全球数据安全观察

总第 126 期 2023 年第 7 期

(2023.02.20-2023.02.26)

大数据协同安全技术国家工程研究中心

NERCBDS
大数据协同安全技术
国家工程研究中心

目录

政策形势.....1
1、国家互联网信息办公室公布《个人信息出境标准合同办法》.....1
2、《关于加强境内企业境外发行证券和上市相关保密和档案管理工作的规定》公布.....1
3、北京市经济和信息化局 2023 年课题研究方向发布.....2
4、《深圳市数据产权登记管理暂行办法》（征求意见稿）意见公布.....2
5、《杭州市公共数据授权运营实施方案（试行）》（征求意见稿）发布.....2
6、河南省数据要素市场培育试点城市拟确定名单公示.....3
技术、产品与市场.....4
1、《企业跨境数据流动安全合规白皮书》发布.....4
2、联合国发布《隐私增强技术指南》.....4
3、2024 年中国数据库市场规模将达 461 亿元，本土厂商热度持续攀升.....5
4、同比增长 18%！2022 年我国大数据产业规模达 1.57 万亿元.....6
5、《2022 全球数据合规与隐私科技发展报告》发布.....6
业界观点.....9
1、专家解读丨《个人信息出境标准合同办法》出台 贡献数据跨境流动中国方案.....9
2、邬贺铨：可以尝试通过 IPV6 提升数据安全能力.....11
3、刘元春：数实融合要把握两个关键问题.....12
4、张蕴萍、翟妙如：重视数据要素价值释放中的反垄断治理问题.....14

5、银行业 APP 个人信息保护合规性研究与探索.....16
数据安全事件 18
1、印度火车票务平台遭遇大规模数据泄露，涉及超 3100 万人.....18
2、TELUS 调查被盗源代码、员工数据的泄露.....18
3、美国国防部服务器没密码，3TB 敏感数据泄露.....19
4、又曝出新冠疫情患者数据泄露，印度卫生部未予置评.19
5、游戏巨头动视暴雪疑似员工敏感信息及游戏数据泄露.20
6、苹果设备发现新漏洞，可以恶意访问用户数据.....21
7、澳大利亚零售商的客户数据因第三方供应商泄露而受损.....22
8、“黑客”恶作剧攻击连锁公司数据库，恶意删除数据 22
9、OyeTalk 会泄露用户的聊天记录已被安装超过 500 万次.....23
10、亚洲某两个数据中心被黑涉及苹果、微软和三星等公司.....23
11、勒索团伙 0mega 公开美国 Aviacode 超过 200 GB 的文件.....24

政策形势

1、国家互联网信息办公室公布《个人信息出境标准合同办法》

2 月 24 日，国家互联网信息办公室公布《个人信息出境标准合同办法》，自 2023 年 6 月 1 日起施行。国家互联网信息办公室有关负责人表示，出台《办法》旨在落实《个人信息保护法》的规定，保护个人信息权益，规范个人信息出境活动。

http://www.cac.gov.cn/2023-02/24/c_1678884830036813.htm

2、《关于加强境内企业境外发行证券和上市相关保密和档案管理工作的规定》公布

2 月 24 日，中国证券监督管理委员会、财政部、国家保密局、国家档案局公布了《关于加强境内企业境外发行证券和上市相关保密和档案管理工作的规定》，该文件是对《关于加强在境外发行证券与上市相关保密和档案管理工作的规定》的修订，包括加强对企业保密责任的强调等。

http://www.gov.cn/zhengce/zhengceku/2023-02/25/content_5743312.htm

3、北京市经济和信息化局 2023 年课题研究方向发布

2 月 20 日，北京市经济和信息化局发布了 2023 年将重点关注的 12 项课题研究方向，其中包括要推进数据要素市场化配置研究，基于对国内外数据要素市场化配置相关情况的梳理以及北京数据要素市场发展指标的分析，提出北京的发展路径和建议。

http://jxj.beijing.gov.cn/jxdt/gzdt/202302/t20230220_2920177.html

4、《深圳市数据产权登记管理暂行办法》（征求意见稿）意见公布

2 月 20 日，深圳市发展和改革委员会发布关于公开征求《深圳市数据产权登记管理暂行办法》（征求意见稿）意见的通告，以规范数据产权登记行为，保护数据要素市场参与主体的合法权益，促进数据作为生产要素开放流动和开发利用。

http://sf.sz.gov.cn/ztzl/gfxwj/gfxwjyjzj_171008/content/post_10436031.html

5、《杭州市公共数据授权运营实施方案（试行）》（征求意见稿）发布

2 月 17 日，杭州市数据资源管理局发布《杭州市公共数

据授权运营实施方案（试行）》（征求意见稿），以加快公共数据有序开发利用，培育数据要素市场。其中，针对数据安全方面，《方案》明确了“稳慎有序，安全可控”的基本原则，并提出了，鼓励通过数据管理能力成熟度（DCMM）和数据安全能力成熟度（DSMM）3 级以上认证。

http://minyi.zjzwfw.gov.cn/dczjnewls/dczj/idea/topic_6067.html

6、河南省数据要素市场培育试点城市拟确定名单公示

2 月 26 日，河南省工业和信息化厅大数据产业发展局拟确定郑州市、开封市、洛阳市、新乡市、许昌市等 5 地市为河南省数据要素市场培育试点城市。

https://gxt.henan.gov.cn/2023/02-26/2696279.html

技术、产品与市场

1、《企业跨境数据流动安全合规白皮书》发布

《企业跨境数据流动安全合规白皮书（2023）》由中移研究院主笔、中移国际与启明星辰共同编写，基于对全球跨境数据流动发展态势的研究，系统分析了企业跨境数据流动不同模式下所涉及到的典型场景，聚焦企业跨境数据流动面临的迫切问题，提出以“管理体系、技术体系与运营体系协同发展”为核心的企业跨境数据流动安全合规指导方案，并预测了企业跨境数据流动的发展方向。《白皮书》认为，未来五年，企业跨境数据流动将迎来监管规则的行业化特征日趋突显、相关技术日趋成熟并广泛应用、企业合规体系建设由“合规性驱动”转向“业务价值驱动”等趋势。

https://mp.weixin.qq.com/s/W1Q50af4kf-Lmepu7SyYsg

2、联合国发布《隐私增强技术指南》

2 月 13 日，联合国大数据和数据科学专家委员（UNCEBD）会发布《隐私增强技术指南》（The PET Guide）。指南重点关注隐私增强技术在官方统计数据中的应用，旨在帮助各国的国家统计局更好地理解和运用隐私增强技术处理敏感数据，提升数据的准确性和安全性，进而助力政府科

学合理决策。

隐私增强技术是用于安全处理和共享敏感数据的技术，旨在平衡隐私保护和数据可用性，可以分为输入端和输出端两大类。

https://www.wangan.com/p/11v72031d3847b1c

3、2024 年中国数据库市场规模将达 461 亿元，本土厂商热度持续攀升

中国数据库管理系统市场保持快速增长趋势，预计到 2024 年将达 461 亿元。从技术架构来看，集中式关系型数据库仍然为当前市场的主流，但云数据库及分布式数据库也成为众多厂商研发的重点以及用户部署的新方向。

在未来的数据库选型过程中，有 53.8%的调研对象对于数据库产品的安全可靠性要求依然很高，其中大多为金融机构和政府。结合访谈结果来看，相关单位认为随着行业的发展，数据库产品的安全可靠性逐渐得以保证，未来最需要考虑的因素应该是不同产品之间的兼容性以及业务系统和数据的平滑、无损迁移。

https://www.secrss.com/articles/52171

4、同比增长 18%！2022 年我国大数据产业规模达 1.57 万亿元

记者从日前举行的 2023 中国国际大数据产业博览会新闻发布会上获悉：2022 年我国大数据产业规模达 1.57 万亿元，同比增长 18%，成为推动数字经济发展的重要力量

数字基础设施实现跨越式发展。2022 年底，我国已建成全球最大的光纤网络，光纤总里程近 6000 万公里，数据中心总机架近 600 万标准机架，全国 5G 基站超过 230 万个，均位居世界前列。

数字产业创新发展加快提升。人工智能、物联网等领域的发明专利授权量居全球前列，数字经济核心产业规模加快增长，全国软件业务收入从 2012 年的 2.5 万亿元增长到 2022 年的 10.8 万亿元。

https://www.secrss.com/articles/52124

5、《2022 全球数据合规与隐私科技发展报告》发布

回顾近一年的发展，报告全面梳理了国内外数据安全与算法应用的合规体系，对隐私科技的概念、内涵和外延进行更新，基于整体性研究，提出五大主要发现：

（1）全球近 100 个国家和地区已制定数据保护相关法律，数据安全、算法应用有关立法进程加快,合规本地化的全球性趋势将进一步加强;

（2)全球数据合规领域执法力度加强,截至 11 月 30 日，**GDPR 执法总数 1216 起，罚款总额超 20 亿欧元**。企业面临合规人员招聘、安全产品及服务采购等合规成本与监管罚款等不合规支出的双重压力;

（3）企业更加重视数据合规与隐私保护，完善数据合规与隐私保护职能和管理体系，提升数据合规与隐私保护汇报层级，加大数据合规与隐私保护的人员和资金投入。22%的企业直接向高级管理层汇报工作，82%的企业认为在过去 12 个月的投入满足需求;

（4）更多企业发现隐私计算的价值并付诸实践，隐私计算在更多风险控制和数据流通等业务场景中发挥着重要作用，并在元宇宙、工业互联网与区块链等新兴科技中崭露头角。在未来十二个月，更多企业选择保持对隐私科技的投入水平，力图稳中求进;

（5）从隐私科技产业发展来看，**数据分类分级、数据流通监控、数据风险与隐私影响评估、数据与隐私综合治理**是当前的热门细分赛道。后续围绕提高数据的匿名化程度，增

强算法可解释性，加强落实伦理先行原则，将进一步赋能隐私科技的合规能力。

https://mp.weixin.qq.com/s?__biz=Mzk0MjMzNzMxMw==&mid=2247512270&idx=2&sn=ba1d1104dea3af0d85ed5d56800cc89c&scene=21#wechat_redirect

业界观点

1、专家解读丨《个人信息出境标准合同办法》出台 贡献数据跨境流动中国方案

我国的个人信息出境标准合同在形式上参考了国际上较常见的标准合同条款模板，同时充分考虑了中国法律的本土化表达，并在以下方面充分展现了中国方案的优越性:

第一，注重制度匹配。《办法》在清晰界定自身适用范围的同时，也实现了与其他数据出境安全管理制度的有效衔接。比如,《数据出境安全评估办法》要求数据处理者与境外接收方拟订合同等具有法律效力的文件,《办法》提出的标准合同内容与上述法律文件内容要求衔接适用。因此，仅涉及个人信息出境的数据处理者申报数据出境安全评估时，相关法律文件可参照《办法》附件拟订。

第二，细化风险管理。《办法》在《个人信息保护法》第五十五条提出个人信息保护影响评估(以下简称“影响评估”)后进一步针对出境场景细化了影响评估的评估项，比如境外接收方承诺履行的个人信息保护义务、措施和能力；个人信息出境后遭到篡改、破坏、泄露、丢失、非法利用等的风险。个人信息处理者在选定标准合同作为个人信息跨境传输合规路径的情况下，需要在向境外提供个人信息前进行影响评

估，此为对《个人信息保护法》的落实。

第三，平衡商业自由和监管需要。我国对标准合同采用“自主缔约与备案管理相结合”的原则。一方面，标准合同无需事先审批即可生效；另一方面，个人信息处理者的备案行为为网信部门持续监督提供了管理抓手。《办法》第六条规定，标准合同应当严格按照本办法附件订立，生效后个人信息处理者方可开展个人信息出境活动；第七条规定，个人信息处理者应当在标准合同生效之日起 10 个工作日内向所在地省级网信部门备案。从文义上理解，《办法》明确了标准合同应该严格按照《办法》附件订立，省级网信部门备案不会对合同生效产生影响。

第四，场景覆盖全面。根据标准合同范本第一条第（二）项，“境外接收方”是指在中华人民共和国境外自个人信息处理者处接收个人信息的组织、个人。这里的境外接收方既包括可以自主决定处理目的、处理方式的组织、个人，也包括受个人信息处理者委托处理个人信息的受托人。因此，订立标准合同的双方可能有“处理者—受托人”和“处理者—处理者”两种情形，也就是说，境内处理个人信息的受托人，不能作为标准合同的相对方，再次转委托境外主体处理个人信息。

第五，注重国际衔接。我国标准合同的主要内容，如个人信息再提供、处理安全、自动化决策处理等方面借鉴了有

关国家、地区的有益做法，为数据跨境流动制度的国际合作奠定了基础，争取与更多的国家地区建立稳定可行的数据流通双多边机制。

http://www.cac.gov.cn/2023-02/24/c_1678882701238102.htm

2、邬贺铨：可以尝试通过 IPV6 提升数据安全能力

近日，中国工程院院士邬贺铨在 2023 新经济智库大会上，围绕“数实融合——网络技术创新的新赛道”作了主题演讲。

在谈到产业数据化与数据安全时，邬贺铨提出，现阶段垂直行业和基础设施的发展对数据安全压力越来越大，可以尝试通过 IPV6 提升数据安全能力。

IPV6 技术下的扩展地址字段可以来定义 IP 包的业务属性，比如用户的 ID、APP 的 ID、服务质量等级、承载的业务、对信道带宽资源抖动及丢包率的要求。网络可以从这个 IP 包地址字段，直观地了解 IP 流业务对网络信道的要求，可以有针对性地提供信道和 QS 服务，进一步在地址字段里定义数据属性，确定什么数据更加敏感，让网络区别这个数据，提供分流敏感数据的服务。

另外，基于 IPV6 的数据流检测，可以在传输中实时反映信道里所经历的时延、抖动和丢包率，并且更重要的是可

以实现路径溯源。传统的互联网只有源地址、目的、地址，中间互联网 IP 包即便是同一个业务，也可能走不同的路由，是逐个路由器来选择的，即路径不确定。现在，通过数据流检测，可以还原 IP 包走过的路径，可以支撑跨境数据流动管理。

http://www.cbdio.com/BigData/2023-02/24/content_6172043.htm

3、刘元春：数实融合要把握两个关键问题

上海财经大学校长，中国人民大学原副校长、中国宏观经济论坛（CMF）联合创始人刘元春提出要抓住的数实融合第三次浪潮中最关键问题，在于两个方面：第一个是内在利益协调机制的问题，第二个是以市场主导为动力的问题。

一、社会迎接新技术浪潮的过程中，必须形成激励相容的内在利益协调机制

数字经济一个很重要的本质是将数字这种要素凸显和独立化，使它在生产系统的边际作用全面得到提升，这就是最简单的数字经济理解。在生产体系、社会体系中间，劳动、资本、管理、组织以及数字这一系列要素之间的组合关系，会发生革命性变化。这个变化在技术层面表现为一些技术特性，比如 IT 技术、网络技术、智能技术的变化，使生产组合

关系、社会组合关系发生变化。

但是另外一个很重要的层面，不是技术关系，而是利益关系，在边际贡献最大的这种要素，它所获得的收益是最大的。而被替代的要素，其边际收益会急剧下降，甚至消失。在转型过程中间，要想能够促进技术进步，必须要创造能够协调新要素与传统要素所有者利益之间关系的体系，让创新者享受创新的红利，让利益受损者适当得到补偿，这是一种新的经济形态可持续发展的核心要点。

如何在各种新旧产业交替过程中间，要素所有者、产业形态，工人他们之间的利益协调。在未来数实融合过程中，不是数字经济与实体经济的融合这样简单地来思考，更为重要的是要在要素替代、产业转化、组织变革中间的利益协调，要形成新的协调机制和制度创新。

二、数实融合的另一个关键问题是动力问题，让市场成为主导

在思考下一步发展时，会看到组织创新是一个关键。关键就在于我们企业主体、社会主体、政府主体，在智能转换过程中要有可持续性的利益绑定。从经济的角度来看，不同产业、不同规模的企业都要各自构建出新的利润形成体系，这是最关键的。目前很多头部企业在数实融合推进中间取得了很好的成就，能够克服在要素替代、组织替代中的各种成

本，但是中小企业作为经济中最为核心、最为活跃的细胞，在转型中间还面临着大量的数字鸿沟和大量的成本阻碍。国家的产业政策、技术创新政策，对于少数头部企业的扶持是可获取、可持续的。但是如果想向下层进行全面的深入，就面临一个最根本的问题，数字经济与实体经济的融合。

因此，下一步很重要的一个战略，就是要在目前国家全面产业布局，在新基建，在核心技术，在产业扶持所推进的政策中间，能够转换成一种市场可持续的利润创造。

http://www.cbdio.com/BigData/2023-02/23/content_6172033.htm

4、张蕴萍、翟妙如：重视数据要素价值释放中的反垄断治理问题

虽然数据具有非竞争性，但在价值释放过程中，高质量数据作为稀缺资源必然引发竞争。在数据的收集、转化或流通等不同环节，竞争壁垒都可能出现，干扰数据市场秩序，进而造成数据垄断，限制数据要素价值的实现，包括马太效应加深数据鸿沟、锁定效应与网络效应强化用户黏性、机会成本过高抑制数据开放。

推动经济社会高质量发展必须重视数据要素的价值释放，打破制约数据流通的藩篱，其中一项重要任务就是逐步

完善数据要素反垄断治理体系。

第一，明确数据市场竞争规则，细化垄断行为约束条款。落实数据治理规范建设，健全个人利益与公共利益的诉讼制度，加强企业自证要求，解决诉讼举证难的问题，针对数据市场上的垄断行为，采用分类列举的方式作出具体规定，建立案例参考制度，实现垄断行为的有效界定与追责。

第二，明确数据权利归属，建立动态产权体系。完善数据产权分割的法律规范，明确数据权责划分，提升大数据思维与应用能力，利用区块链等技术建立产权登记备案体系，探索构建分级分类的数据治理模式，创新数据产权保护路径，加强政策引导，统筹规制市场各主体行为，协调解决各方利益诉求。

第三，加强数据安全监管体系建设，完善数据反垄断治理机制。探索形成安全高效的数据流通模式，着力支持数据安全技术攻关，提升数据管理能力，积极推进数据风险防护系统布局。建立数据交易信用制度，严厉打击不正当竞争行为，加强行业自律。健全数据金融与财政制度，规范数据服务与流通秩序，引入数字化监管模式，发挥政府、社会与市场的协同联动作用，营造良性数据竞争环境，推动数字经济发展行稳致远。

http://www.china.com.cn/opinion2020/2023-

02/24/content_85126037.shtml

5、银行业 APP 个人信息保护合规性研究与探索

移动互联网发展下，APP 成为人们经济生活重要部分，对于服务民生、促进社会经济发展具有重要作用。银行业在 APP 个人信息保护中面临以下困境：信息收集与保护冲突、信息处理与保护矛盾、信息处理与保护矛盾。

对此给出银行业 APP 个人信息保护实践建议：

（1）信息收集实施区别监管

银行业机构必须根据《个人金融信息保护技术规范》（简称《技术规范》）与《信息安全技术个人信息安全规范》（简称《安全规范》）规定，制定信息披露条款、信息收集授权书等文件，以明示、公开方式获得用户书面同意，对照标准规定，执行分级分类。间接收集信息，银行机构承担查询、保证“来源正当”责任，确保信息提供方授权和信息相匹配，不能以书面合同方式，推卸审查信息义务，确保银行业机构能够做好采集、使用个人信息第一站工作。

（2）信息处理审查信息委托方

1）遵循“收集目的”要求。金融市场由于不断扩展，用户信息量巨大，范围较为广泛，深度挖掘信息能够可形成个人数据画像，便于银行业机构实施精准营销，提高用户黏性，

却也增加了用户泄露信息风险，必须对集团内部共享信息收集目的加以限制，维护用户隐私。

2）第三方机构遵守标准。科技不断发展下，银行开发APP不可避免会和科技公司合作，即便自身科技水平满足开发APP需求，却也会将业务外包，减少经营成本。所以，在APP个人信息保护中，银行和第三方机构必须遵守相应标准。银行机构选择服务前，应调查第三方能力、信用，确保金融信息安全下，和第三方签订保密协议，或是服务协议约定保密条款，设置信息共享“隔离带”。关注第三方及业界动态，了解评估其服务与产品后引入，避免外包人员与银行用户信息直接接触，保证信息安全性。

3）防控信息泄露风险。银行机构需加强个人信息风险管理，日常活动与流程中采取多样化方式进行风险控制。具体包括身份认证和访问控制、个人信息内部管理、日志记录和审计。

https://www.secrss.com/articles/52103

数据安全事件

1、印度火车票务平台遭遇大规模数据泄露，涉及超 3100 万人

2 月 21 日报道，印度流行的火车票预订平台 RailYatri 遭遇大规模数据泄露，暴露了超过 3100 万 (31,062,673) 名用户/旅客的个人信息。据信，该漏洞发生在 2022 年 12 月下旬，敏感信息数据库现已在线泄露。

泄露的数据包括电子邮件地址、全名、性别、电话号码和位置，这可能使数百万用户面临身份盗用、网络钓鱼攻击和其他网络犯罪的风险。

https://mp.weixin.qq.com/s/bv-8wkbYWhVQyttz337_aQ

2、TELUS 调查被盗源代码、员工数据的泄露

2 月 23 日，据外媒报道，加拿大第二大电信公司 TELUS 正在调查一起潜在的数据泄露事件，此前一名威胁行为者在网上分享了疑似员工数据单（包括姓名和电子邮件地址）的样本。威胁行为者随后发布了屏幕截图，显然显示了公司持有的私人源代码存储库和工资单记录。

https://www.bleepingcomputer.com/news/security/telus-investigating-leak-of-stolen-source-code-employee-data/

3、美国国防部服务器没密码，3TB 敏感数据泄露

2 月 26 日消息，上周末，安全研究人员 Anurag Sen 发现美国国防部一台存储了 3TB 内部军事电子邮件的服务器在线暴露长达两周，该服务器托管在微软的 Azure 政府云上，供美国国防部客户使用，与其他商业客户物理隔离，可用于共享敏感的政府数据。其中许多数据与美国特种作战司令部（USSOCOM）有关，USSOCOM 是美国负责执行特殊军事行动的军事单位。

令人惊讶的是，暴露的服务器由于配置错误没有密码，任何人都可通过互联网访问。据 Anurag Sen 透露，暴露数据包含过去几年的大量内部军事电子邮件，其中一些包含敏感的人员信息。

https://mp.weixin.qq.com/s/Wt23_rOiJhrBhJnHXLFAjQ

4、又曝出新冠疫情患者数据泄露，印度卫生部未予置评

2 月 21 日消息，印度再次曝光一起 COVID-19 患者数据泄露事件，由印度卡纳塔克邦维护的 arogya.karnataka.gov.in 数据库已被泄露。兜售的黑客声称，该数据库内包含个人 ID、姓名、地址、电话号码、电子邮箱及密码等信息。

从帖子中列出的数据样本来看，泄露的数据包含来自班

加罗尔（印度第三大城市）等地区的信息。据称这些数据的源头是由卡纳塔克邦政府维护的数据库，由当地私营实验室负责收集 COVID-19 相关信息。迄今为止，卡纳塔克邦登记的 COVID-19 病例总数超过 400 万。

外媒 Cyber Express 已经就此事向印度卫生部及该邦卫生署发出置评请求，但目前尚未收到回复。

https://www.wangan.com/p/11v727c60cd2ed3b

5、游戏巨头动视暴雪疑似员工敏感信息及游戏数据泄露

2 月 2 日，据外媒报道，黑客通过网络钓鱼动视暴雪员工，成功访问了该公司的内部系统，并泄露了部分员工敏感个人信息和游戏数据。

推特账号@vxunderground 分享的截图显示，去年 12 月 4 日，黑客通过网络钓鱼的方式骗取了动视员工的验证码，获得了其 Slack 帐户的访问权限，并窃取了动视暴雪的部分内部文件。受害员工来自人力资源部门，这代表着黑客能够访问大量敏感的员工详细信息。黑客还继续试图诱骗其他员工点击恶意链接，所幸未再有人上当受骗。

根据曝光的资料，涉密文件除员工姓名、电子邮件、电话号码、工资、工作地点等敏感的员工个人信息外，还涉及《使命召唤 19》这款游戏的赛季更新计划，另外还有关于《现

代战争 2》即将推出的 DLC、《使命召唤 2023》和《使命召唤 2024》的相关计划也遭到泄露。

https://www.secrss.com/articles/52153

6、苹果设备发现新漏洞，可以恶意访问用户数据

苹果公司修订了它上个月发布的安全公告，更新了影响 iOS、iPadOS 和 macOS 的三个新漏洞。

第一个漏洞是 Crash Reporter 组件中的一个竞赛条件（CVE-2023-23520），可使恶意攻击者以 root 身份读取任意文件。iPhone 制造商表示，它通过额外的验证来解决这个问题。

另外两个漏洞，归功于 Trellix 研究员 Austin Emmitt，位于 Foundation 框架中（CVE-2023-23530 和 CVE-2023-23531），可以武器化来实现代码执行。攻击者可以利用这些漏洞冲出沙盒，以更高的权限执行恶意代码，可能会允许访问日历、地址簿、信息、位置数据、通话记录、摄像头、麦克风和照片。

苹果公司表示:“应用程序可能能够在其沙箱之外执行任意代码或具有某些提升的权限”，并补充说道已经通过“改进的内存处理”修补了这些问题。

https://www.freebuf.com/news/358452.html

7、澳大利亚零售商的客户数据因第三方供应商泄露而受损

2 月 23 日，据外媒报道，属于澳大利亚零售商 The Good Guys 的客户数据在涉及第三方供应商 My Rewards 的安全漏洞中受到损害。

My Rewards 也证实了这一违规行为，初步调查表明，2021 年 8 月其系统遭受了“未经授权的访问”，这导致了数据泄露。该公司表示，这意味着包括姓名、电子邮件地址和电话号码在内的个人身份信息可能已经公开，并指出其所有数据都存储在澳大利亚。

https://www.zdnet.com/article/australia-retailers-customer-data-compromised-in-third-party-breach/?web_view=true

8、“黑客”恶作剧攻击连锁公司数据库，恶意删除数据

2 月 25 日，据重庆之声报道：2023 年 2 月的一个上午，某连锁品牌公司的收银系统和会员系统出现无法登录，无法正常运营的情况。在检查后发现收银系统所在的服务器内的数据被人故意删除。

重庆市公安局江北区分局提醒如何避免防范黑客攻击：一是及时更新服务器系统安全漏洞补丁;二是要加强服务器安全防护能力;三是制定有效的风险预警机制，重要数据一定要备份;四是发现被“黑客”入侵时，要立即断网，保存好现

场的犯罪证据，并马上报警处理。

https://mp.weixin.qq.com/s/dux_bKqV25WVJpRAOkOMHw

9、OyeTalk 会泄露用户的聊天记录已被安装超过 500 万次

据媒体 2 月 22 日报道，Android 语音聊天应用泄露了用户的聊天记录。该应用在 Google Play 上的下载量超过 500 万次，其 Firebase 实例泄露了超过 500MB 的数据，包括未加密的用户聊天记录、用户名和手机国际移动设备识别码(IMEI)号码等。研究人员表示，如果没有对泄露的数据进行备份，攻击者可能会删除数据库导致用户的个人信息永久丢失。应用的开发人员在获悉数据泄露后仍未能限制数据库的访问，谷歌不得不介入设法保护该数据库。

https://www.hackread.com/android-voice-chat-app-data-leak/

10、亚洲某两个数据中心被黑涉及苹果、微软和三星等公司

据媒体 2 月 21 日报道，黑客入侵了位于亚洲的两个数据中心，窃取了苹果、优步、微软、三星、阿里巴巴等科技公司的登录凭证，并远程访问了这些组织的监控摄像头。安全公司 Resecurity 最初在 2021 年 9 月确定了数据泄露事件，但是直到 2023 年 2 月 20 日，黑客 Minimalman 才在黑客论坛 Breachforums 上公开了这些数据。据悉，这两个数据中心

都在 2023 年 1 月强制所有客户更改密码。
https://www.hackread.com/data-centers-hack-data-leak/

11、勒索团伙 0mega 公开美国 Aviacode 超过 200 GB 的文件

媒体 2 月 20 日称，0mega 公开了 Aviacode 超过 200 GB 的文件。Aviacode 主要提供医疗编码服务、医疗编码审计、编码拒绝管理、临床文档改进以及账单和索赔的收入周期管理。2 月 11 日，0mega 发布了被盗数据，其中包括有关员工和承包商的信息。0mega 发言人称，他们早在 2023 年 1 月 1 日就加密了 Aviacode，但该公司从未回应过他们。截至目前，Aviacode 及其母公司 GeBBS 均未回应研究人员关于此事件的询问。
https://www.databreaches.net/aviacode-remains-silent-after-0mega-dumps-200-gb-of-their-files/

《全球数据安全观察》周报

政策形势： 政策法规/地方动态/标准动态

技术、产品与市场： 技术研究/行业洞察/市场趋势

业界观点： 大咖观点/业界报告

数据安全事件： 合规事件/数据泄露/数据勒索

编委会： 钟力、唐会芳、王雨薇、陈璐

如有反馈 邮件请至 nelab@360.cn

http://www.nelab-bdst.org.cn/