

信息安全漏洞周报

2015 年 05 月 04 日-2015 年 05 月 10 日

2015 年第 19 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 103 个，其中高危漏洞 28 个、中危漏洞 69 个、低危漏洞 6 个。上述漏洞中，可利用来实施远程攻击的漏洞有 94 个。本周收录的漏洞中，已有 83 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。其中互联网上出现“Apple Mac OS X ATS fontd 本地权限提升漏洞”、“Mozilla Firefox 存在未明任意代码执行漏洞”等零日漏洞，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 103 个漏洞。报送情况如表 1 所示。其中，奇虎、启明星辰、安天科技、恒安嘉新等单位报送数量较多。此外，CNCERT 各分中心、乌云、漏洞盒子、High-Tech Bridge Security Research Lab 及白帽子向 CNVD 提交了 599 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	387	387
启明星辰	111	0
安天实验室	73	0
恒安嘉新	41	0
天融信	37	2
绿盟科技	9	0

乌云	175	175
漏洞盒子	15	15
High-Tech Bridge Security Research Lab	1	1
CNCERT 宁夏分中心	2	2
CNCERT 福建分中心	1	1
CNCERT 河南分中心	1	1
个人	15	15
报送总计	868	599
录入总计	103（去重）	599

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 ZOHO、Cisco、Magento 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	ZOHO	7	7%
2	Cisco	5	5%
3	Magento	5	5%
4	wftpsrvr	4	4%
5	Junos	4	4%
6	Oracle	3	3%
7	Linux	3	3%
8	ClamAV	3	3%
9	kozoz	3	3%
10	其他	66	63%

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 103 个漏洞。其中应用程序漏洞 75 个，WEB 应用漏洞 12 个，操作系统漏洞 6 个，网络设备漏洞 6 个，数据库漏洞 2 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	75
WEB 应用漏洞	12
操作系统漏洞	6
网络设备漏洞	6
数据库漏洞	2
安全产品漏洞	2

表 3 漏洞按影响类型统计表

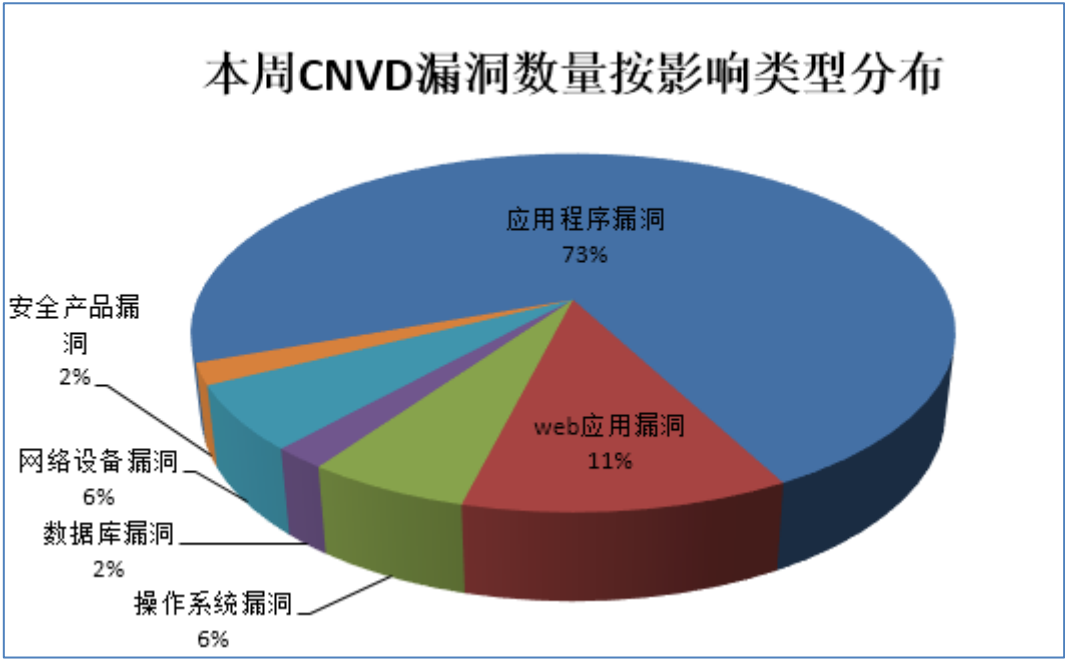


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 7 个电信行业漏洞，2 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）。其中，“汇文软件手机 OPAC 图书馆门户系统 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-2015-02849	Cisco StarOS 会话管理服务拒绝服务漏洞	中	是
电信	CNVD-2015-02859	IBM DB2/DB2 Connect 信息泄露漏洞	低	是
电信	CNVD-2015-02889	Swisscom Centro Grande DSL Router HNDS 服务证书校验失败验证绕过漏洞	中	是
电信	CNVD-2015-02914	D-Link DIR-601 身份验证绕过漏洞	中	是
电信	CNVD-2015-02909	Apache Tomcat 拒绝服务漏洞（CNVD-2015-02909）	中	是
电信	CNVD-2015-02917	Nagios Business Process Intelligence (B	中	是

		PI) index.php 存在未明跨站脚本漏洞		
电信	CNVD-2015-02919	Cisco Unified Communications Manage SQL 注入漏洞	中	是
移动互联网	CNVD-2015-02871	汇文软件手机 OPAC 图书馆门户系统 S QL 注入漏洞	高	是
移动互联网	CNVD-2015-02908	wpa_supplicant/hostapd EAP-pwd 拒绝服务漏洞	中	是
工控系统	CNVD-2015-02869	Elipse SCADA DLL 劫持漏洞	中	否

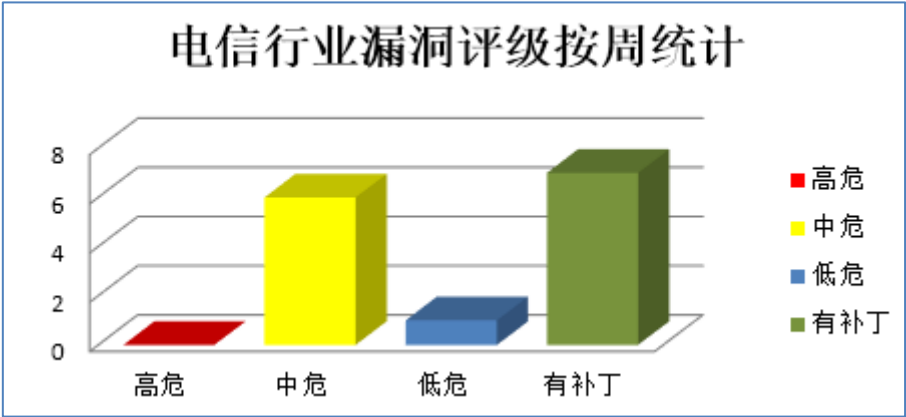


图 1 电信行业漏洞统计

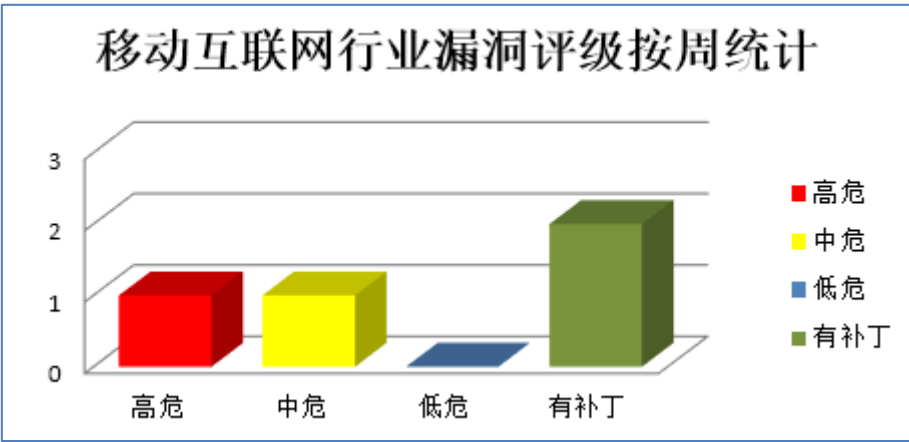


图 2 移动互联网系统行业漏洞统计

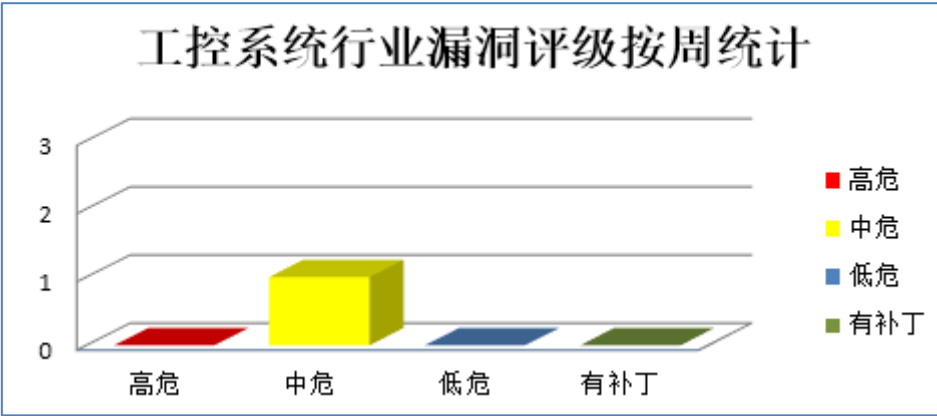


图 3 工控系统行业漏洞统计

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 UCS Central Software 是美国思科（Cisco）公司的一个集计算、虚拟化和网络于一体的软件平台。Cisco Unified Communications Manager 是美国思科（Cisco）公司的 IP Telephony 解决方案的呼叫处理组件。Cisco Unity Connection 是美国思科（Cisco）公司的一套语音留言平台。Cisco Finesse Server 是 Cisco 开发的代理和管理桌面。Cisco ASR 5000 系列是一个运营商级平台,可用于部署高需求的 3G 网络以及向长期演进 (LTE) 迁移。Cisco StarOS 是其设备上的操作系统。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、进行跨站脚本攻击、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 UCS Central Software 任意命令执行漏洞、Cisco Unified Communications Manager SQL 注入漏洞、Cisco Unity Connection CUCReports 页面跨站请求伪造漏洞、Cisco Finesse Server 存在多个跨站脚本漏洞、Cisco StarOS 会话管理服务拒绝服务漏洞。其中“Cisco UCS Central Software 任意命令执行漏洞”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-2015-02920>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02919>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02918>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02850>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02849>

2、Oracle Data Quality 产品远程代码执行漏洞

Oracle Data Quality 是美国甲骨文（Oracle）公司的一套提供了全面的数据质量管理环境的软件。该软件支持数据管理、数据集成和数据迁移等。本周，上述产品被披露存在远程代码执行漏洞。攻击者可利用漏洞，通过诱使用户打开恶意的网页或文件，在浏览器上下文中执行任意代码。

CNVD 收录的相关漏洞包括：Oracle Data Quality DscXB onloadstatechange 内存错误引用远程代码执行漏洞、Oracle Data Quality LoaderWizard SetEntities 类型混淆远程代码执行漏洞、Oracle Data Quality LoaderWizard DataPreview 类型混淆远程代码执行漏洞。其中，“Oracle Data Quality LoaderWizard SetEntities 类型混淆远程代码执行漏洞、Oracle Data Quality LoaderWizard DataPreview 类型混淆远程代码执行漏洞”的漏

洞综合评级均为“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-2015-02936>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02937>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02938>

3、Google Chrome 产品安全漏洞

Google Chrome 是一款流行的 WEB 浏览器。本周，上述产品被披露存在拒绝服务漏洞和内存错误引用漏洞。攻击者可利用漏洞发起拒绝服务攻击或执行任意代码。

CNVD 收录的相关漏洞包括：Google Chrome 拒绝服务漏洞（CNVD-2015-02898）、Google Chrome DOM 内存错误引用漏洞（CNVD-2015-02865）。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/flaw/show/CNVD-2015-02898>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02865>

4、Junos 产品安全漏洞

Junos Space Network Management Platform 是一个网络管理平台解决方案。本周，上述产品被披露存在跨站脚本漏洞。攻击者可利用漏洞注入恶意脚本或 HTML 代码。

CNVD 收录的相关漏洞包括：Junos Space Network Management Platform SSL 证书处理跨站脚本漏洞、Junos Space Network Management Platform 网络监视工具跨站脚本漏洞、Junos Space Network Management Platform SNMP 应答伪造跨站脚本漏洞、Junos Space Network Management Platform Event Viewer Syslog 通信日志消息跨站脚本漏洞。目前，厂商已经发布了“Junos Space Network Management Platform SSL 证书处理跨站脚本漏洞”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-2015-02880>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02879>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02878>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-02877>

5、HP ThinPro OS 连接设置选项特权访问漏洞

HP ThinPro OS 是瘦客户端操作系统。本周，HP ThinPro OS 被披露存在综合评级为“高危”的特权访问漏洞。攻击者利用该漏洞可提升权限。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-2015-02939>

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-2015-02837	AlienVault Unified Security Management 远程代码执行漏洞	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： https://www.alienvault.com/forums/discussion/4415/
CNVD-2015-02858	EMC RSA Identity Management 和 Governance 未授权访问漏洞	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.emc.com/support/rsa/index.htm
CNVD-2015-02865	Google Chrome DOM 内存错误引用漏洞（CNVD-2015-02865）	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://googlechromereleases.blogspot.com/2015/04/stable-channel-update_28.html
CNVD-2015-02898	Google Chrome 拒绝服务漏洞（CNVD-2015-02898）	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://googlechromereleases.blogspot.com/2015/04/stable-channel-update_28.html
CNVD-2015-02896	Foxit 多个产品内存破坏漏洞	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.foxitsoftware.com/support/security_bulletins.php#FRD-27 http://www.foxitsoftware.com/Secure_PDF_Reader/version_history.php
CNVD-2015-02894	LibAxl XML 处理存在未明堆缓冲区溢出漏洞	高	目前厂商已经发布了安全公告及相关升级补丁,修复了此安全问题,请到厂商主页下载: http://www.aspl.es/xml/
CNVD-2015-02907	EMC AutoStart ftagent 命令执行漏洞	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.emc.com/storage/autostart.htm
CNVD-2015-02913	International Components for Unicode 整数溢出漏洞	高	暂无
CNVD-2015-02912	International Components for Unicode 堆缓冲区溢出漏洞	高	暂无
CNVD-2015-02930	Quassel IRC SQL 注入漏洞	高	用户可联系供应商获得补丁信息： http://quassel-irc.org/node/120

表 3 部分高危漏洞列表

小结：本周，Cisco 多款产品被批露存在多个安全漏洞。攻击者可利用漏洞获取敏感信息、进行跨站脚本攻击、执行任意命令或发起拒绝服务攻击。此外，Oracle Data Quality 产品被披露远程代码执行漏洞，Google Chrome 和 Junos 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、进行跨站脚本或发起拒绝服务攻击。另外，HP ThinPro OS 被披露存在一个高危零日漏洞，攻击者利用该漏洞可提升权限。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 DB2/DB2 Connect 产品漏洞

IBM DB2 是一个大型的商业关系数据库系统。

本周，IBM 修补了上述产品存在的信息泄露漏洞，避免攻击者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/57970>

本周要闻速递

1. Mac 下的 360 “MacKeeper” 曝任意代码执行漏洞

Mackeeper 是一款 Mac OS 系统优化软件，集杀毒、加密、数据备份、系统清理和软件卸载于一身，可以认为是 Mac 下的 360。5 月 7 日，Mackeeper 被发现存在严重的安全漏洞，在其处理 URL 的代码中存在远程代码执行漏洞，当用户访问被恶意构造的网页即可触发高危漏洞，同时当用户访问恶意构造的网站时，几乎不需要交互，就可以以最高系统权限 Root 执行任意代码。此外，漏洞发现人员还公布了 POC（漏洞验证程序）来演示用户用 Safari 访问恶意构造的网站时，可以执行任意代码，在 POC 中执行的代码是卸载 MacKeeper，原因是 MacKeeper 使用自定义 URL 结构执行命令时，未对输入数据做安全检查，导致了任意代码执行。

参考链接：<http://www.freebuf.com/news/66869.html>

2. WordPress 默认主题存在 DOM XSS（跨站脚本）漏洞

WordPress 默认主题存在 DOM XSS（跨站脚本）漏洞，具体的漏洞文件为 example.html。研究表明凡是使用了 genericons 包的 WordPress 插件或主题都会受到这个基于 DOM 的跨站脚本漏洞的影响，因为通常情况下 genericons 包中都含有一个 example.html 文件。影响范围较大的插件包括 JetPack 插件，此外，受影响的还有默认安装的 TwentyFifteen 主题。

参考链接：<http://www.freebuf.com/news/66695.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