注入漏洞、Cisco Unified Communications Manager 拒绝服务漏洞（CNVD-2014-04949、CNVD-2014-04950）、Cisco Unity Connection SQL 注入漏洞、Cisco Unity Connection 存在未明漏洞。目前，除“Cisco Unified Communications Manager 命令注入漏洞（CNVD-2014-04950）、Cisco Unity Connection SQL 注入漏洞”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-2014-05030>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04949>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04950>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04925>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04895>

4、Google 产品安全漏洞

Google Chrome 是一款流行的 WEB 浏览器。Google V8 是其中的一套开源 JavaScript 引擎。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、发起拒绝服务攻击或执行任意脚本代码。

CNVD 收录的相关漏洞包括：Google Chrome 存在多个漏洞（CNVD-2014-05045）、Google Chrome 信息泄露漏洞（CNVD-2014-05026）、Google Chrome 远程代码执行漏洞（CNVD-2014-05028）、Google V8 JavaScript Engine 拒绝服务漏洞。其中“Google Chrome 存在多个漏洞（CNVD-2014-05045）、Google Chrome 远程代码执行漏洞（CNVD-2014-05028）”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-2014-05045>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05026>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05028>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04971>

5、TomatoCart SQL 注入漏洞

TomatoCart 是一个用 PHP 开发的开源电子商务软件。本周，TomatoCart 被披露存在综合评级为“高危”的 SQL 注入漏洞。攻击者可利用漏洞访问或修改数据库数据。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-2014-04893>

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-2014-04889	GPGME 'status_handler()'函数堆缓冲区溢出漏洞	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://www.ubuntu.com/usn/usn-2307-1

CNVD-2014-04970	MIT Kerberos 空指针引用远程拒绝服务漏洞	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： http://web.mit.edu/kerberos/www/
CNVD-2014-04905	WordPress 插件 Contus Video Gallery 'admin/models/playlist.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/plugins/contus-video-gallery/
CNVD-2014-04904	Ubuntu 'Unity'包锁屏安全绕过漏洞	高	暂无
CNVD-2014-04902	WordPress 插件 Contus Video Gallery 'admin/models/video.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/plugins/contus-video-gallery/
CNVD-2014-04900	Sphider 'admin/admin.php' SQL 注入漏洞	高	暂无
CNVD-2014-04899	WordPress 插件 Contus Video Gallery 'admin/views/video/addvideo.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/plugins/contus-video-gallery/
CNVD-2014-04897	WordPress 插件 Contus Video Gallery 'front/views/videohome.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/plugins/contus-video-gallery/
CNVD-2014-04892	nginx SMTP 代理远程命令注入漏洞	高	用户可联系供应商获得补丁信息： http://nginx.org/en/download.html
CNVD-2014-04910	WordPress 存在多个漏洞（CNVD-2014-04910）	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://wordpress.org/

表 3 部分高危漏洞列表

小结：本周，微软发布了 2014 年 8 月份的月度例行安全公告，共含 9 项更新，修复了 Microsoft Windows、Internet Explorer、Office、SQL Server 和 .NET Framework 中存在的 37 个安全漏洞。其中，2 项更新的综合评级为最高级“严重”级别。此外，Adobe、Cisco、Google 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、执行未经授权操作或发起拒绝服务攻击。另外，TomatoCart 被披露存在一个高危零日漏洞。攻击者可利用漏洞访问或修改数据库数据。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。

CNVD 整理和发布以下重要安全修补信息。

1、Red Hat 修补多款产品漏洞

Red Hat Directory Server 是一款 LDAPv3 兼容的目录服务程序。389 Directory Server 的前身是 Fedora Directory Server，是一个企业级的 Linux 目录服务器。

本周，Red Hat 修补了上述产品存在的信息泄露漏洞，避免攻击者可利用漏洞获取敏感信息。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/48670>



本周要闻速递

1. 高通芯片存在安全漏洞可泄露敏感信息

8 月 17 日记者获悉，有国外通信安全专家在一份报告中称，高通的骁龙处理器存在严重的安全漏洞。目前高通已对外承认了漏洞的存在。相关安全专家是在“黑帽 2014 大会”的发言中提到该漏洞的，称几乎所有采用高通骁龙处理器的手机都存在此安全漏洞。只要通过一些技术手段，任何人都可以利用该漏洞来攻破 DRM（内容数字版权加密保护技术）方案，可能导致敏感资料曝光。专家称，一些使用高通骁龙处理器的厂商也发现了这一漏洞，并已经做出了修正。

参考链接：<http://finance.chinanews.com/it/2014/08-18/6501327.shtml>

2. BlackHat: 手机运营商软件发现严重漏洞

在这周举行的 Black Hat 黑帽黑客大会上，两名来自 Accuvant 的研究员公布了一个存在于运营商控制软件中的严重漏洞，该漏洞影响安卓，黑莓以及一小部分的 iOS 设备，涉及不同运营商制造的设备及模型。通过这些设备和运营商，黑客能够利用控制软件中的漏洞安装恶意软件，访问数据，增删或者运行任意应用。清除一个设备的全部数据，甚至远程修改屏幕锁屏的 PIN 码，以及其他一些敏感操作。不过 Accuvant 已经恰当的把他们发现的问题告知了服务提供商来缓解潜在的安全威胁。这些存在漏洞的软件的厂商已经公布了一个补丁来解决这种问题。基带运营商也已经编写了补丁代码，相关运营商也正在进行补丁发布的流程。

参考链接：<http://www.freebuf.com/news/40443.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