# 迪普科技 2018 年 10 月

# 信息安全研究月报

杭州迪普科技股份有限公司

Hangzhou DPTech Technologies Co.，Ltd.

# 目 录



 

## 一、 安全漏洞态势

2018 年 10 月份新增安全漏洞 1441 个。比上月增加了 250 个，与前 5 个月平均数量相比，安全漏洞数量大幅增加。本月新增的漏洞中，高危漏洞 13 个，中危漏洞 177 个，低危漏洞 1251 个，同比 2017 年 10 月（漏洞总数 795 个）增加 81.26%。表 1-1 为 2018 年 5 月-2018 年 10 月漏洞危险等级统计。

**表 1-1 2018 年 5 月-2018 年 10 月漏洞危险等级统计**

| | 五月 | 六月 | 七月 | 八月 | 九月 | 十月 |
|---|---|---|---|---|---|---|
| 高危 | 48 | 58 | 10 | 80 | 4 | 13 |
| 中危 | 65 | 115 | 320 | 661 | 14 | 177 |
| 低危 | 5 | 4 | 1593 | 197 | 1173 | 1251 |
| 总数 | 118 | 177 | 1923 | 938 | 1191 | 1441 |

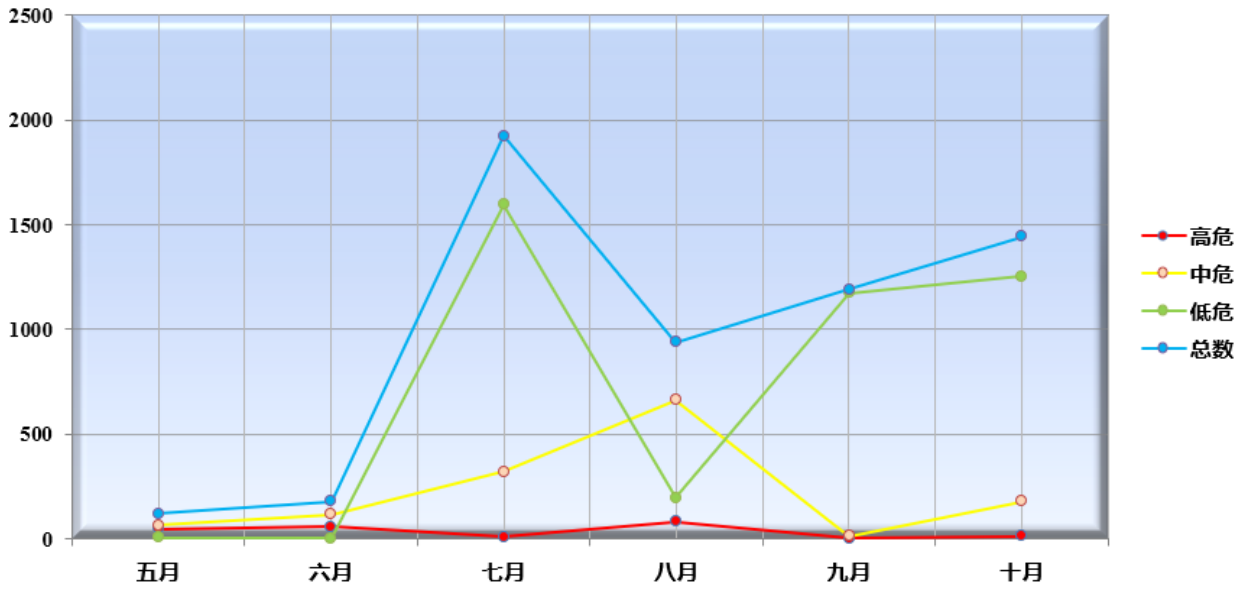


**图 1-1 2018 年 5 月-2018 年 10 月漏洞新增数量趋势**

## 二、 漏洞类型分布

2018 年 10 月份新增的漏洞类型分布如表 1-2 所示。其中跨站脚本，占 12.91%。值得关注的还有信息泄露、SQL 注入、跨站请求伪造等常见漏洞类型。

**表 1-2 2018 年 10 月漏洞类型分布**

| 类型 | 数量 | 比例 |
|---|---|---|
| 未知 | 1001 | 69.47% |
| 跨站脚本 | 186 | 12.91% |
| 跨站请求伪造 | 32 | 2.22% |
| 信息泄露 | 45 | 3.12% |
| SQL 注入 | 36 | 2.50% |
| 权限许可和访问控制 | 32 | 2.22% |
| 路径遍历 | 15 | 1.04% |
| 输入验证 | 44 | 3.05% |
| 数字错误 | 11 | 0.76% |
| 资源管理错误 | 17 | 1.18% |
| 其他 | 22 | 1.53% |

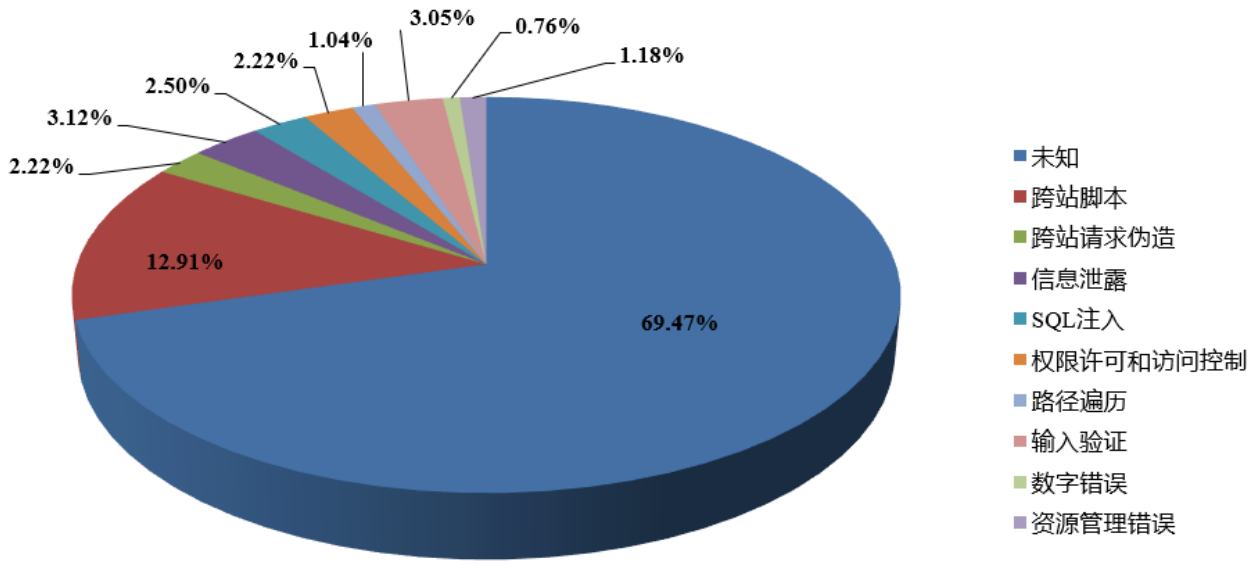


**图 1-2 2018 年 10 月漏洞类型占比**

## 三、 高危漏洞实例

### (一)ThinkPHP SQL 注入漏洞

**CVE 编号：**CVE-2018-18529

**CNNVD 编号：**CNNVD-201810-1109

**发布时间：**2018-10

**危险等级：** ☆☆☆☆

**漏洞类型：** SQL 注入

**受影响软件：**

ThinkPHP 3.2.4

**漏洞描述：** ThinkPHP 是一款快速、兼容而且简单的轻量级国产 PHP 开发框架，可以解决应用开发中的大多数需要。

该漏洞与 Library/Think/Db/Driver/Mysql.class.php 中的 parseKey 函数没有正确处理 key 参数有关，从而引起 SQL 注入漏洞，攻击者可以利用该漏洞获取数据库中的敏感数据，造成敏感数据泄露，甚至控制受影响的服务器。

攻击者可以利用该漏洞进行 SQL 注入，危害系统安全。

**修补建议：** 目前厂商已发布补丁以规避该风险，补丁获取链接：

http://www.thinkphp.cn/

**(一) OpenSSL 旁道攻击信息泄露漏洞**

**CVE 编号：** CVE-2018-0734

**CNNVD 编号：** CNNVD-201810-1435

**发布时间：** 2018-10

**危险等级：** ☆☆☆

**漏洞类型：** 设计缺陷

**受影响软件：**

OpenSSL 1.1.1

OpenSSL 1.1.0-1.1.0i

OpenSSL 1.0.2-1.0.2p

**漏洞描述：** OpenSSL 是一个强大的安全套接字层密码库，其囊括了目前主流的密码算法，常用的密钥，证书封装管理功能以及 SSL 协议，并提供丰富的应用程序供测试或其它目的使用。

该漏洞与 DSA 签名算法存在定时旁路信道攻击有关。攻击者可以利用该漏洞使用签名算法中的变量来恢复私钥，影响系统安全。

攻击者可以利用该漏洞恢复私钥，危害系统安全。

 

**修补建议：**目前厂商已发布补丁以规避该风险，补丁获取链接：

https://www.openssl.org/news/secadv/20181030.txt

**(二) WordPress WPML 插件跨站脚本漏洞**

**CVE 编号：**CVE-2018-18069

**CNNVD 编号：**CNNVD-201810-290

**发布时间：**2018-10

**危险等级：**☆☆

**漏洞类型：**跨站脚本

**受影响软件：**

WordPress WPML <= 3.6.3

**漏洞描述：**WordPress 是一种使用 PHP 语言开发的博客平台，该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。在国际上广泛使用了，可以兼容自开发的插件。功能强大，应用广泛。

该漏洞是由于程序未对‘locale_file_name_’参数进行正确的过滤，与‘process_forms’函数有关，攻击者可以利用该漏洞向 wp-admin/admin.php 文件发送请求注入任意的恶意 Web 脚本或 HTML 代码。

攻击者可以利用该漏洞进行跨站脚本攻击，危害系统安全。

**修补建议：**目前厂商还未发布补丁，厂商链接：http://wpml.org

**(三) Joomla!安全漏洞**

**CVE 编号：**CVE-2018-17855

**CNNVD 编号：**CNNVD-201810-474

**发布时间：**2018-10

**危险等级：**☆☆

**漏洞类型：**设计缺陷

**受影响软件：**

Joomla! 1.5.0 - 3.8.12

 

**漏洞描述：**Joomla!是 Open SourceMatters 团队开发的一套开源的使用 PHP 语言和 MySQL 数据库的内容管理系统(CMS)，是网站的一个基础管理平台。可以在 Linux、Windows、MacOSX 等各种不同的平台上执行。

该漏洞与 com_users 有关，如果攻击者访问了可以在注册过程中批准管理验证的用户的邮件帐户，可以利用该漏洞激活自己的邮件账户。

攻击者可以利用该漏洞激活自己的邮件账户，危害系统安全。

**修补建议：**目前厂商已发布补丁以规避该风险，补丁获取链接：

https://developer.joomla.org/security-centre/754-20181004-core-acl-violation-in-com-users-for-the-admin-verification

**(四)Apache Tomcat URL 重定向漏洞**

**CVE 编号：**CVE-2018-11784

**CNNVD 编号：**CNNVD-201810-135

**发布时间：**2018-10

**危险等级：**☆☆

**漏洞类型：**设计缺陷

**受影响软件：**

Apache Tomcat 9.0.X < 9.0.12

Apache Tomcat 8.5.X < 8.5.34

Apache Tomcat 7.0.X < 7.0.91

**漏洞描述：**Apache Tomcat 是美国 Apache 软件基金会的 Jakarta 项目的一款轻量级免费的开放源代码的 Web 应用服务器，主要用于开发和调试 JSP 程序。

该漏洞与 Apache Tomcat 没有正确过滤用户的输入有关。攻击者可以利用精心设计的 URL 诱使用户点击并跳转到攻击者控制的站点，从而发起网络钓鱼攻击。

攻击者可以利用该漏洞发起网络钓鱼攻击，危害系统安全。

**修补建议：**目前厂商已发布补丁以规避该风险，补丁获取链接：

https://lists.apache.org/thread.html/23134c9b5a23892a205dc140cdd8c9c0add233600f76b313dda6bd75@%3Cannounce.tomcat.apache.org%3E

 

## 四、 本月安全要闻

### (一)冰岛史上最大网络攻击行动：黑客冒充警方欺诈民众

10 月 15 日下午消息，据中国台湾地区媒体报道，安全厂商 Cyren 揭露，有数千名冰岛民众在上周收到了网络钓鱼邮件，而且黑客是以冰岛警方的名义发送邮件，还建立了可以假乱真的官方网站，企图于使用者电脑上植入恶意程式并记录受害者所输入的机密资讯。由于冰岛的人口只有 35 万，因此这一攻击已被视为是冰岛史上最大的网络攻击行动。

这一攻击行动始于今年 10 月 6 日，黑客以所入侵的帐号注册了 www.logregian.is 网域名称，与冰岛警方的官网 www.logreglan.is 只差了一个字母，并在邮件中威胁使用者若不遵守规定可能会遭到逮捕，继之提供来自伪造网站的连结。

当使用者造访假冒的警察网站时，会被要求输入社会安全码，输入之后，该站竟然能够验证使用者的身分，从而跳出使用者的姓名，还要求使用者输入邮件中所附的验证码以再次验明正身。

至此使用者几乎已不再怀疑，很容易就会听从网页上的指示，下载一个具密码保护的.rar 档案，输入网页上所提供的密码，解压缩后则会出现一个 Yfirvold.exe 执行档，这是个兼具键盘侧录功能的远端存取木马，执行后会开始搜集存放于浏览器中的机密资讯并侧录键盘，再将资料上传至黑客设于德国与荷兰的远端服务器。

Cyren 表示，该恶意程式明确锁定了冰岛民众，因为它会检查受害者是否造访冰岛主要的多家网络银行。

冰岛警方已认定这是冰岛迄今所出现的最大的网络攻击行动，也已确认许多收件人都已沦为受害者，并根据电子邮件及网站所使用的文字，以及黑客所拥有的冰岛民众资料，相信它是由内贼所为。

友情链接：http://hackernews.cc/archives/24276

### (二)美国中期选举将近 3500 万人资料泄漏，黑客：在政府有人

10 月 17 日下午消息，据中国台湾地区媒体报道，随着美国中期选举即将于下个月展开，威胁情报业者 Anomali Labs 及网络安全业者 Intel 471 本周一联手揭露他们发现有人在某个黑客论坛中兜售美国 19 州的选民资料，其中 3 州的选民资料就高达 2,300 万人，估计总数将超过 3,500 万人，且根据研究人员的查证，这些资料的可信度很高。

 

每一州的选民资料价格不同，视州别及数量从 150 美元到 12,500 美元不等，例如路易斯安那州 300 万选民资料的价格为 1,300 美元，而德州的 1,400 万选民资料即要价 12,500 美元；资料内容包含选民的姓名、电话、地址及投票纪录等，卖家甚至承诺会每周更新资料。

根据卖家的说法，他们在州政府内部有人，可每周收到最新资料，有时还要亲自到该州取得资料。意谓着这些资料的外泄不一定是来自于技术上的入侵，而很可能是有心人士自合法管道取得选民资料后恶意进行的散布。

不管资料来源如何，暗网中已经有人发动众筹来购买这些名单，并打算于黑客论坛上公布所购得的选民资料，已成功集资 200 美元，买下了堪萨斯州选民名单，亦已开放论坛用户下载。

研究人员指出，选民名单应是不能用在商业目的，也不得在网络上公布，却有未经授权的组织企图利用这些名单获利，选民名单曝光的选民资料再加上诸如社会安全码或驾照等外泄资料，可能会被犯罪份子用来进行身分诈骗或其它非法行为。

友情链接：http://hackernews.cc/archives/24289

**(三)国泰航空 940 万名乘客个人数据在 3 月被盗，包含出行地点数据**

据外媒报道，日前大型国际航空公司国泰航空披露，在今年 3 月发生的一次数据泄露事件中，该公司的 940 万名乘客的记录被盗，另外含有姓名、出生日期、住址等个人信息的护照信息也可能已经泄露。据悉，此次事件还涉及到了每位乘客的具体出行地点以及客户服务代表的评论等等。

另外，国泰航空还指出，有 403 个过期信用卡卡号、27 个没有 CVV 号码的信用卡卡号遭到访问。

这家航空公司在周三发布的声明中指出，公司目前没有任何证据显示任何一名乘客的信息遭到滥用，而受影响的 IT 系统则完全跟其飞行操作系统独立开来，所以该次网络攻击事件对其飞行安全不会带来影响。此外，国泰航空表示，没有密码遭到泄露。

国泰航空总部位于中国香港，但它的服务遍布全球包括北美、欧洲、中国内地、中国台湾地区、日本、东南亚和中东。

这家公司选择在 6 个月后公布数据泄露事件的做法也许会在欧洲市场遇到阻碍，因为那边最新通过的通用数据保护条例要求公司在发现违规情况三天后就要告知客户和执法部门。

 

此外，国泰航空表示，他们现在正在与中国香港警方以及相关部门沟通。而认为自己可能受到影响的客户可以访问 infosecurity.cathaypacific.com 或直接拨打公司电话或发电子邮件来获取进一步的信息。

友情链接：http://news.zgswcn.com/2018/1025/858347.shtml

**(四)branch.io 漏洞令 6.85 亿网民面临跨站攻击**

漏洞挖掘人员发现重大安全漏洞，影响 Tinder、Yelp、Shopify、西联等主流网站，使用这些站点的数亿用户均受威胁。

研究人员是在挖掘约会网站网页代码时发现的该可利用编程缺陷。在 Tinder.com 的子域名 go.tinder.com 上发现了跨站脚本漏洞后，研究人员向 Tinder 应用的开发商提交了漏洞报告。

后来发现，他们挖出的这个漏洞不仅仅是约会网站某个子域名的问题。安全公司 VPNMentor 的研究团队称，该现已修复的安全漏洞曾令多达 6.85 亿网民暴露在跨站脚本攻击(XSS)风险之下，黑客可通过该漏洞盗取数据和劫持账户。登录了受影响服务的用户只要点击了恶意链接或打开了陷阱网页，就可能成为跨站脚本攻击的受害者。

受影响用户数高达 9 位数是因为该安全问题实际上存在于名为 branch.io 的工具集中。该工具集用于跟踪网站和 App 用户，确定他们的来路，比如是从 Facebook、电子邮件链接、推特还是从别的什么应用点进来的。因为该漏洞埋藏在 branch.io 的代码中，嵌入到了无数服务和移动应用里，所以可能面临跨站脚本攻击的人数飙升至近 7 亿。

本周早些时候，发现该漏洞的 Ariel Hochstad 解释称：

我们一发现这些漏洞就立即通过负责任披露程序联系了 Tinder，并与他们合作共同解决问题。我们了解到该脆弱终端并非 Tinder 所有，而是属于 branch.io——全球很多大公司都会使用的溯源平台。

美国大型评论网站 Yelp、电汇公司西联、Shopify 和照片分享站点 Imgur 都在用该脆弱组件。Hochstadt 估测受影响网站用户账户数在 6.85 亿左右。

漏洞本身是个极讨厌的文档对象模型(DOM)跨站脚本表单，能使攻击者透过跨站调用通过基本安全检查。

 

基于 DOM 的跨站脚本攻击中，HTML 源代码和攻击的响应是一模一样的。也就是说，响应中是找不到恶意攻击载荷的，Chrome XSS Auditor 之类浏览器内置 XSS 缓解功能很难检测出来。

branch.io 号称全球每月用户超 20 亿，但其发言人对此事没有任何评论。

Hochstadt 表示曾私下向 branch.io 报告过该问题，branch.io 也有能力修复该漏洞，而目前尚未发现该漏洞被利用的案例。但用户仍应考虑修改口令，并密切注意自己的账户有没有什么可疑的行为。

友情链接：https://www.aqniu.com/news-views/39550.html

**(五)FitMetrix 健身软件开发公司 119GB 用户数据被指在线暴露**

据外媒 ZDNet 报道，大量 FitMetrix 用户的个人资料被国际网络安全咨询公司 Hacken 的网络风险研究总监 Bob Diachenko 发现通过一组 ElasticSearch 服务器暴露在了网络上，所包含数据的总大小超过 119GB。

根据 Diachenko 的说法，他是在本月 5 日通过 Shodan 搜索引擎发现这组 ElasticSearch 服务的，无需密码即可查看数据。这也就意味着，任何知道该服务器 IP 地址的人都可以随意访问大量的 FitMetrix 用户个人资料。

根据 FitMetrix 官网显示的信息，它是一家为健身房、工作室、企业健康计划和医疗保健专业人士提供心率监测软件的公司。该公司成立于 2013 年，在今年早些时候已经被总部位于美国加州圣路易斯奥比斯波的另一家健身房软件开发公司 Mindbody 收购。

Diachenko 告诉 ZDNet，FitMetrix 通过这台服务器暴露的不仅限于用户个人资料，还包括一些有关设施和其他数据点的信息。具体来讲，主要涉及的信息包括用户姓名、性别、出生日期、电子邮箱地址、用户名、身高体重，以及各种 FitMetrix 计划指标。

Diachenko 还告诉 ZDNet，虽然能够确定这组服务器至少包含了 119GB 的数据，但他无法确定具体受影响的 FitMetrix 用户数量。从 MindBody 提交给美国证券交易委员会的文件来看，该公司声称每月活跃用户超过 3500 万，但尚不清楚其中有多少人正在使用由 FitMetrix 开发的软件。

此外，Diachenko 还表示，这组服务器还暴露了一个似乎用于管理 FitMetrix 服务器基础架构的 API 密钥。不仅如此，Diachenko 还在服务器上发现了一封勒索信，似乎是由远程攻击者留下的，内容如下：

 

"ALL YOUR INDEX AND ELASTICSEARCH DATA HAVE BEEN BACKED UP AT OUR SERVERS, TO RESTORE SEND 0.1 BTC TO THIS BITCOIN ADDRESS 14ARsVT9vbK4uJzi78cSWh1NKyiA2fFJf3 THEN SEND AN EMAIL WITH YOUR SERVER IP, DO NOT WORRY, WE CAN NEGOCIATE IF CAN NOT PAY"

根据 Diachenko 的说法，这封勒索信创建于 2017 年 1 月份。虽然攻击者很可能只是想通过恐吓来勒索赎金，但这也意味着现在至少已经有两个人发现了这组在线暴露的服务器——Bob Diachenko 和这名攻击者。是否还有其他人发现，以及数据是否已经被泄露，尚不清楚。

在发现该服务器之后，Diachenko 曾多次试图与 Mindbody 取得联系，但均没有成功。不过，从目前的情况来看，Mindbody 似乎已经意识到了这个问题，因为这组服务器已经不再能够被公开访问。

“我们最近意识到，与在线存储的 FitMetrix 技术相关的某些数据可能已被暴露，而我们已经采取了措施来解决这个问题。” MINDBODY 首席信息安全官 Jason Loomis 在回复给 ZDNet 的电子邮件中表示，“目前的迹象表明，这些数据的确包含了由 FitMetrix 管理的消费者信息，这些数据已经于 2018 年 2 月被 Mindbody 收购，但并不包括任何登录凭证、密码、信用卡信息或个人健康信息。”

Loomis 还表示，Mindbody 会严肃对待客户和消费者隐私和数据的安全，并将通过此次事件不断改善其安全现状。

友情链接：https://www.hackeye.net/securityevent/16731.aspx

 