迪普科技 2018 年 7 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.

版权所有 侵权必究 All rights reserved

目 录

一、 安全漏洞态势

2018 年 7 月份新增安全漏洞 1923 个。比上月增加了 1746 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 10 个，中危漏洞 320 个，低危漏洞 1593 个，同比 2017 年 7 月（漏洞总数 1063 个）增长 80.90%。表 1-1 为 2018 年 2 月-2018 年 7 月漏洞危险等级统计。

表 1-1 2018 年 2 月-2018 年 7 月漏洞危险等级统计

	二月	三月	四月	五月	六月	七月
高危	**367**	**144**	**436**	**48**	**58**	**10**
中危	**502**	**277**	**313**	**65**	**115**	**320**
低危	**112**	**52**	**56**	**5**	**4**	**1593**
总数	**981**	**473**	**805**	**118**	**177**	**1923**

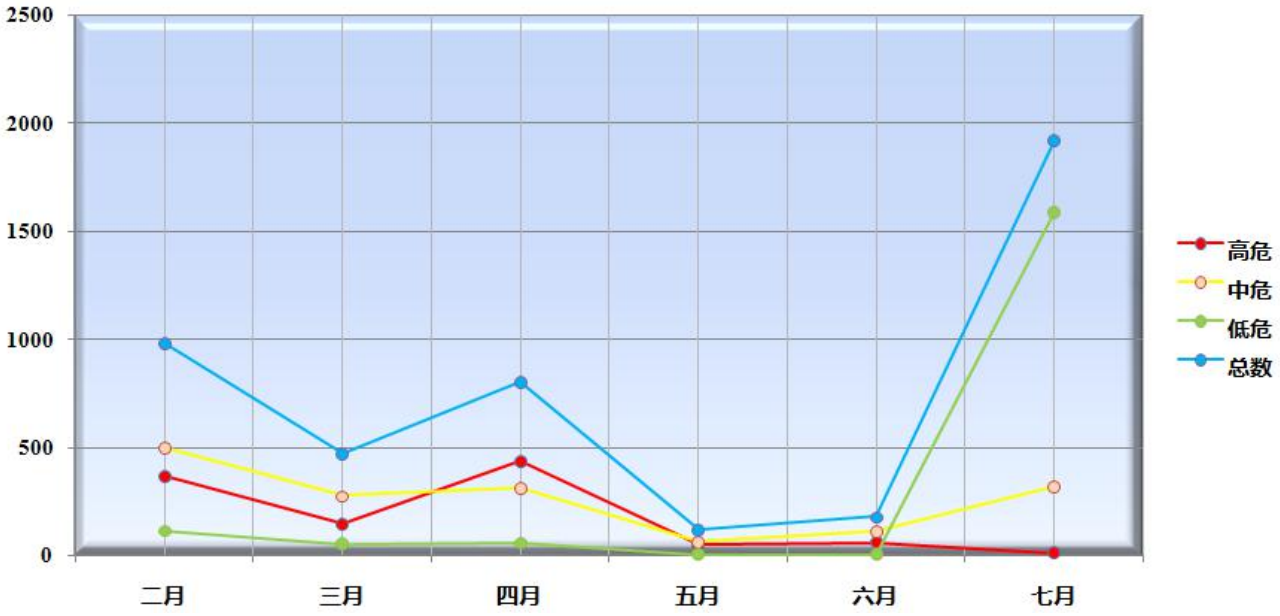

图 1-1 2018 年 2 月-2018 年 7 月漏洞新增数量趋势

二、 漏洞类型分布

2018 年 7 月份新增的漏洞类型分布如表 1-2 所示。其中数字错误，占 24.08%。值得关注的还有跨站脚本、信息泄露等常见漏洞类型。

表 1-2 2018 年 7 月漏洞类型分布

类型	数量	比例
未知	1109	57.67%
加密问题	8	0.42%
数字错误	463	24.08%
输入验证	8	0.42%
跨站脚本	116	6.03%
信息泄露	44	2.29%
权限许可和访问控制	32	1.66%
SQL 注入	29	1.51%
跨站请求伪造	28	1.46%
其他	63	3.28%
路径遍历	23	1.20%

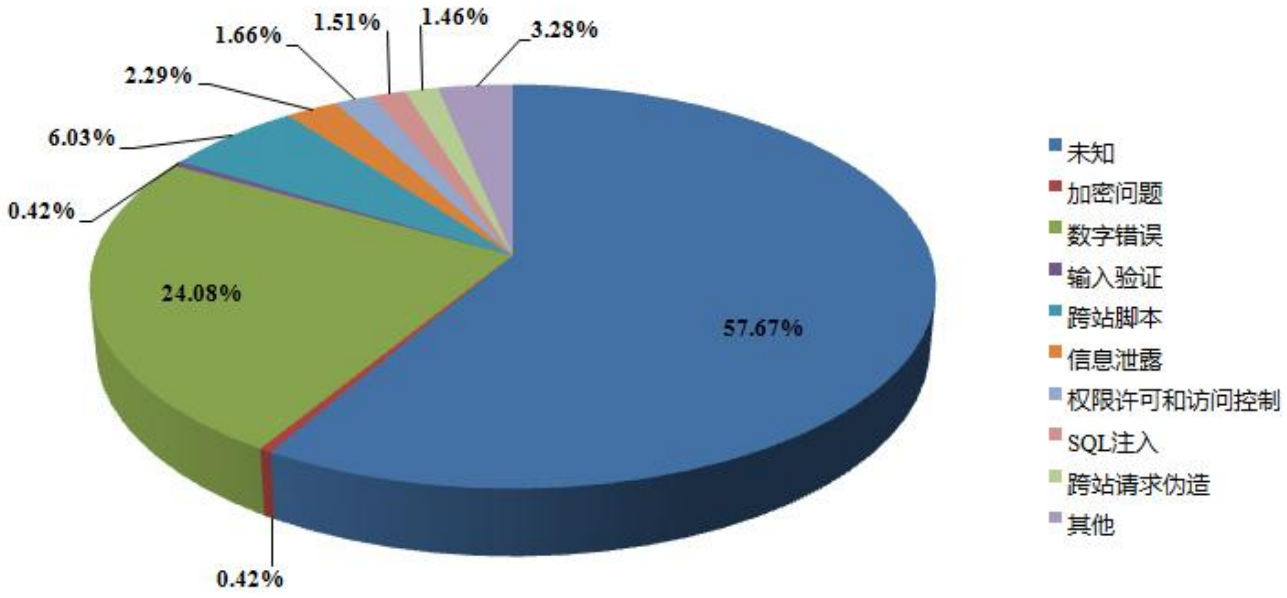

图 1-2 2018 年 7 月漏洞类型占比

三、 高危漏洞实例

(一) Weblogic 反序列化高危漏洞

CVE 编号：CVE-2018-2893

CNNVD 编号：CNNVD-201807-1276

发布时间：2018-07

危险等级：☆☆☆☆

漏洞类型：反序列化

受影响软件：

Weblogic 10.3.6.0

Weblogic 12.1.3.0

Weblogic 12.2.1.2

Weblogic 12.2.1.3

漏洞描述：Weblogic 是 Oracle 公司出品的一款应用服务器，通常也会被称为中间件，主要用于大型分布式 Web 应用的开发和部署，在国内外应用非常广泛。序列化是指将一个类对象存储成二进制文件的过程，反序列化是指将二进制文件还原成类对象的过程。

Oracle 官方 4 月的补丁（针对 CVE-2018-2628 的修复）存在黑名单限制不严格的问题，导致黑客可以利用 JDK 固有的一些特殊类进行反序列化漏洞绕过攻击，因此通过 4 月份补丁修复的 Weblogic 服务器依然存在风险，需及时加固。此次绕过攻击原理跟 CVE-2018-2628 类似，也是通过 T3 协议通信，利用 JRMP（Java Remote Method Protocol）方式传输恶意的序列化数据给受害服务器进行攻击。

攻击者可以利用该漏洞绕过限制进行反序列化攻击，危害系统安全。

修补建议：在不使用 T3 协议的情况下，直接禁用该协议。及时更新 JDK 和 JRE 软件版本，缓解反序列化系列漏洞的利用。关注 Oracle 官方补丁更新，获取链接：

http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html

(二) WebLogic 任意文件上传远程代码执行漏洞

CVE 编号：CVE-2018-2894

CNNVD 编号：CNNVD-201807-1277

发布时间：2018-07

危险等级：☆☆☆☆

漏洞类型：代码执行

受影响软件：

WebLogic 10.3.6.0

WebLogic 12.1.3.0

WebLogic 12.2.1.2

WebLogic 12.2.1.3

漏洞描述：Weblogic 是 Oracle 公司出品的一款应用服务器，通常也会被称为中间件，主要用于大型分布式 Web 应用的开发和部署，在国内外应用非常广泛。

ws_utc 为 WebLogic Web 服务测试客户端，在开发模式下，其配置页面存在未授权访问的问题，攻击者通过访问/ws_utc/config.do 配置页面， 用有效的 WebLogic Web 路径替换存储 JKS Keystores 的文件目录，再通过上传任意文件获取服务器权限。

攻击者可以利用该漏洞远程执行任意代码，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：

http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html

(三) Jenkins 任意文件读取漏洞

CVE 编号：CVE-2018-1999002

CNNVD 编号：CNNVD-201807-1740

发布时间：2018-07

危险等级：☆☆☆

漏洞类型：文件读取

受影响软件：

Jenkins <= 2.132

Jenkins <= 2.121.1

漏洞描述：Jenkins 是美国 CloudBees 公司基于 Java 开发的一种开源软件项目，主要用于执行工作的监控和持续的软件版本发布或者测试项目的监控。支持的版本控制工具包括 AccuRev、CVS、Subversion、Git、Mercurial、Perforce、Clearcase、RTC，也可以执行 Apache Ant、Apache Maven、sbt 项目、任意 shell 脚本和 Windows 批处理命令。

该漏洞与 org/kohsuke/stapler/Stapler.java 文件有关，在匿名用户拥有可读权限的时候，攻击者可以利用该漏洞在 HTTP 请求报文 Accept-Language 头部构造目录遍历的../恶意代码读取服务器上的敏感文件。

攻击者可以利用该漏洞读取服务器上的敏感文件，危害系统安全。

修补建议：升级到 Jenkins 2.121.2 最新版本，补丁获取链接：

https://jenkins.io/security/advisory/2018-07-18/#SECURITY-914

(四) WordPress 任意文件删除漏洞

CVE 编号：None

CNNVD 编号：None

发布时间：2018-07

危险等级：☆☆☆

漏洞类型：设计缺陷

受影响软件：

Wordpress <=4.9.6

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。

攻击者可以利用该漏洞删除包含数据库凭据的 wp-config.php 文件，使用其作为管理员帐户选择的凭据重新进入安装过程，最后导致攻击者可以在服务器上执行任意代码。

攻击者可以利用该漏洞删除服务器文件，甚至执行任意代码。

修补建议：目前厂商还没有提供补丁或者升级程序，厂商链接：

https://wordpress.org/

(五) Apache Tomcat 信息泄露漏洞

CVE 编号：CVE-2018-8037

CNNVD 编号：CNNVD-201807-1993

发布时间：2018-07

危险等级：☆☆

漏洞类型：信息泄露

受影响软件：

Apache Tomcat 9.0.0.M9 - 9.0.9

Apache Tomcat 8.5.5 - 8.5.31

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。

该漏洞是由于跟踪连接闭包的错误可能导致在新连接中重用用户会话，攻击者可以利用该漏洞获取一些敏感信息，导致信息泄露。

攻击者可以利用该漏洞获取敏感信息，危害系统安全。

修补建议：应用补丁或者升级程序，补丁获取链接：

http://mail-archives.us.apache.org/mod_mbox/www-announce/201807.mbox/%3C20180722090623.GA92700%40minotaur.apache.org%3E

四、 本月安全要闻

（一） 大量 Mega 帐户的登录信息遭泄露，并暴露了用户文件

据外媒 ZDNet 报道，Mega 这家于新西兰成立并提供在线云存储和文件托管服务的公司，目前被发现其平台中有成千上万的帐号凭证信息已在网上被公开发布。

被泄露的信息以文本文件形式提供，据了解这份文本文件包含超过 15,500 条用户名、密码和文件名的数据，这意味着这些帐号都曾出现异常登录的情况，并且帐号中的文件名也被爬取了。

这份文本文件最早由 Digita Security 公司的首席研究官和联合创始人 Patrick Wardle 于 6 月份在恶意软件分析网站 VirusTotal 上发现，而这份文件是在几个月前由一名据称在越南的用户上传的。

ZDNet 表示他们已验证这些帐号，确认这些数据来自 Mega，通过联系多位用户，还确定这些电子邮件、密码和一些文件都是在 Mega 上使用的。

据”Have I Been Pwned”网站的管理员 Troy Hunt 分析，这些数据并不是通过直接入侵 Mega 而获取的，而是被撞库了。他说文件中 98%的电子邮件地址已经存在于他的

数据库中（于先前的漏洞中收集）。ZDNet 也表示，在他们联系的人中，有五人说他们在不同的网站上使用过相同的密码。

目前还不知道是谁创建的这份列表，也不知道这些数据是如何被爬取到的。虽然 Mega 提供端到端加密，但登录时没有使用双因素身份认证方式，因此攻击者只需使用登录凭据便可登录每个帐户，并抓取帐号中文件的文件名。

Mega 董事长 Stephen Hall 表示，Mega 不能通过检查文件内容来充当审查员的角色，因为它在被上传到 Mega 之前已在用户的设备上被加密，除了在技术上不可行之外，Mega 和其他主要云存储提供商实际上也做不到，毕竟每秒上传 100 多个文件。

这不是 Mega 第一次遇到安全问题。2016 年，黑客声称通过利用其服务器中的安全漏洞获取了内部 Mega 文档。黑客还表示获取了与管理帐户关联的七个电子邮件地址。

Stephen Hal 表示当时没有任何用户数据遭到破坏。

友情链接：http://hackernews.cc/archives/23549

（二） 美国医疗保健公司 Blue Springs Family Care 近 4.5 万条记录遭泄露

Blue Springs Family Care 是一家位于美国密苏里州的医疗保健公司，成立于 1979 年，主要为杰克逊县的当地居民提供家庭医疗服务。最近的新闻报道显示，Blue Springs Family Care 遭遇了勒索软件攻击，而被落入攻击者手里的数据达到了近 4.5（44,979）万条。

该公司在一封公开信中指出，攻击者可能获得了各种患者记录信息，这至少包括：患者的全名、住址和出生日期、帐号、社会保险号、残疾等级、医疗诊断和驾驶执照/身份证号码。

公开信还指出，勒索软件攻击首次发现于 2018 年 5 月 12 日。负责对此次攻击进行调查的人员发现，该公司的计算机系统已被“未经授权的一方”攻击，并且各种恶意软件程序已上传至系统，而其中一个恶意软件程序就包含了恶意加密功能。

在发现异常之后，Blue Springs Family Care 立即聘请了一家取证信息技术公司。该公司对受感染的系统进行了隔离并安装了监控软件，以便他们能够查明是否有任何未经授权的实体获得了对受感染系统的访问权限。

Blue Springs Family Care 表示，他们已经与另一家电子健康记录提供商达成合作协议，而这个新的合作伙伴会对所有健康数据进行加密保护。

友情链接：https://www.hackeye.net/securityevent/15361.aspx

（三） 智利 1.4 万信用卡资料被黑客组织盗取

【环球网综合报道】据新加坡《联合早报》26 日报道，智利政府周三（25 日）晚透露，黑客盗取了智利约 1.4 万张信用卡的资料，并将这些资料公布在社交媒体上。

报道称，在这起案件中，黑客公布了信用卡卡号、有效期限及安全码，受攻击影响的银行包括桑坦德银行（Santander）、伊塔乌银行（Itau）、丰业银行（Scotiabank）和智利银行（Banco de Chile），这些银行已通知客户遭入侵一事。

报道称，智利政府并未透露此次信用卡资料被盗事件可能造成的损失。

智利政府的银行监管机构表示，这起袭击行动是黑客组织“影子经纪人”（Shadow Brokers）展开的，该组织因入侵美国国家安全局（NSA）而闻名。

今年 6 月，智利银行曾透露，黑客盗取了该银行 1000 万美元（约 1360 万新元）。智利银行当时说，黑客是从东欧或亚洲发动袭击，部分遭盗窃的款项最后被汇到香港。

友情链接：https://baijiahao.baidu.com/s?id=1607051481939062489&wfr=spider&for=pc

（四） 美国自动语音话务公司数以千计的选民信息遭曝光

据外媒 ZDNet 报道，一家位于弗吉尼亚州的主营政治竞选的自动语音话务公司 Robocent 的选民信息记录遭到外泄，约有 2600 条选民的个人信息遭到曝光，记录包含选民的姓名、住址和政治倾向以及音频通话记录。

Kromtech 信息安全公司的安全研究员 Bob Diachenko 率先在个人博客中披露了其数据遭到曝光，并向媒体分享了经过隐私处理的数据记录截图，除了上述信息还包括选民的性别、电话、年龄和出生年月，邮编，民族，语言和教育水平。经过“计算”的政治倾向，例如“弱支持民主党”“坚定支持共和党”或“摇摆”。尽管美国大部分州的选民注册信息属于公开记录，但这些数据严格限于特定的目的，有些州严格防止选民数据用于商业用途。Robocent 的联合创始人 Travis Trawick 确认公司的数据被安全保管，被曝光的数据记录来自于 2013-2016 年的公司统计，在过去两年中并未被使用。目前公司正在调查被公开数据，“所有曝光的数据都是公开访问信息，如果’法律需要’他会联系受影响的用户”。

友情链接：https://baijiahao.baidu.com/s?id=1606400981775228499&wfr=spider&for=pc

（五） Facebook 首次因数据泄密丑闻遭罚款：金额 66.4 万美元

新浪科技讯北京时间 7 月 11 日早间消息，Facebook 将因为剑桥分析（Cambridge Analytica）数据泄露事件而面临第一次处罚——来自英国的 66.4 万美元罚单。

英国信息委员会办公室（ICO）周二宣布对 Facebook 罚款，66.4 万美元是处罚金额上限。他们认为 Facebook 缺乏强有力的隐私保护措施，而且忽视了有望阻止剑桥分析操纵舆论的重要信号，其中也包括 2016 年英国脱欧公投。

在与 Facebook 进一步沟通之后，此项处罚可能会有所调整。ICO 通常不会披露初步结果，但他们表示，此次之所以这么做，主要是因为公众对此十分关注。该机构还承诺将在 10 月份更新内容。

Facebook 首席隐私官艾琳·伊根（Erin Egan）在周二的声明中承认，Facebook 本应采取更多措施调查跟剑桥分析有关的声明，并在 2015 年采取行动。

英国的处罚可能只是开始。欧洲其他地区和美国同样也在调查此事。例如，美国联邦贸易委员会也有可能对 Facebook 处以巨额罚款。美国联邦调查局和证券交易委员会也在调查 Facebook 与剑桥分析之间的联系。

伊根提到了很多与该公司有关的调查。“我们一直在与 ICO 就剑桥分析的调查展开密切合作，同时也在跟美国和其它国家的政府合作。”她说，“我们会评估这份报告，并尽快对 ICO 作出回应。”

英国的调查范围很广，不仅局限于 Facebook，还包括整个生态系统，涉及 172 家组织和 285 名个人，涵盖为政治目的而收集和销售网民数据的行为。英国信息专员伊利莎白·德纳姆（Elizabeth Denham）对科技公司、政党和其他在线收集敏感信息的各方“极度缺乏透明度”的行为表达了不安。

“ICO 调查得出一项重要结论是，Facebook 的透明度不足，难以让用户明白政党或竞选活动将通过何种方式、因为何种原因而瞄准他们。”德纳姆说，“虽然这些关于 Facebook 广告模式的担忧普遍存在于商业应用之中，但在用于政治竞选时显得格外突出。”

英国监管者在大约 40 页的报告中指责 Facebook 允许剑桥大学研究员亚历山大·科根（Aleksandr Kogan）开发了一款代表剑桥分析收集 Facebook 用户及其好友数据的应用。这家社交媒体巨头允许应用在 2015 年之前收集这些信息，但英国监管者周二表示，他们担心该网站的很多用户“可能并没有充分了解他们的数据被人以这种方式获取”。

英国调查人员还质疑 Facebook 可能没有提供充足的保护措施，确保其他第三方应用开发者不会滥用社交数据。该机构称，Facebook 在 2014 年错过了一次机会，未能阻止科根在该网站上的行为。

他们还表示，目前正在考虑对科根和剑桥分析公司前 CEO 亚历山大·尼克斯（Alexander Nix）进行处罚。

英国的主要担忧是 Facebook 的数据在多大程度上被用于操纵脱欧公投。英国政府周二还表示，他们将对剑桥分析母公司 SCL Elections 发起刑事诉讼。

英国监管者承诺对 Facebook 展开更严格的审查。剑桥分析曾经表示，在 2015 年收到 Facebook 的通知后，他们已经删除了相关数据。但英国监管者正在对此调查。他们发现，有证据显示，这些数据的副本被分享给其他机构，甚至分享到系统外部的机构，这也导致剑桥分析的陈述真实性存疑。

自从数据泄露丑闻遭到曝光后，Facebook 承诺对其平台上的所有第三方应用进行评估，同时采取新的透明度措施，包括针对其网站上的所有政治广告设立一个在线“储藏室”。

但这并非欧洲首次处罚 Facebook。欧盟反垄断监管者去年对 Facebook 罚款 1.22 亿美元。欧盟竞争专员认为，这家社交网络公司在 2014 年收购聊天应用 WhatsApp 时针对其隐私承诺提供误导性信息。Facebook 还因为没有遵守法国的数据保护规定而遭到过 16.4 万美元罚款。

友情链接：http://www.sohu.com/a/235632332_786964