迪普科技 2018 年 4 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 4 月份新增安全漏洞 377 个。比上月减少了 96 个，与前 5 个月平均数量相比，安全漏洞数量小幅减少。本月新增的漏洞中，高危漏洞 125 个，中危漏洞 211 个，低危漏洞 41 个，同比 2017 年 4 月（漏洞总数 1196 个）减少 68.48%。表 1-1 为 2017 年 11 月-2018 年 4 月漏洞危险等级统计。

表 1-1 2017 年 11 月-2018 年 4 月漏洞危险等级统计

	十一月	十二月	一月	二月	三月	四月
高危	282	392	237	367	144	125
中危	287	247	438	502	277	211
低危	89	31	121	112	52	41
总数	658	670	796	981	473	377

图 1-1 2017 年 11 月-2018 年 4 月漏洞新增数量趋势

二、 漏洞类型分布

2018 年 4 月份新增的漏洞类型分布如表 1-2 所示。其中缓冲区溢出，占 6.90%。值得关注的还有跨站脚本等常见漏洞类型。

表 1-2 2018 年 4 月漏洞类型分布

类型	数量	比例
缓冲区溢出	26	6.90%
权限许可和访问控制	12	3.18%
信息泄露	10	2.65%
输入验证	10	2.65%
跨站脚本	25	6.63%
资源管理错误	11	2.92%
未知	263	69.76%
跨站请求伪造	9	2.39%
代码注入	1	0.27%
路径遍历	3	0.80%
其他	7	1.86%

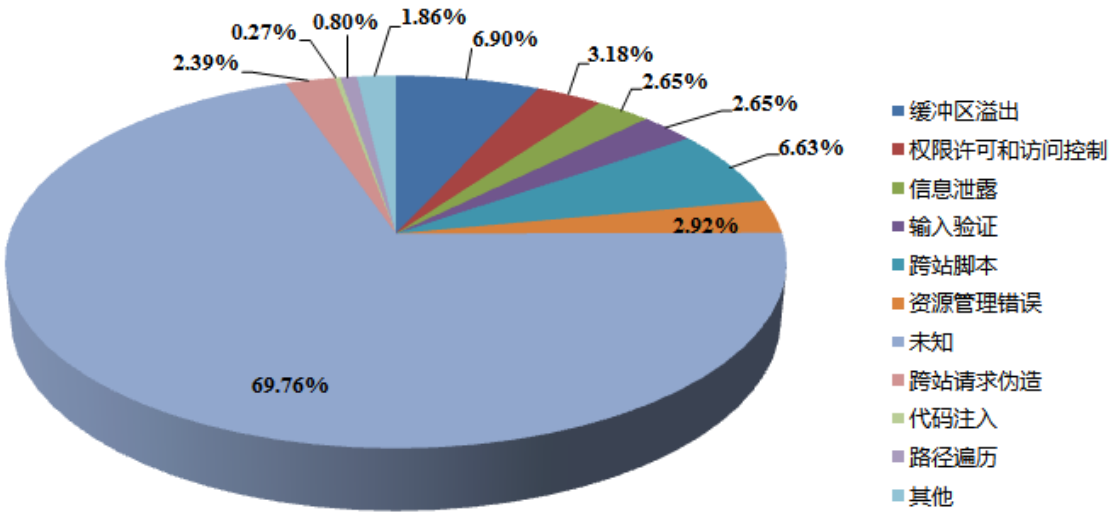

图 1-2 2018 年 4 月漏洞类型占比

三、 高危漏洞实例

(一) Oracle WebLogic Server WLS 核心组件远程代码执行漏洞

CVE 编号：CVE-2018-2628

CNNVD 编号：CNNVD-201804-803

发布时间：2018-04

危险等级：☆☆☆☆

漏洞类型：远程代码执行

受影响软件：

Oracle WebLogic Server 10.3.6.0

Oracle WebLogic Server 12.1.3.0

Oracle WebLogic Server 12.2.1.2

Oracle WebLogic Server 12.2.1.3

漏洞描述：WebLogic 是美国 Oracle 公司使用 J2EE 技术开发的一款应用服务中间件，支持应用开发、生产、应用和部署的整个生命周期的管理。在 WebLogic 的默认配置中，T3 协议默认开启，用来作为 WebLogic 和其他 Java 程序通信的通道。

该漏洞使用 T3 服务协议，攻击者通过将要执行的代码进行反序列化操作，然后将数据通过 T3 协议发送至服务器端，服务端在反序列化操作过程中会远程加载 RMI registry，获得的 registry 又会被反序列化执行，最终实现远程命令执行。

修补建议：目前厂商已经发布了升级补丁，补丁获取链接：

http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html

(二) Oracle Enterprise Manager Products Suite Enterprise Manager Ops Center 组件访问控制错误漏洞

CVE 编号：CVE-2018-2742

CNNVD 编号：CNNVD-201804-1273

发布时间：2018-04

危险等级：☆☆☆☆

漏洞类型：越权

受影响软件：

Enterprise Manager Ops Center 组件 12.2.2 版本

Enterprise Manager Ops Center 组件 12.3.3 版本

漏洞描述：Oracle Enterprise Manager Products Suite 是美国甲骨文（Oracle）公司的一套企业内部部署管理平台。Enterprise Manager Ops Center 是其中的一个企业数据中心监控管理组件。

该漏洞存在于 Oracle Enterprise Manager Products Suite 中的 Enterprise Manager Ops Center 组件的 Framework 子组件中，利用该漏洞攻击者可以读取、更新、插入和删除系统中的数据，甚至造成拒绝服务攻击。

攻击者可以利用该漏洞越权操作系统中的数据，危害系统安全。

修补建议：目前厂商已经发布了升级补丁，补丁获取链接：

http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html

(三)Drupal Core 远程代码执行漏洞

CVE 编号：CVE-2018-7602

CNNVD 编号：CNNVD-201804-1490

发布时间：2018-04

危险等级：☆☆☆☆

漏洞类型：远程代码执行

受影响软件：

Drupal 的 7.x 版

Drupal 的 8.x 版

漏洞描述：Drupal 是由 Drupal 社区维护的一款 PHP 语言开发、由内容管理框架和 PHP 开发框架共同组成的免费且开源的内容管理框架。

该漏洞和 2018 年 3 月份发布的 Drupal Core 远程代码执行漏洞有关，由于 Durpal 官方对漏洞修复不完全，导致补丁被绕过，进而实现远程代码执行。

攻击者可以利用该漏洞远程执行恶意代码，危害系统安全。

修补建议：尽快打上该漏洞官方补丁或者升级到最新稳定版本。目前厂商已经发布了升级补丁，补丁获取链接：

1、8.x 版本：

https://cgit.drupalcode.org/drupal/rawdiff/?h=8.5.x&id=bb6d396609600d1169da29456ba3db59abae4b7e

2、7.x 版本：

https://cgit.drupalcode.org/drupal/rawdiff/?h=7.x&id=080daa38f265ea28444c540832509a48861587d0

(四)WordPress Catapult UK Cookie Consent 插件跨站脚本漏洞

CVE 编号：CVE-2018-10310

CNNVD 编号：CNNVD-201804-1458

发布时间：2018-04

危险等级：☆☆☆

漏洞类型：跨站脚本

受影响软件：

WordPress Catapult UK Cookie Consent 插件版本小于 2.3.10

漏洞描述：Wordpress CMS 是使用 PHP 语言开发的一款适用于个人、中小企业的博客内容发布平台，该平台允许通过简单的配置即可快速搭建一个站点。Catapult UK Cookie Consent 是 Wordpress 中一个添加缓存通知栏的插件。

由于在 Catapult UK Cookie Consent 小于 2.3.10 的版本中，代码未将用户的输入数据进行充分的过滤，导致存在跨站脚本漏洞。攻击者通过通过构造特定的请求可以在正常用户的浏览器中执行任意的脚本代码。

攻击者可以利用该漏洞执行任意脚本代码，危害系统安全。

修补建议：目前厂商已经发布了升级补丁，补丁获取链接：

https://wordpress.org/plugins/uk-cookie-consent/#developers

(五)Google Chrome WebGL 缓冲区错误漏洞

CVE 编号：CVE-2018-6073

CNNVD 编号：CNNVD-201804-442

发布时间：2018-04

危险等级：☆☆☆☆

漏洞类型：缓冲区溢出

受影响软件：

Google Chrome 版本小于 65.0.3325.146

漏洞描述：Chrome 是 Google 旗下的一款桌面 Web 浏览器，WebGL 是 Chrome 中的一个绘图标准。

该漏洞存在于 Google Chrome 小于 65.0.3325.146 的版本中，由于程序没有正确的执行边界检测，导致 WebGL 中存在堆缓冲区溢出漏洞。攻击者通过诱导受害者浏览特定的网页触发该漏洞，最终可以使得攻击者在受害者系统中执行任意代码或者造成拒绝服务。

攻击者可以利用该漏洞导致缓冲区溢出，造成任意代码执行或者拒绝服务攻击，使程序崩溃。

修补建议：目前厂商已经发布了升级补丁以修复此漏洞，补丁获取链接：

https://chromereleases.googleblog.com/2018/03/stable-channel-update-for-desktop.html

四、 本月安全要闻

(一)芬兰赫尔辛基新企业中心数据泄露，超过 13 万芬兰公民成事件受害者

根据芬兰媒体 Svenska Yle 的报道，超过 13 万名芬兰公民似乎已经成为了数据泄露事件的最新受害者。而从受害者数量来看，这将是该国有史以来发生的第三大数据泄露事件。

芬兰通信管理局（FICORA）于本周五通过自己的网站向所有芬兰公民发出警告称，一个由赫尔辛基新企业中心（“Helsingin Uusyrityskeskus”）负责维护的网站（liiketoimintasuunnitelma[.]com）在本周二遭遇了匿名黑客的攻击，大约有 13 万用户的账户用户名和密码被窃取，同时被窃取的还包括其他一些机密信息。

在芬兰，任何想要创业的人都可以通过一些机构获得免费的企业咨询，如新企业中心（Uusyrityskeskus）、经济交通和环境中心（Elinkeino-,liikenne- ja ympäristökeskus，即 ELY-keskus）、劳动与经济发展办公室（Työ- ja elinkeinotoimisto，即 TE-toimisto）和创业-芬兰（Yritys-Suomi）。

在完成合理的商业构想之后，创业者可以联系这些机构，以获得来自专业人士提供的商业运作发展咨询和帮助。机构的工作人员会帮助创业者进行全面的市场调查、可行性数据分析并调查获得资金的可能性。创业者也可以获得关于如何制定创业计划的咨询，并在做出创业决定时得到支持。

Liiketoimintasuunnitelma 就是这样一个网站，其目的在于帮助注册用户分析公司的整体业务以及阐明预期的企业盈利能力和成功前景，这对于在芬兰投资的创业者来说很有帮助。

FICORA 表示，该网站并没有对存储的任何信息进行加密，无论是用户名还是密码都采用明文形式进行储存，这使得网络犯罪分子更容易利用它们。

在本周二了解到这起网络攻击事件之后，Helsingin Uusyrityskeskus 立即关闭了受影响的网站，并在网站主页上发布了关于该事件的新闻稿。

赫尔辛基新企业中心董事会主席 JarmoHyökyvaara 在新闻稿中表示：“我们对于所有可能因这起犯罪而遭受精神或经济损失的用户表示抱歉。不幸的是，我们目前还不能确定具体有多少人，以及有哪些具体信息受到影响。我们已经就此事通知了警方，因此受影响的用户无需再单独通知警方。”

JarmoHyökyvaara 还强调，注册用户的个人详细资料并不存储在受影响的网站上，因此就注册用户而言，泄露的信息可能仅限于用户名和密码。

由于用户名和密码是以明文形式泄露的，因此 JarmoHyökyvaara 建议，如果有用户在其他信息系统或网络服务使用了相同用户名和密码，应该立即对这些密码进行修改。而一旦 Liiketoimintasuunnitelma 网站重新恢复上线，还应该立即对该网站的账户密码进行修改。

友情链接：https://www.hackeye.net/securityevent/13132.aspx

(二)泰国电信运营商 TrueMove H 数据泄露，4.6 万用户资料可在线公开访问

TrueMove H 是泰国三大电信运营商之一，也是泰国国内最大的 4G 移动网络运营商，并在去年宣布将通过与爱立信（Ericsson）合作推出泰国第一张 5G 网络。

英国科技新闻网站 The Register 在上周五（4 月 13 日）发表的报道中指出，TrueMove H 似乎成为了数据泄露事件的最新受害者。因亚马逊 AWS S3 存储桶配置错误，其 4.6 万用户的个人信息被公开暴露在互联网上，包括身份证扫描件。

根据 The Register 的说法，这个问题是由安全研究员 Niall Merrigan 发现的。他起初试图直接与 TrueMove H 进行联系，但该公司的工作人员并没有对此事表现出积极性。直到他向对方表示将公开这个问题时，对方才在本月 4 日向他进行了邮件回复并表示“正在处理”。

Merrigan 在上周四（4 月 14 日）上午 10:00 左右对 TrueMove H 的 S3 存储桶进行了再次检查，他发现配置错误问题以及这些文件仍然存在。大约在晚上 19:00 左右，TrueMove H 才对这些文件进行了限制访问处理。

Merrigan 告诉 The Register，TrueMove H 的 S3 存储桶共存储了超过 32GB 大小的数据，共有 4.6K 万个文件，主要是 JPG 和 PDF。从内容上来看，它们大多数都是身份证、护照以及驾驶执照的扫描件，而这些包含大量敏感信息的文件并没有得到任何安全保护。

在 TrueMove H 对这些文件进行了限制访问处理之后，Merrigan 在上周五发表了一篇用于分析该案例的博文。他解释说，类似 bucket stream 和 bucket-finder 这样的工具可被用来扫描在互联网上暴露的亚马逊 AWS S3 存储桶。

在这个案例中，Merrigan 使用了 bucket-finder，它可以帮助网络管理员查找出配置文件、源代码和其他可能存在的数据泄露问题。这个搜索器能够通过 AWS S3 API 获取前 1000 个文件，Merrigan 将这些文件加载到了一个小型 SQL 数据库中进行分析，他在其中便发现了 True Move H。

TrueMove H 在上周六（4 月 15 日）发表的一份澄清声明中称，这起数据泄露事件只会影响到其子公司 I True Mart。泄露用户数据的安全问题目前已经得到解决，该公司会继续与全球网络安全专家密切合作对事件进行彻底调查，并会通过采取法律行动来确保用户信息受到保护。

友情链接：https://www.hackeye.net/securityevent/13325.aspx

(三)英国数码商品购物网站数据库泄露，致军方警方政府购买记录曝光

根据英国科技新闻网站 The Register 的报道，英国热门数码商品在线购物网站 DronesForLess.co.uk 在无意间泄露了数千名警方、军方、政府以及个人消费者的购买记录以及个人信息。导致事件发生的根本原因来自于，该网站的交易数据库意外在线暴露并且没有得到加密保护。

根据 The Register 的说法，这一事件是由来自英国 Secret-bases 公司的技术顾问 Alan Turnbull 发现的，他将自己的发现作为独家消息告知给了 The Register 的记者 Gareth Corfield。

Alan 告诉记者，DronesForLess.co.uk 网站的运营商并没有对他们网络基础设施的关键部分进行妥善的保护，这使得该网站对于充满好奇心的人来说是“完全开放的”，仅使用谷歌语句搜索就能够很轻松地找到这些数据。

The Register 在得知这一消息后，对事件的真实性进行了确认。他们发现，约有 13,000 条日期显示为 2015 年 10 月至 2018 年 3 月 31 日期间的购买记录被存储在 DronesForLess.co.uk 的网站服务器上，而这些数据并没有进行加密处理甚至没有设置密码保护。

事件的严重性不言而喻，这种情况意味着任何人只要能够在网上找到这个网站服务器，就能够任意浏览上面的数据。

根据报道的描述，这些购买记录还包含了消费者的详细个人信息，如姓名、地址、电话号码、电子邮箱地址、IP 地址、用于访问该网站的设备信息、所购买商品的详情、发卡银行以及支付卡号码的后四位。

从购买记录来看，在这些消费者中不乏有来自警方、军方以及政府的工作人员，比如：

一名来自伦敦警察厅的在职警务人员购买了一架“大疆精灵 3”无人机，收货地址显示是位于伦敦的皇后大厦总部，购买人留下的电子邮件地址还包含了其所在部门的缩写；

一名英国陆军预备役少校为其部队总部订购了一架价值 1100 英镑的无人机；

英国国防部采购部门的一名工作人员购买了一架“大疆悟 Inspire 2”无人机，并配备有备用电池和意外损坏保险；

英国国家犯罪局的一名工作人员使用自己的工作邮箱（***@nca.x.gsi.gov.uk）购买了一台尼康 Coolpix 数码相机。

The Register 表示，这仅仅是购买记录中的很小一部分，其他消费者还包括：英国私有国防研究所 Qinetiq 的工作人员、英国国防科技实验室位于波斯陶山的雷达研发基地、英国陆军步兵试验和开发部队以及英国全国上下大大小小的警察局、地方议会、政府机构。当然，更多的还是一些私人订单。

值得注意的是，从警方、军方以及政府工作人员购买的商品类型来看，大多数是一些相机和其他光学装置以及无人机，目前尚不清楚这些商品是来自于个人购买还是官方购买。

The Register 已于上周二将这起数据泄露事件向 DronesForLess.co.uk 进行了通报，该网站并没有对此事做出任何解释，只是对所有泄露的数据进行了删除处理，目前这些数据已经无法在被公众访问。

友情链接：https://www.hackeye.net/securityevent/13269.aspx

(四)一位中年大妈的泄愤之路：凭 VPN 闯入美国航空公司网络系统

在上周四，一名 59 岁的美国妇女因侵入 PenAir（Peninsula Airlines）公司的票务和预订系统而被联邦法院判刑。PenAir 是美国的一家航空公司，成立于 1955 年，是阿拉斯加和美国东北部最大的支线航空公司之一。

根据法庭文件显示，被告名为 Suzette Kugler，曾是 PenAir 公司的一名雇员。她在 PenAir 公司工作了 29 年，直到 2017 年 2 月份，并且似乎是与前雇主不欢而散。

在工作期间，Kugler 管理着 PenAir 公司的 Sabre 数据库系统，而这个系统是该航空公司票务和预订服务的核心。

在 Kugler 离开 PenAir 公司的前一周，她利用拥有的系统权限创建了一个具有高级特权的虚假员工账户，用于控制对 Sabre 系统的访问。

在 2017 年 4 月 5 日，Kugler 利用这个账户登录了 PenAir 公司的 Sabre 系统，并对一名工作人员的账户进行了删除，以阻止其对系统的访问。

Kugler 在 2017 年 5 月 2 日再次登录了 Sabre 系统，不过这次她删除了八个 PenAir 机场站的相关信息，这使得机场站的工作人员无法完成与预订、出票、改签或登机服务。

经过 PenAir 工作人员一整夜的努力，所有的信息都重新被录入了 Sabre 系统，并没有给 PenAir 公司的乘客造成延误。

不过，Kugler 并没有就此结束她的罪行。她在第二天再次登录了 Sabre 系统，并删除了两张待处理的航班座位图，而这些座位图被用于告知 PenAir 工作人员乘客预定的座位。这意味着如果没有座位图，乘客将无法登上各自的航班。

幸运的是，被 Kugler 删除的座位图在航班起飞前三天是无法被乘客提前访问的。这为 PenAir 工作人员提供了一个重新创建座位图的机会，以避免了给乘客带来不必要的麻烦。

这一系列异常状况最终引起了 PenAir 公司注意，他们立即联系美国联邦调查局对此问题进行彻底调查。由 Kugler 创建的虚假员工账户在调查中被发现，最终她也被调查人员锁定。

调查人员对 Kugler 使用的两台笔记本电脑进行了分析，发现她仍保留了 PenAir 公司内部使用的 VPN 连接软件。该软件包含了一个名为“scvpn.log”的日志文件，对日志文件的进一步分析揭示了 Kugler 的所有不当行为。因为调查人员发现她在离职后仍在使用这款软件，而她使用软件的时间与相关事件发生的时间完全匹配。

Kugler 在今年 1 月份承认了自己的罪行，并于上周四得到了联邦法院的宣判。由于 Kuglar 此前并无任何犯罪记录，并且也没有给 PenAir 公司带来过大的经济损失，因此法官给予了她宽大处理。

Kugler 最终被判处 250 小时的社区服务和五年缓刑。另外，由于给 PenAir 公司造成了大约在在 5000 美元至 6500 美元之间成本损失，Kugler 还需要向 PenAir 支付 5616 美元的赔偿金，并在判决生效时一次性支付。

友情链接：https://www.hackeye.net/securityevent/13372.aspx

(五)离职员工窃取客户联系人名单，SunTrust 银行 150 万客户信息遭泄露

美国 SunTrust 银行在本周五证实 ,在一名离职员工偷窃了该公司的客户联系人名单之后，超过 150 万名客户的个人信息可能已经因此遭到泄露。

SunTrust 银行是美国金融服务控股公司 SunTrust Banks,Inc 旗下最大的子公司 ,主要提供储蓄、信托、信用、投资等服务业务。根据相关资料显示，截至到 2016 年 9 月，SunTrust 银行在美国东南部 11 个州和华盛顿特区设有 1400 家银行分行和 2160 台自动柜员机。

据《今日美国（USA TODAY）》报道，在本周五上午举行的公司业绩电话会议上，SunTrust 银行的首席执行官 William Rogers 称，这属于团伙作案，这名离职的前员工通过与第三方合作成功对公司的客户联系人名单进行了盗窃。名单包含的客户个人信息包括客户的姓名、地址、电话号码以及某些账户余额。

Rogers 强调，可能遭到泄露的信息仅限于此，并不包括诸如社会安全号码、帐号、PIN、用户 ID、密码或驾照信息这样的敏感客户个人信息。

“我们向可能受此影响的客户道歉，我们加强了对账户的监控并增加了其他安全措施。虽然我们尚未发现重大欺诈活动，但我们承诺，我们会为客户因欺诈而遭受的损失负责。”Rogers 在一份声明中表示。

Rogers 表示，SunTrust 银行正在积极配合第三方安全专家和执法部门进行事件调查。尽管调查工作仍在在进行中，但出于对客户负责，SunTrust 银行正在主动通知约 150 万名客户。

除了现有的 SunTrust 安全协议外，该公司还通过美国三大征信局之一的 Experian（益博睿）向每一名受影响的客户提供了额外的信用监控服务。

友情链接：https://www.hackeye.net/securityevent/13448.aspx

