

信息安全漏洞周报

2014 年 5 月 26 日-2014 年 6 月 1 日

2014 年第 22 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 159 个，其中高危漏洞 40 个、中危漏洞 98 个、低危漏洞 21 个。上述漏洞中，可利用来实施远程攻击的漏洞有 146 个。本周收录的漏洞中，已有 119 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“Zam Foo 存在多个远程命令执行漏洞”、“Easy File Management Web Server 栈缓冲区溢出漏洞”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、合作伙伴及个人报送了本周收录的全部 159 个漏洞。报送情况如表 1 所示。其中，安天实验室、绿盟科技、天融信、启明星辰等单位报送数量较多。此外，CNCERT 各分中心、习科网络安全、High-Tech Bridge Security Research Lab 及多个白帽子向 CNVD 提交了 70 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
安天实验室	98	0
绿盟科技	91	0
天融信	76	0
启明星辰	71	0
恒安嘉新	50	0
习科网络安全	44	44
CNCERT 山东分中心	7	7

CNCERT 江西分中心	3	3
CNCERT 山西分中心	2	2
CNCERT 黑龙江分中心	1	1
CNCERT 安徽分中心	1	1
CNCERT 新疆分中心	1	1
High-Tech Bridge Security Research Lab	2	2
个人	9	9
报送总计	456	70
录入总计	159（去重）	70

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、WebKit、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	31	20%
2	WebKit	18	11%
3	Cisco	16	10%
4	WordPress	8	5%
5	Apache	6	4%
6	TYPO3	5	3%
7	Drupal	4	3%
8	TeamPass	4	3%
9	Red Hat	3	2%
10	其他	64	39%

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 159 个漏洞。其中应用程序漏洞 98 个，WEB 应用漏洞 38 个，网络设备漏洞 11 个，数据库漏洞 9 个，操作系统漏洞 2 个，安全产品漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	98
WEB 应用漏洞	38
网络设备漏洞	11

数据库漏洞	9
操作系统漏洞	2
安全产品漏洞	1

表 3 漏洞按影响类型统计表

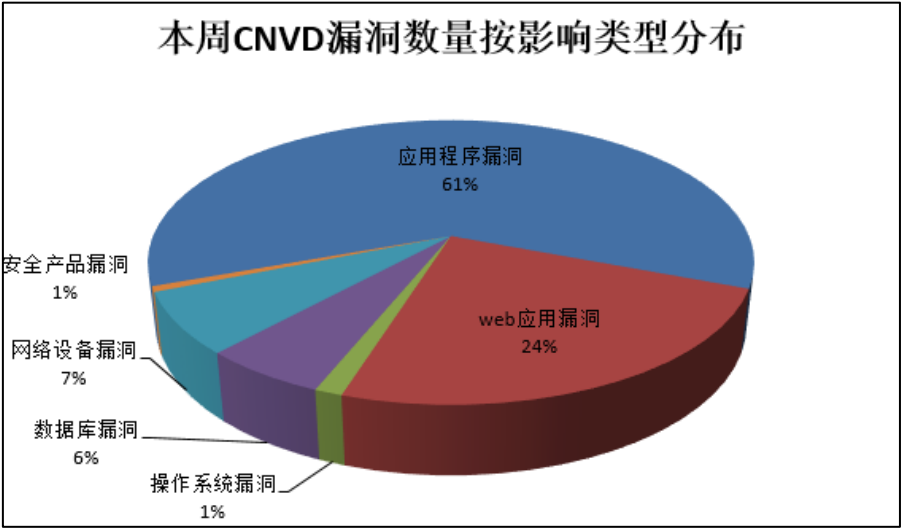


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 23 个电信行业漏洞、1 个移动互联网行业漏洞和 3 个工控行业漏洞（如下列表所示）。其中，“Cisco NX-OS Virtual Device Context SSH 远程权限提升漏洞、Cisco 多个 NX-OS Products Smart Call Home Feature 缓冲区溢出漏洞、Cisco NX-OS MTS 服务远程拒绝服务漏洞、Cisco NX-OS Virtual Device Context SSH Key 远程权限提升漏洞、DIR-505 和 DIR-505L 栈缓冲区溢出漏洞、Cogent Real-Time Systems Cogent DataHub 堆缓冲区溢出漏洞”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-2014-03246	IBM DB2 空指针引用拒绝服务漏洞	中	是
电信	CNVD-2014-03248	IBM DB2 ATS 缓冲区溢出漏洞	中	是
电信	CNVD-2014-03245	Cisco NX-OS Virtual Device Context SSH 远程权限提升漏洞	高	是
电信	CNVD-2014-03244	Cisco 多个 NX-OS Products Smart Call Home Feature 缓冲区溢出漏洞	高	是
电信	CNVD-2014-03249	IBM DB2 'SQLDROWFETCH ()' 函数拒绝服务漏洞	中	是
电信	CNVD-2014-03250	IBM DB2 Server DB2PFCHR 存在未明内存泄露漏洞	中	是
电信	CNVD-2014-03251	Cisco NX-OS MTS 服务远程拒绝服	高	是

		务漏洞		
电信	CNVD-2014-03252	Cisco NX-OS Virtual Device Conte xt SSH Key 远程权限提升漏洞	高	是
电信	CNVD-2014-03257	Cisco Identity Services Engine Web Framework SQL 注入漏洞	中	是
电信	CNVD-2014-03284	Cisco IOS 权限访问漏洞	中	是
电信	CNVD-2014-03302	Cisco IOS XE Software PPPoE 数据 包处理拒绝服务漏洞	中	是
电信	CNVD-2014-03303	IBM DB2 多个产品本地权限提升漏 洞	中	是
电信	CNVD-2014-03317	DIR-505 和 DIR-505L 栈缓冲区溢出 漏洞	高	是
电信	CNVD-2014-03316	多个 IBM 产品安全绕过漏洞（CNV D-2014-03316）	低	是
电信	CNVD-2014-03315	多个 IBM 产品任意文件上传漏洞	中	是
电信	CNVD-2014-03314	多个 IBM 产品 SQL 注入漏洞	中	是
电信	CNVD-2014-03344	多个 IBM 产品'customreport.jsp'跨站 脚本漏洞	低	是
电信	CNVD-2014-03364	Zyxel P-660HW-T1 存在多个跨站请 求伪造漏洞	低	否
电信	CNVD-2014-03378	Apache Tomcat 远程拒绝服务漏洞	中	是
电信	CNVD-2014-03377	Apache Tomcat AJP 请求远程拒绝 服务漏洞	中	是
电信	CNVD-2014-03376	Apache Tomcat 信息泄露漏洞（CNV D-2014-03376）	低	是
电信	CNVD-2014-03375	Apache Tomcat 信息泄露漏洞（CNV D-2014-03375）	低	是
电信	CNVD-2014-03392	多个 IBM 产品跨站脚本漏洞（CNV D-2014-03392）	低	是
移动 互联 网	CNVD-2014-03266	Outlook.com for Android 本地信息 泄露漏洞	低	否
工控 系统	CNVD-2014-03277	Emerson DeltaV '\DeltaV'目录授权 安全绕过漏洞	中	是
工控 系统	CNVD-2014-03278	Emerson DeltaV 硬编码证书安全绕 过漏洞	低	是
工控 系统	CNVD-2014-03282	Cogent Real-Time Systems Cogent DataHub 堆缓冲区溢出漏洞	高	是

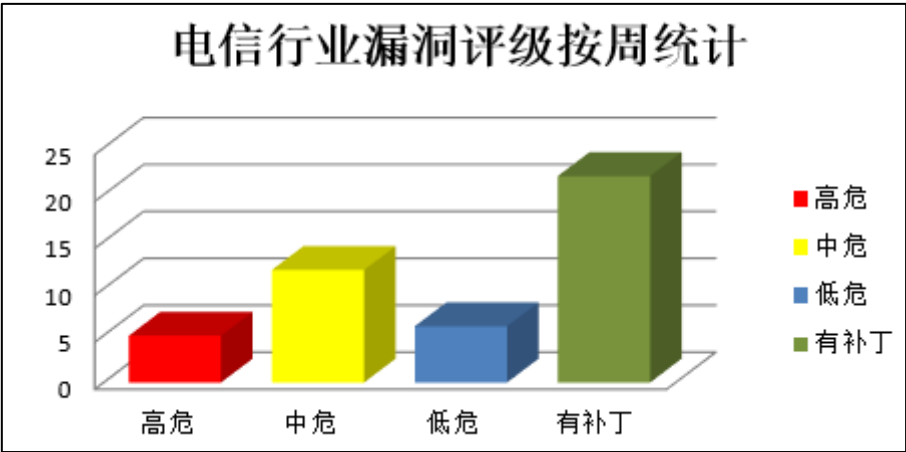


图 1 电信行业漏洞统计

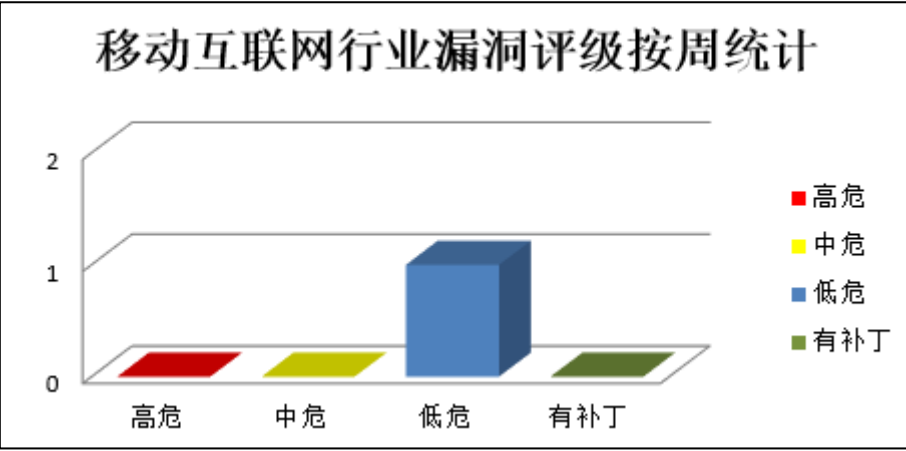


图 2 移动互联网行业漏洞统计

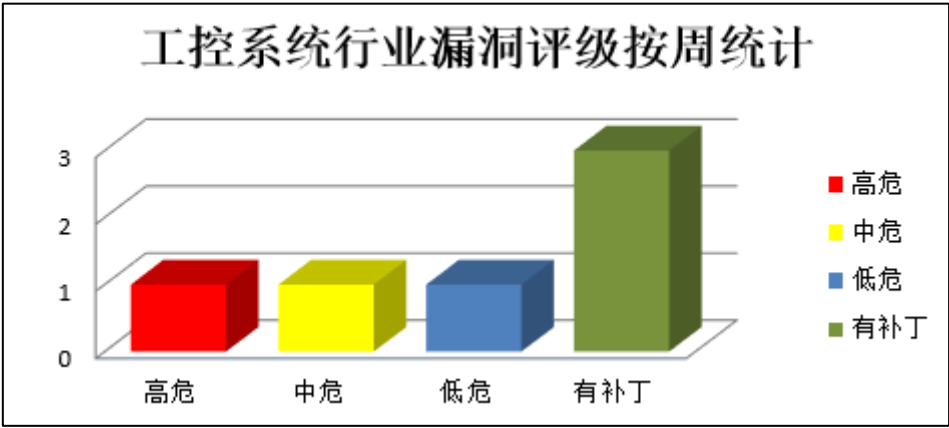


图 3 工控行业漏洞统计



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、ElasticSearch 远程命令执行漏洞

ElasticSearch 是一个基于 Lucene 构建的开源，分布式，RESTful 搜索引擎。近期，该产品被披露存在远程命令执行漏洞。由于 Elasticsearch 用的脚本引擎是 MVEL，该引擎的默认配置打开了动态脚本功能，导致攻击者可以利用工具执行任意代码。该漏洞的综合评级为“高危”。厂商已经发布了漏洞修补程序。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-2014-03397>

2、Cisco 产品安全漏洞

Cisco NX-OS 是一个数据中心级的操作系统；Cisco Tidal Enterprise Scheduler 是一款跨平台的企业工作日程应用软件。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞在受影响的设备上提升权限，执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco NX-OS Virtual Device Context SSH Key 远程权限提升漏洞、Cisco NX-OS MTS 服务远程拒绝服务漏洞、Cisco 多个 NX-OS Products Smart Call Home Feature 缓冲区溢出漏洞、Cisco NX-OS Virtual Device Context SSH 远程权限提升漏洞、Cisco Tidal Enterprise Scheduler 代理本地权限提升漏洞。上述漏洞的综合评级均为“高危”。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-2014-03252>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03251>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03244>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03245>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03242>

3、IBM 产品安全漏洞

IBM DB2 Universal Database Server 是一款大型的商业关系数据库；IBM Tivoli Storage Manager 是一款遵循 ANSI SAN 标准的可扩展解决方案；IBM Sametime 是一套社交通信工具；IBM Maximo Asset Management 是一套综合性资产生命周期和维护管理的解决方案。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、提升权限或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：IBM DB2 / DB2 Connect 特权提升漏洞、IBM Tivoli Storage Manager Server 本地未授权访问漏洞、IBM Maximo Asset Management 和 SmartCloud Control Desk 信息泄露漏洞、IBM Sametime Meeting Server 存在未明漏洞、IBM Sametime Meeting Server 拒绝服务漏洞。其中“IBM DB2 / DB2 Connect 特权提升漏洞”的综合评级为“高危”。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-2014-03323>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03322>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03338>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03389>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03387>

4、WebKit 产品安全漏洞

WebKit 是一个开源的浏览器引擎，也是苹果 Mac OS X 系统引擎框架版本的名称。本周，上述产品被披露存在内存破坏漏洞，攻击者可利用漏洞在受影响浏览器上下文中执行任意代码。

CNVD 收录的相关漏洞包括：WebKit 内存破坏漏洞（CNVD-2014-03286、CNVD-2014-03285、CNVD-2014-03288、CNVD-2014-03287、CNVD-2014-03289）。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-2014-03286>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03285>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03288>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03287>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03289>

5、TYPO3 安全漏洞

TYPO3 是一款开源的内容管理系统。本周，该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、执行未授权操作或任意代码。

CNVD 收录的相关漏洞包括：TYPO3 存在未明 PHP 对象注入漏洞、TYPO3 power mail Extension 存在多个漏洞、TYPO3 存在多个漏洞、TYPO3 验证子件安全绕过漏洞、TYPO3 会话劫持漏洞。其中，除“TYPO3 验证子件安全绕过漏洞、TYPO3 会话劫持漏洞”外，上述漏洞的综合评级均为“高危”。厂商已发布了上述漏洞的修补程序。CNVD 提醒相关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-2014-03343>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03320>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03321>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03342>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03341>

6、Enquete yS SQL 注入漏洞

Enquete yS 是一套投票系统。本周，Enquete 被披露存在综合评级为“高危”的 SQL 注入漏洞。攻击者利用漏洞可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-2014-03311>

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-2014-03354	Links Directory 'header.phpsub_result'参数 SQL 注入漏洞	高	暂无
CNVD-2014-03369	Red Hat OpenShift Enterprise 默认密码漏洞	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://github.com/openshift/openshift-extras/blob/enterprise-2.1/enterprise/install-scripts/generic/openshift.sh
CNVD-2014-03363	DirectFB 存在多个缓冲区溢出漏洞	高	暂无
CNVD-2014-03362	TeamPass '/upload/upload.files.php' Crafted PHPSESSID 任意文件上传漏洞	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://github.com/nilsteampassnet/TeamPass/commit/fd549b245c0f639a8d47bf4f74f92c37c053706f https://github.com/nilsteampassnet/TeamPass/commit/8820c8934d9ba0508ac345e73ad0be29049ec6de
CNVD-2014-03361	TeamPass 'sources/main.queries.php' SQL 注入漏洞	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://github.com/nilsteampassnet/TeamPass/commit/8820c8934d9ba0508ac345e73ad0be29049ec6de
CNVD-2014-03360	TeamPass '/sources/datatable/datable.kb.php'参数 SQL 注入漏洞	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://github.com/nilsteampassnet/TeamPass/commit/fd549b245c0f639a8d47bf4f74f92c37c053706f
CNVD-2014-03383	CoSoSys Endpoint Protector 存在多个漏洞	高	暂无
CNVD-2014-03382	DirectFB 'Dispatch_Write()'函数缓冲区溢出漏洞	高	暂无
CNVD-2014-03381	Red Hat OpenShift Enterprise 'rubygem-openshift-origin-node'本地命令注入漏洞	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://rhn.redhat.com/errata/RHSA-2014-0530.html
CNVD-2014-03395	Ruby 'string.c'远程内存破坏漏洞	高	用户可联系供应商获得补丁信息： http://www.ruby-lang.org/

表 3 部分高危漏洞列表

小结：本周，ElasticSearch 被披露存在远程命令执行漏洞，攻击者可以利用工具执行任意代码。Cisco、IBM、WebKit、TYPO3 多款产品被披露存在多个漏洞，攻击者利用漏洞可获取敏感信息、提升权限或执行任意代码。此外，Enquete 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。

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、EMC 修补 Documentum D2 产品漏洞

EMC Documentum D2 是企业文档管理解决方案。

本周，EMC 修补了 Documentum D2 存在的权限提升漏洞，避免经过身份验证的远程用户通过调用 core 或 D2FS web-service 方法，利用此漏洞绕过目标访问限制，并执行任意 DQL 查询。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/45911>

本周要闻速递

1. Safari 7.0.4 浏览器修补 22 个安全漏洞

苹果上周为 OS X 10.9 以及 OS X 10.8 更新了 Safari，目前的最新版本为 7.0.4。苹果在更新日志中表示，最新版本的 Safari 修复了与 Webkit 相关的两个 bug。本次更新修复的安全漏洞多达 22 个，其中有 21 个可导致任意远程代码执行，如果用户仍然保留老版本的 Safari，系统很可能会因为遭受攻击而瘫痪。建议 OS X 10.9 和 OS X 10.8 用户进行升级。

参考链接：<http://tools.yesky.com/178/37407178.shtml>

2. WordPress 存在安全漏洞

WordPress 存在一个安全漏洞，由于未加密的 cookie 可能导致用户的个人资料泄露，当用户访问 WordPress 的时候，该网站会发送一个 cookie，但是这个 cookie 是以纯文本形式发送的，并没有经过加密。也就是说如果该 cookie 被拦截就有可能被利用。并且测试结果表明，通过截取 cookie 获得的信息可以让黑客毫无障碍的通过验证，并对用户的 email、博客和私信等进行修改。

参考链接：<http://tech.sina.com.cn/s/2014-05-29/08199407554.shtml>

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