国盟信息安全通报

2021 年 04 月 25 日第 238 期

全国售后服务中心

国盟信息安全通报

（第 238 期）

国际信息安全学习联盟

2021 年 4 月 25 日

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 569 个，其中高危漏洞 147 个、中危漏洞 352 个、低危漏洞 70 个。漏洞平均分值为 5.66。本周收录的漏洞中，涉及 0day 漏洞 208 个（占 37%），其中互联网上出现“Remote Clinic 跨站脚本漏洞、WCMS 目录遍历漏洞（CNVD-2021-28257）”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 3828 个，与上周（3147 个）环比增加 22%。

主要内容

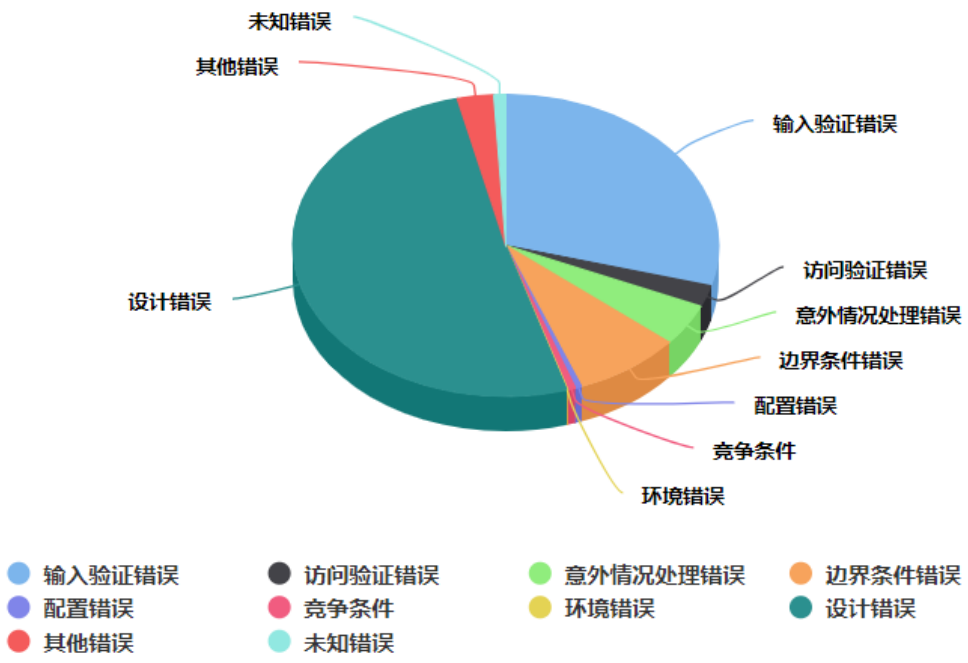
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

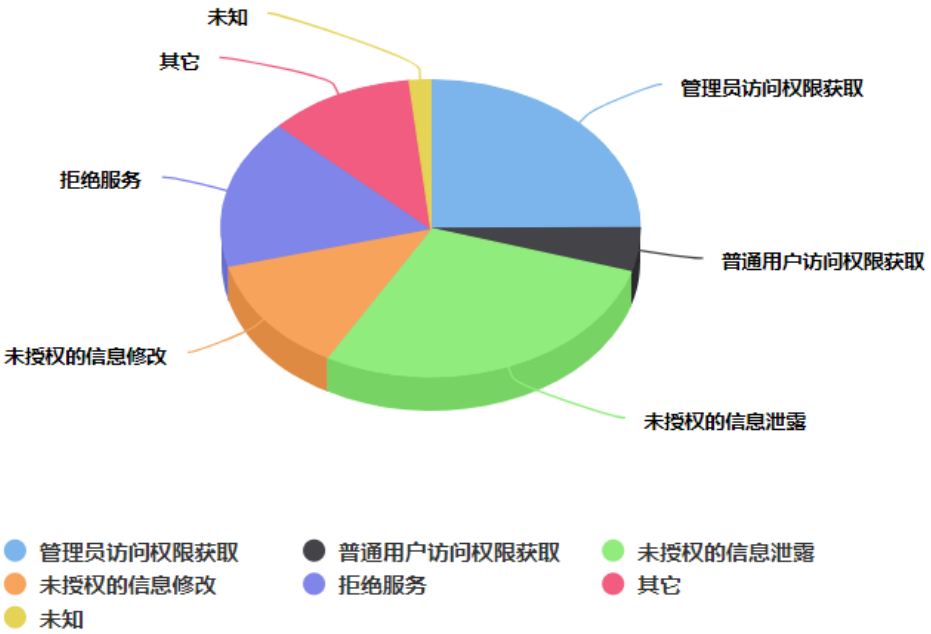
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 569 个，其中高危漏洞 147 个、中危漏洞 352 个、低危漏洞 70 个。漏洞平均分值为 5.66。本周收录的漏洞中，涉及 0day 漏洞 208 个（占 37%），其中互联网上出现“Remote Clinic 跨站脚本漏洞、WCMS 目录遍历漏洞（CNVD-2021-28257）”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 3828 个，与上周（3147 个）环比增加 22%。

二、安全漏洞增长数量及种类分布情况

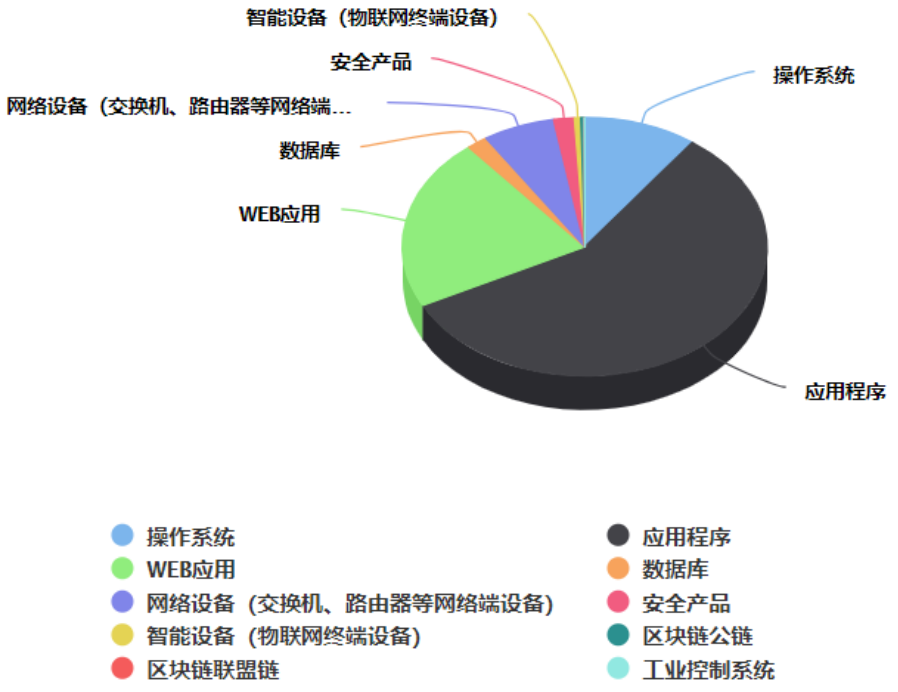
➢ **漏洞产生原因（2021 年 4 月 11 日—2021 年 4 月 25）**



➢ 漏洞引发的威胁（2021 年 4 月 11 日—2021 年 4 月 25）



➢ 漏洞影响对象类型（2021 年 4 月 11 日—2021 年 4 月 25）



三、安全产业动态

➢ 推进网络强国建设的强大思想武器和科学行动指南

伟大实践产生伟大思想，伟大思想引领伟大实践。党的十八大以来，习近平总书记高度重视网络安全和信息化工作，提出一系列新思想新观点新论断，形成了内涵丰富、科学系统的习近平总书记关于网络强国的重要思想。我们要把学习宣传贯彻习近平总书记关于网络强国的重要思想摆在更加突出重要的位置，进一步凝聚起推动网络强国建设的强大精神力量。

深入学习宣传贯彻习近平总书记关于网络强国的重要思想，就要坚持以党的创新理论武装头脑、指导实践、推动工作，不断把握和拓展中国特色治网之道。习近平总书记坚持马克思主义立场观点方法，系统回答了为什么要建设网络强国、怎样建设网络强国的一系列重大理论和实践问题，为推进网络强国建设指明了前进方向、提供了根本遵循。我们要夯实理论之基，坚持用党的创新理论武装头脑、指导实践、推动工作，深刻领会其中的理论逻辑、历史逻辑、实践逻辑，深刻把握其中的基本立场、基本观点、基本方法，深刻汲取其中的真理力量、实践力量、人格力量；要探索治网之道，把握网信工作规律，形成更加成熟、更加完备、更加定型的中国特色治网模式；要回答时代之问，以我们正在做的事情为中心，推动网络强国建设实现新突破、创造新业绩、开创新局面。

深入学习宣传贯彻习近平总书记关于网络强国的重要思想，就要坚持不断提高“两个维

护”的能力和水平，确保党中央重大决策部署的贯彻落实。党的十八大以来，网信事业发展之迅速、变化之巨大、成绩之显著，归根结底在于以习近平同志为核心的党中央坚强领导，在于习近平总书记关于网络强国的重要思想的科学指引。我们要始终把讲政治作为第一位的要求，增强“四个意识”、坚定“四个自信”、做到“两个维护”，不断提高政治判断力、政治领悟力、政治执行力，始终在思想上政治上行动上同以习近平同志为核心的党中央保持高度一致，确保党中央关于网信工作的各项决策部署不折不扣落到实处。

深入学习宣传贯彻习近平总书记关于网络强国的重要思想，就要坚持以人民为中心的发展思想，让互联网发展成果更好造福人民。网信工作与近 10 亿网民直接相连，与 14 亿人民群众的获得感、幸福感、安全感息息相关。我们要始终把人民对美好生活的向往作为网信工作的奋斗目标，开展好党史学习教育“我为群众办实事”实践活动，实现党性与人民性的高度统一、对党负责与对人民负责的高度统一、尊重网信发展规律与尊重人民历史主体地位的高度统一，不断以网信事业的新进展新成效服务人民、造福人民。

深入学习宣传贯彻习近平总书记关于网络强国的重要思想，就要坚持立足新发展阶段、贯彻新发展理念、构建新发展格局，不断推动网信事业高质量发展。习近平总书记深刻阐述了网络强国建设与全面建设社会主义现代化国家、实现中华民族伟大复兴的内在关系。我们要科学谋划“十四五”网信事业发展新蓝图，着眼构建网上网下“同心圆”，加强网络内容建设管理；着眼加快科技自立自强，大力推进信息领域关键核心技术突破；着眼发挥驱动引领作用，加快推动数字产业化、产业数字化；着眼防范化解风险，全面加强网络安全保障体系和能力建设；着眼构建网络空间命运共同体，加强网信国际交流合作，为实施“十四五”规划、全面建设社会主义现代化国家开好局起好步提供强大网上舆论支持、可靠网络安全保障、有力信息化支撑。

深入学习宣传贯彻习近平总书记关于网络强国的重要思想，就要坚持加强党对网信工作的集中统一领导，不断提高信息化条件下党的执政能力和领导水平。要把提高信息化条件下党的领导水平和执政能力作为重大时代课题，毫不动摇地坚持党管互联网，加强党对网信工作的集中统一领导，加强网信系统党的建设和干部队伍建设，充分运用信息化的理念、思路、方法、手段推进党的建设新的伟大工程、推进国家治理体系和治理能力现代化，不断增强党的创造力、凝聚力、战斗力，使风华正茂的百年大党始终勇立时代潮头，使生机勃勃的中国特色社会主义事业不断开创发展新局。（作者：中央宣传部副部长，中央网信办主任、国家网信办主任 庄荣文）

➢ 牢固树立正确的网络安全观

“要树立正确的网络安全观，加快构建关键信息基础设施安全保障体系，全天候全方位感知网络安全态势，增强网络安全防御能力和威慑能力。”2016 年 4 月 19 日，习近平总书记在网络安全和信息化工作座谈会上发表重要讲话，为我国网络安全和信息化事业发展指明了前进方向，为我们提升维护网络安全能力、推动网络社会治理创新提供了根本遵循。

党的十八大以来，习近平总书记以宏阔视野和战略思维，就如何认识、运用、发展、管理互联网等提出了一系列战略性、前瞻性、创造性观点，深刻回答了事关网信事业发展的一系列重大理论和实践问题。习近平总书记关于网络安全和信息化工作的重要论述，是习近平新时代中国特色社会主义思想的重要组成部分，是推动新时代网络安全和信息化发展的行动指南。

新思想引领新时代，新理念指导新实践。党的十八大以来，在习近平总书记关于网络强国的重要思想引领下，我国网络安全工作取得历史性成就，网络安全防线进一步筑牢，人民群众在网络空间的获得感、幸福感、安全感显著提升。在以习近平同志为核心的党中央坚强领导下，公安部部署全国公安机关深入贯彻党中央决策部署，牢固树立网络安全观，依法严厉打击涉网违法犯罪，积极构建国家网络安全综合防控体系，提升网络安全事件应急指挥和处置能力，切实加强网络空间治理，有力维护了网络空间安全。

没有网络安全就没有国家安全。互联网既是人们生活的新空间，也是国家和社会治理的新领域。截至 2020 年 12 月，我国网民规模已达 9.89 亿。信息革命时代潮流与中华民族伟大复兴历史进程发生了历史性交汇，互联网成为事业发展的最大增量，也是我们面临的最大变量。网络空间天朗气清、生态良好，符合人民利益；网络空间乌烟瘴气、生态恶化，侵害

人民利益。我们必须科学认识网络传播规律，提高用网治网水平，使互联网这个最大变量变成事业发展的最大增量，切实维护国家网络安全和人民群众切身利益。

“十四五”规划和 2035 年远景目标纲要强调加强网络安全保护，要求“提升安全防护和维护政治安全能力”。新的发展形势下，公安机关必须深入学习贯彻习近平总书记关于网络安全和信息化工作的一系列重要论述，牢固树立正确的网络安全观，坚持统筹发展和安全，坚持网络安全为人民、网络安全靠人民，不断提高对互联网规律的把握能力、对网络舆论的引导能力、对信息化发展的驾驭能力、对网络安全的保障能力，坚决维护网络意识形态安全，着力提升维护网络安全能力，切实承担起网络安全捍卫者、网络强国建设者的职责使命，为营造风清气正的网络空间、推进网络强国建设作出新的更大的贡献，以优异成绩庆祝建党 100 周年。（来源：中国公安网）

➢ 中国金融个人信息保护

2020 年 12 月 8 日，中国银行保险监督管理委员会（CBIRC）主席在新加坡金融科技节上发表演讲，表明中国政府将密切关注金融科技领域。金融科技日益兴起，特别是在国内移动支付领域中，两大巨头支付宝和微信支付大量应用电子支付的功能。然而，金融科技的发展会带来哪些个人信息保护方面的挑战？中国个人金融信息的监管现状如何？中国即将出台的《个人信息保护法（草案）》和《数据安全法（草案）》是否会对海外金融机构带来影响呢？中国的法律法规要求与欧盟《一般数据保护条例》（GDPR）之间存在哪些异同呢？对于中国和海外金融机构来说，要开展哪些合规工作以应对监管格局的转型呢？

金融科技：个人信息保护痛点

首要的挑战是大量的个人金融信息处理，可能会导致难以对这些信息实施全生命周期的治理和安全管控。由于许多科技公司利用市场优势，过度地收集、使用、甚至出售信息，这些活动可能没有获取客户的同意。因此，可能会侵犯企业的利益和消费者的个人隐私。

第二个挑战是很难识别所有涉及个人金融信息处理的第三方支付平台。由于大量的第三方支付平台在金融服务中扮演着重要角色，使金融机构更难全面准确的识别出第三方上涉及个人信息处理的支付服务。

第三个挑战是现存法律体系在个人信息保护层面的缺失。中国金融行业尚未出台个人金融信息保护的法律，更不用说新兴的金融科技领域。因此，监管要求的缺失给金融机构日常运营促进个人金融信息保护合规工作的开展带来了挑战。

尽管金融行业尤其是金融科技领域在个人信息保护方面面临上述三个挑战，但是违反法律法规要求不仅会给金融机构带来声誉损失，还会造成大笔经济上的罚款。2020 年 7 月 28 日，中国银保监会上海监管局对两家未能妥善保护消费者个人信息的中资银行分别处以 100 万元人民币的罚款。因此对于金融机构来说，保护客户个人金融信息的责任迫在眉睫。

中国法律法规、指南和标准

尽管我国尚未出台个人信息保护相关法律规定，但有两部法律草案正在审议中。同时，作为中国长期实践形成的民事法律规范《中华人民共和国民法典》，也于 2021 年 1 月 1 日正式生效，其中人格权编的第六章“隐私权和个人信息保护”规定了隐私和个人信息的定义、个人信息处理的原则和条件、自然人的权益以及个人信息处理者的职责。此外，相关部门陆续发布关于个人信息保护和移动应用程序（APPs）的指南，以及一系列金融行业标准和指导方针，推动金融机构开展个人金融信息保护的合规工作。

法律草案：个人信息保护法和数据安全法

•《个人信息保护法（草案）》：2020 年 10 月 21 日，中国发布了备受期待的《中华人民共和国个人信息保护法（草案）》（以下简称“PIPL”），并提交十三届全国人大常委会第一次审议。该草案共八章七十个条款，旨在保护个人信息权益，规范个人信息处理活动，保障个人信息依法有序自由流动，促进个人信息合理利用。与 2016 年颁布的《网络安全法》相比：（1）扩大了域外法律效力，适用于中国境外的数据处理者；（2）明确了敏感个人信息的处理规则，要求在处理此类信息时，个人信息处理者应当取得个人的单独同意；（3）提供了多项个人信息处理的法律基础，包括履行合同、法定义务和公共利益等，取代了《网络安全法》仅基于同意的法律基础；（4）增加了对采用自动化决策手段的要求，以保证决策的透明度和

处理结果的公平合理，充分保护个人信息主体的权利。

•**《数据安全法（草案）》** ：2020 年 7 月 2 日，《数据安全法（草案）》提交全国人大常委会审议。该草案同样具有域外效力，聚焦重要数据的保护。草案要求按照数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄漏或者非法获取、非法利用，对国家安全利益造成的危害程度，对数据开展分级分类保护管理。各地区、各部门需确定重要数据保护目录，重要数据的处理者应对其数据活动定期开展风险评估，并设立数据安全负责人和管理机构。同时规定，执法机构以维护国家安全和调查案件目的收集数据，需经过严格的批准手续依法进行；对于境外执法机构调取境内数据，组织和个人需向主管机关报告并获得批准。

指南：个人信息保护和移动应用程序（APP）：尽管上述两部法律草案仍在审议中，但国家相关部门出台了一系列个人信息保护和 APP 相关的指南。 个人信息保护—国家市场监管管理总局和国家标准化管理委员会于 2020 年发布一系列指导方针《信息安全技术个人信息安全规范（修订版）》（GB/T 35273-2020）于 2020 年 10 月 1 日起实施，提供加强个人信息保护的具体要求；《个人信息安全影响评估指南》（GB/T 39335-2020）于 2021 年 6 月 1 日生效，为个人信息保护法草案中的第 54 条提供了支持。

移动应用程序（APP）—国家信息安全标准化技术委员会（TC260）和中国网络空间管理局（CAC）发布了一系列移动应用运营商相关数据处理活动规定的正式或非正式的指南和标准，包括自我评估、软件开发包的使用，以及移动应用程序功能所需的个人信息的最小范围等。

金融行业标准

在金融行业，中国人民银行（PBOC）发布一系列金融行业标准，包括：

•《个人金融信息保护技术规范》（JR/T 0171-2020）- 于 2020 年 2 月 13 日颁布，规定个人金融信息分为三级和七类。 按敏感程度分为三类 - C3 类别信息（用户识别信息）、C2 类别信息（可识别特定个人金融信息主体身份与金融状况的个人金融信息，以及用于金融产品与服务的关键信息）、C1 类别信息（机构内部的信息资产）； 按内容分为七类 – 个人金融信息分为账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息和其他反映特定个人金融信息主体某些情况的信息。

•《金融数据安全 数据安全分级指南》（JR/T 0197-2020）–于 2020 年 9 月 23 日颁布，根据对国家安全、公众权益、个人隐私、企业合法权益等对象的影响程度，从高到低划分为严重损害、一般损害、轻微损害和无损害等四个等级。

• 《中国人民银行金融消费者权益保护实施办法》（人行[2020]5 号）(以下简称“新办

法”)－于 2020 年 9 月 1 日颁布，并于 2020 年 11 月 1 日生效。与 2017 年发布的实施办法相比，有五项重大变化：

1.法律效力增强 - 从原办法的规范文件升级为部门章程，违反新规定可能会移送司法机关依法追究刑事责任(新办法第 64 条)；

2.扩大适用范围到普惠金融 - 适用对象从银行和支付机构扩大到商业银行理财子公司、金融资产管理公司、信托公司、汽车金融公司、消费金融公司以及征信机构、个人本外币兑换特许业务经营机构；适用业务方面，扩大到利率管理、人民币管理、外汇管理、黄金市场管理、国库管理、支付清算管理、反洗钱管理、征信管理相关的业务、与上述业务相关的金融营销宣传和消费者金融信息保护以及其他人民银行职责范围内的金融消费者权益保护(新办法第 52 条)；

3.关注金融消费者的八大权利 – 延续原办法八大权利，包括金融消费者的财产安全权、知情权、自主选择权、公平交易权、依法求偿权、受教育权、受尊重权和信息安全权。新办法强化了受尊重权，着重对自主选择权和公平交易权提出具体要求，削弱了个人信息控制权如查询、删除、修改的权利 (新办法第 14 条-第 21 条)；

4.以知情权为重点的市场营销规范化 - 机构应当以适当方式供金融消费者自主选择是否同意银行、支付机构将其金融信息用于营销、用户体验改进或者市场调查的目的 (新办法第 30 条)；

5.加大违法处罚力度 - 侵害消费者金融信息依法得到保护的权利的机构，按照《消费者权益保护法》第五十六条最高可处五十万元人民币（约 7.4 万美元）(新办法第 60 条和《中国消费者权益保护法》第 56 条)。

对海外金融机构的全球影响

监管机构除了会对损害中国公民的权利或国家安全和公共利益的金融机构处以经济罚款外，中国网络空间管理局（CAC）还会将其列入黑名单中。适用于海外金融机构收集中国个人金融信息的场景，包括： •组织、个人在中华人民共和国境内处理自然人个人信息的活动，适用个人信息保护法； •在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，有下列情形之一的，也适用个人信息保护法：以向境内自然人提供产品或者服务为目的；为分析、评估境内自然人的行为； 法律、行政法规规定的其他情形。

中国 PIPL vs GDPR

中国的《个人信息保护法（草案）》同其他十一个国家的隐私法类似，都与 GDPR 存在一定的相似程度。这十一个国家包括：巴西的《一般数据保护法（LGPD）》，澳大利亚的隐私

法案（Privacy Act），美国《加利福尼亚消费者隐私权法案（CCPA）》，日本的《个人信息保护法案》、韩国的《个人信息保护法案（PIPA）》、泰国的《个人数据保护法案（PDPA）》、智利的《数据隐私法》、新西兰的《隐私法案（2020 版）》、印度的《个人数据保护法案（PDPB）》、南非的《个人信息保护法（POPIA）》以及加拿大的《个人信息保护与电子资料法案（PIPEDA）》。图 1 是中国个人信息保护法草案与欧盟一般数据保护条例之间的相似点和不同点。

相似点	不同点
•域外适用法律；（PIPL 第三条） **•违规行为可能会被处以巨额罚款-违反 PIPL 罚款高达五千万元人民币（约 744 万美元），或上一年营业额的 5%；（PIPL 第六十二条）** **•个人在开展个人数据处理活动中的各项权利，包括知情权、决定权、查阅和复制权、更改和补充权、删除权，解释个人信息处理规则的权利以及个人行使权利申请的机制。（PIPL 第四十四条-四十九条）**	•与 GDPR 不同，不区分数据控制者和数据处理者；（PIPL 第九条） •关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。确需向境外提供的，应当通过国家网信部门组织的安全评估；法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定；（PIPL 第四十条） •基于个人同意处理敏感个人信息（包括金融账户信息）的，个人信息处理者应当取得个人的单独同意。包括金融账户信息在内的敏感信息在中国需要单独的同意；（PIPL 第三十条） •个人信息处理者知道或者应当知道其处理的个人信息为不满十四周岁未成年人个人信息的，应当取得其监护人的同意，而 GDPR 规定为 16 岁；（PIPL 第十五条） •PIPL 处理的合法性基础不包括合法性利益。（PIPL 第十三条）

图 1—中国 PIPL 与欧盟 GDPR 的相似点和不同点

海外金融机构合规工作

由于两部法律草案目前仍在审查中，中国尚未出台针对数据安全和隐私相关的国家层面的法律，但是，这并不意味着金融机构尚不需要采取任何措施，因为一旦违反相关监管要求，可能会给机构带来高额的罚款。此外，由于金融科技的迅猛发展，中国即将出台的法律法规可能会阻碍海外金融机构在中国开展金融科技业务。下面是海外金融机构需主动满足监管合规要求的合规事项参考：在中国设立专门的部门或指定人员监督信息处理过程；发布中国机构客户和员工的隐私声明；管理中国公民的个人金融信息；建立并维护个人金融信息处理活动记录；标记数据字典，绘制个人数据地图和数据流转图；更新跨境数据传输合同、标准合同条款。

中国金融机构的下一步行动

个人金融信息保护的挑战之一是数据治理。金融机构应平衡数据共享和数据保护之间的关系。例如，澄清在什么情况下消费者的大数据可以被用于商业目的，确定数据保留期限以及数据共享的程度。下面提供了可能会对个人金融信息保护有价值的分步骤指导方针：

1.个人金融信息分类分级管理：制定一套完整的个人金融信息分类分级管理制度；明确

个人金融信息全生命周期的技术安全防护要求；更新完善数据地图和数据字典，通过识别个人信息传输场景，重点识别个人金融信息转移或交换过程中的相关第三方，并提出具体技术性要求。

2. 开展行政性保护工作：更新隐私声明/隐私政策：更新官网、手机银行 APP 同客户和员工签署的内部隐私声明、以及协议/合同； 完善数据泄漏事件流程和制度，以及数据主体权利响应制度，包括补充删除用户个人信息及注销用户账户的流程，以及开展个人信息影响评估的流程；建立个人信息保护定期审计流程，对个人信息保护的政策、相关流程和安全措施的有效性进行评估。

3.指派专人监督个人信息保护并制定沟通机制：明确职责分工，比如建立个人信息保护组织架构，并明确相关部门职责分工； 建立并完善内部和外部的沟通机制；开展隐私保护意识培训。

4.个人信息保护相关 IT 系统改造：对相关系统和移动金融客户端 APP 开展 IT 系统改造工作：包括个人信息收集明示同意、定义特殊种类（或敏感）个人数据、制定数据保留期限、提供消费者拒绝营销的选项等。对相关 IT 系统分类。对于本地维护系统，开展 IT 系统改造工作；对于与第三方对接的系统，更新同第三方的服务水平协议和工作说明书。

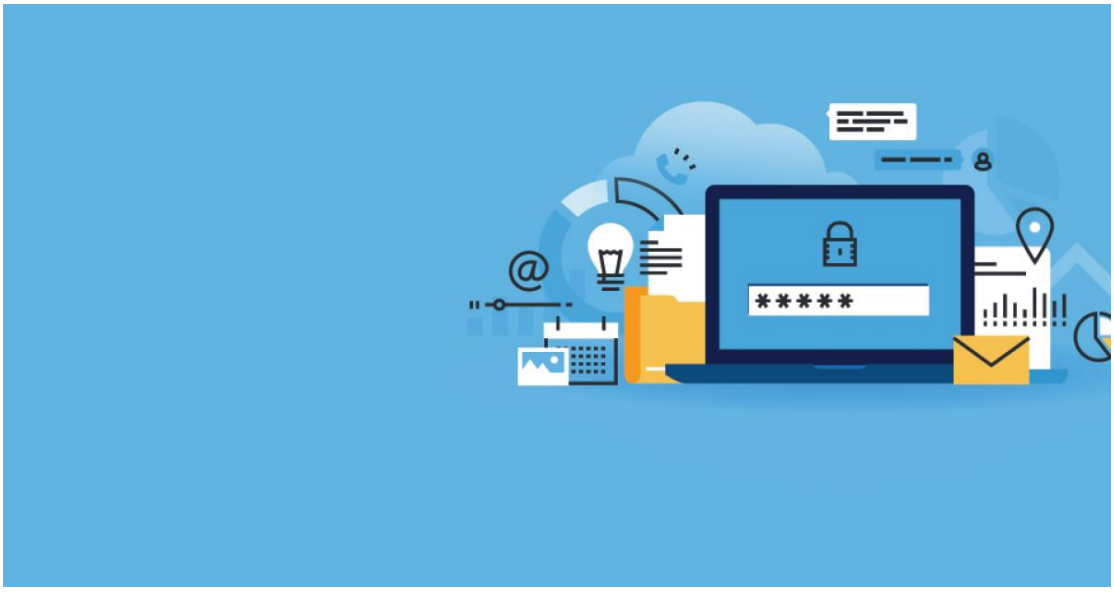
结论

在数字化转型时代，越来越多的金融机构为了向客户提供更好的服务，大范围采用自动化决策和人工智能等新技术，使得大量的个人信息特别是敏感信息被处理。由于个人金融信息具有社会、经济和治理价值，因此如何平衡消费者权利和金融服务的关系，对金融机构来说是至关重要的。尽管中国的《个人信息保护法（草案）》和《数据安全法（草案）》仍未形成终稿，但是中国监管机构正在密切关注金融行业的个人信息保护，特别对于具有强监管且高风险特性的金融科技行业。因此，对于向中国市场提供金融服务的全球金融机构，应积极采取适当的管理性和技术性保护措施，以应对中国个人金融信息保护监管格局的转型。（来源：ISACA News and Trends/Industry News）

➢ 新规对个人信息保护的特别界定及意义

手机等智能移动终端预置、下载安装的应用软件以及基于软件开放平台开发的、用户无需安装即可使用的小程序，为人们的衣食住行乃至工作、生活和学习、娱乐过程中提供了便

利的解决手段，发挥着越来越多的作用。与此同时，一些移动应用程序运营商存在在用户不知情的情况下，对普通用户的个人数据超范围采集，过度商业开发甚至用于谋求不正当利益的情况。实践中大量商业机构、刑事犯罪分子利用窃取的个人数据实施刑事犯罪活动，严重侵犯用户个人权益。如果长期无法有效遏止，势必危害互联网产业的健康发展，损害广大网民的合法权益。



四部委近日发布的《常见类型移动应用程序必要个人信息范围规定》（以下简称《规定》），明确了 39 类常见的移动互联网应用程序提供服务过程中收集个人信息的范围，为移动互联网应用程序运营商收集个人信息划定清楚的界限，将互联网应用程序收集个人信息的行为规范在合理、合法的范围内，对整个产业发挥指引作用。《规定》的实施，促进移动互联网应用程序的运营商理性而有节制地收集个人信息，有利于保护更多公民的个人信息相关权益免受侵害。

现实生活中在移动应用程序开发者、运营商与用户三者之间存在严重的不平衡关系，用户处于信息极易被过度收集和非法使用的情况下，《规定》的出台将移动应用程序收集个人信息的范围限定在“必要”范围内，并且要求移动应用程序开发者和运营商不得因为用户不同意提供非必要个人信息而拒绝提供服务，帮助移动应用程序开发者和运营商与用户之间建立更加合理、平衡的权利义务关系，增强用户个人信息保护能力，降低用户个人信息被用于非法活动的风险。

一、如何理解“必要个人信息”

《规定》第三条定义必要个人信息是指保障移动应用程序基本功能服务正常运行所必需的个人信息，缺少该信息移动应用程序无法完成基本功能、无法提供正常服务。换言之，用

户必须提供某些信息才可以享有移动应用程序提供的服务，所以运营商和开发者有权要求用户提供信息，这是使用移动应用程序的前提条件之一。

准确理解必要个人信息，还可以比对一下《规定》的具体条文。《规定》针对 39 种实践中常见的移动应用程序提供的基本服务内在需求，分别划定了服务提供者、运营者所能够收集信息的范围。不同类型的移动应用程序对服务提供者、运营者要求用户提供的信息范围、信息类型并不相同。判断是否是超范围采集信息，需要依据移动应用服务的类型，来确定服务提供者、服务运营者能够收集的用户信息范围。

因为这些信息是开启和提供移动应用程序时要求用户必须提供的基本信息，否则无法正常提供服务。我们将用户提供这类基本信息的行为，视作与移动应用程序运营商之间建立法律关系的前提条件，双方因此形成服务与被服务关系，由此产生民事法律关系或其他方面的关系。

因为这是必要个人信息，用户提供这类信息因此具有明显的义务性。用户必须根据法律要求，如法律要求实名制的要求。用户还应当承担因提供的信息存在瑕疵而导致移动应用程序无法或无法正确提供服务的法律后果。

举例来讲，几乎所有的移动互联网应用程序都要求用户在开启或使用服务时向运营方提供其电话号码。用户有义务提供真实、合法、有效并且处于自己实际控制状态的电话号码，并通过与运营商服务绑定的移动终端使用相关的服务。否则移动应用程序服务提供者或运营商不承担相应的法律责任。同时，一旦用户通过自己提供的必要个人信息与服务提供者建立关联性，用户还有义务确保自己提供的这些基本信息处于稳定状态。如果因为用户个人的原因而影响这些基本的信息，比如因为用户泄露服务提供者给用户提供的确认码，或因为保管不善导致移动设备被他人非法利用，则用户应当承担服务提供者无法正常提供服务的法律责任和后果。如果致使用户合法权益受到损害，除非用户能够证明服务提供者的过错，否则用户自己承担相应的法律责任和后果。

二、如何理解“不得拒绝条款”

不得拒绝条款，是《规定》第四条内容。该条款至少包括以下几个方面的内容：

首先，这是监管机构对运营商和用户之间权利义务关系的一次再平衡。这种平衡增加了用户的选择权，同时对运营商的权利进行了适当的限制。众所周知，在《规定》出台之前，移动应用程序运营商和用户之间的权利、义务关系并不平衡，一些运营商借助强大的商业能力、专业的操作团队和数据应用能力，形成并不断扩大对用户的控制力，并以此迫使用户违背意愿让渡个人信息。

《规定》的不得拒绝条款，将使用户具有更完备的个人信息保护权利。一方面用户可以通过让渡个人信息来获得更加周到而全面的服务，另一方面，如果用户认为没有必要拿出更多个人信息换取更多服务，就有权以有限范围的个人信息获得基础服务。运营商不得通过打包提供服务的方式，或者利用其与用户不平等的地位关系，向用户强行出让不需要的服务，以换取用户更多的个人信息。

其次，不得拒绝条款带有明显的预防性质，立法本意是限制运营商滥用其支配地位，但该条款并没有将运营商和用户之间就个人信息的收集或提供范围予以强行限定。运营商可以用更优质或类型更多的服务，换取用户提供更多的个人信息。对此，用户具有主动选择权。

第三，不得拒绝条款的立足点，是希望通过监管力量的介入，通过权利、关系再平衡的方式，改变既往运营商和用户之间不平等或用户对运营者随意收集个人信息的作法无法予以有效抵制的现状。

鉴于个人信息蕴含巨大的商业价值，可能诱发运营商过度收集信息，不得拒绝条款就成为对抗、制约这种收集冲动的外部力量，并有助避免因过度收集数据导致其他再生性恶果，有利于更有效保护用户的信息权益、隐私权益。

三、落实过程中需要解决的问题

《规定》生效前，过度收集、滥用用户个人信息是一个存在了很长时间的问题。《规定》将收集信息的范围非常有限而明确地限定，对处于优势地位的运营商来讲，无疑是一次权限再调整。《规定》的实施，需要运营商，不管过去长时间运营的，还是新上线或将来上线运营的运营商，都需要设计新的个人信息收集处理规则，都需要通过加大人力和技术投入，更好地处理用户个人信息收集。

运营商需要切实落实好《规定》要求，否则会减弱运营商的运营能力和为用户提供更好使用体验、更充分分享数字红利的能力。如果这些能力弱化，移动应用程序及其所链接的整个社会的生活、分配、消费等各个环节的能力，服务社会各方面的能力，都可能减弱。同时，以各类移动应用程序为平台而生产、处理和使用数据的能力，也有可能受到实质性影响。（作者：王四新 中国传媒大学人类命运共同体研究院副院长）

四、政府之声

➢ 国家医保局印发《关于加强网络安全和数据保护工作的指导意见》

2021 年 4 月 9 日，国家医保局发出《关于印发加强网络安全和数据保护工作指导意见的通知》（以下简称《通知》），要求到 2022 年，基本建成基础强、技术优、制度全、责任明、管理严的医疗保障网络安全和数据安全保护工作体制机制。到“十四五”期末，医疗保障系统网络安全和数据安全保护制度体系更加健全，智慧医保和安全医保建设达到新水平。

《通知》提出，要全面推进网络安全水平提升。主体责任明晰，监督管理机制完善，基础设施完备，网络安全技术能力、态势感知、预警能力、突发网络安全事件应急响应能力显著提升，网络安全有效保障。切实落实关键信息基础设施重点保护要求，加强关键信息基础设施网络安全监测预警体系建设，提升关键信息基础设施应急响应和恢复能力。进一步完善网络结构安全、本体安全和基础设施安全，逐步推广安全免疫。加强内外网安全隔离，严禁医保专网接入互联网。

同时，依法依规对数据的产生、传输、存储、使用、共享、销毁等实行全生命周期安全管理，提高数据安全防护能力和个人隐私保护力度。强化个人隐私保护，采用适当的安全控制措施，确保数据的产生、采集和汇集过程合规、安全。个人信息的采集，坚持法定授权原则，法定授权外个人信息采集事项须先获得自然人或者其监护人同意。处理个人信息应当遵循合法、正当、必要原则，不得过度使用。（来源：国家医疗保障局）

- **国家医疗保障局关于印发加强网络安全和数据保护工作指导意见的通知**
- **全文：**http://www.nhsa.gov.cn/art/2021/4/9/art_37_4834.html

➢ 交通运输部关于印发《交通运输政务数据共享管理办法》的通知

2021 年 4 月 6 日，交通运输部关于印发《交通运输政务数据共享管理办法》的通知。通知明确要求政务数据共享应遵循以下原则：

（一）以共享为原则，不共享为例外。政务数据原则上均应共享，国家相关法律法规或政策制度明确不得共享的除外。（二）需求导向，无偿使用。使用部门提出明确的共享需求和政务数据使用用途，提供部门应及时响应并无偿提供共享服务。（三）统一标准，平台交换。按照国家及行业相关标准规范进行政务数据的编目、采集、存储、交换和共享工作。政务部门应基于部、省两级共享平台开展政务数据共享。（四）建立机制，保障安全。建立健全政务数据共享管理机制。加强对政务数据共享全过程的身份鉴别、授权管理和安全保障，确保政务数据安全。（来源：交通运输部）

- **《交通运输政务数据共享管理办法》**
- **全文：**https://xxgk.mot.gov.cn/2020/jigou/kjs/202104/t20210416_3569651.html

➢ 国家七部门联合发布《网络直播营销管理办法（试行）》

2021 年 4 月 23 日，国家互联网信息办公室、公安部、商务部、文化和旅游部、国家税务总局、国家市场监督管理总局、国家广播电视总局等七部门联合发布《网络直播营销管理办法（试行）》（以下简称《办法》）。国家互联网信息办公室有关负责人就《办法》相关问题答记者问。

一、问：请介绍《办法》制定出台的背景？

答：网络直播营销，也就是通常所说的直播带货，作为一种新兴商业模式和互联网业态，近年来发展势头迅猛，在促进就业、扩大内需、提振经济、脱贫攻坚等方面发挥了积极作用，但同时出现了直播营销人员言行失范、利用未成年人直播牟利、平台主体责任履行不到位、虚假宣传和数据造假、假冒伪劣商品频现、消费者维权取证困难等问题，人民群众对此反映强烈，有必要及时出台相应的制度规范。《办法》作为贯彻落实《网络安全法》《电子商务法》《广告法》《反不正当竞争法》《网络信息内容生态治理规定》等的重要行政规范性文件，对规范网络市场秩序，维护人民群众合法权益，促进新业态健康有序发展，营造清朗网络空间具有重要现实意义。

二、问：《办法》的制定思路是什么？

答：《办法》坚持立足当前与着眼长远相结合，坚持促进发展与规范管理相结合，坚持继承性与创新性相结合，充分考虑网络直播营销发展趋势、行业实际、各类参与主体特点，按照全面覆盖、分类监管的思路，一方面针对网络直播营销中的“人、货、场”，将“台前幕后”各类主体、“线上线下”各项要素纳入监管范围，另一方面明确细化直播营销平台、直播间运营者、直播营销人员、直播营销人员服务机构等参与主体各自的权责边界，进一步压实各方主体责任。

三、问：《办法》对直播营销平台提出哪些明确要求？

答：《办法》明确直播营销平台应当建立健全账号及直播营销功能注册注销、信息安全管理、营销行为规范、未成年人保护、消费者权益保护、个人信息保护、网络和数据安全管理等机制、措施。《办法》强调平台应当依法依规开展安全评估、履行备案手续、取得相关行政许可，具备维护直播内容安全的技术能力、制定平台规则公约的管理能力，要求平台制

定直播营销商品和服务负面目录，认证并核验直播间运营者和直播营销人员的真实身份信息，加强网络直播营销信息内容管理、审核和实时巡查，对涉嫌违法违规的高风险营销行为采取管理措施，提供付费导流等服务需承担相应平台责任，建立健全未成年人保护机制，加强新技术新应用新功能上线和使用管理，建立直播间运营者账号的分级管理制度和黑名单制度，建立健全投诉、举报机制。此外，《办法》还对平台协助消费者维权、协助依法纳税等方面提出了细化要求。《办法》在压实平台主体责任方面有所创新：一是提出事前预防，要求平台对粉丝数量多、交易金额大的重点直播间采取安排专人实时巡查、延长直播内容保存时间等防范措施。二是注重事中警示，要求平台建立风险识别模型，对风险较高和可能影响未成年人身心健康的行为采取弹窗提示、显著标识、功能和流量限制等调控措施。三是强调事后惩处，要求平台对违法违规行为采取阻断直播、关闭账号、列入黑名单、联合惩戒等处置措施。

四、问：《办法》对直播间运营者和直播营销人员提出哪些明确要求？

答：《办法》提出直播营销人员和直播间运营者为自然人的，应当年满十六周岁，要求直播间运营者、直播营销人员遵守法律法规和公序良俗，真实、准确、全面地发布商品或服务信息，明确直播营销行为 8 条红线，突出直播间 5 个重点环节管理，对直播营销活动相关广告合规、直播营销场所、互动内容管理、商品服务供应商信息核验、消费者权益保护责任、网络虚拟形象使用提出明确要求。《办法》还要求，直播间运营者、直播营销人员与直播营销人员服务机构开展商业合作的，应当与直播营销人员服务机构签订书面协议，明确信息安全管理、商品质量审核、消费者权益保护等义务并督促履行。

五、问：《办法》在保护消费者合法权益方面提出哪些举措？

答：针对社会舆论广泛关切的消费者权益保护问题，《办法》进行了多处强化。直播营销平台应当及时处理公众对于违法违规信息内容、营销行为投诉举报。消费者通过直播间内链接、二维码等方式跳转到其他平台购买商品或者接受服务，发生争议时，相关直播营销平台应当积极协助消费者维护合法权益，提供必要的证据等支持。直播间运营者、直播营销人员应当依法依规履行消费者权益保护责任和义务，不得故意拖延或者无正当理由拒绝消费者提出的合法合理要求。

六、问：为了更好地开展监督管理，《办法》明确了有关部门哪些职责？

答：《办法》提出，国家七部门建立健全线索移交、信息共享、会商研判、教育培训等工作机制，加强对行业协会商会的指导，对严重违反法律法规的直播营销市场主体名单实施信息共享，依法开展联合惩戒。同时，《办法》完善了民事、行政和刑事法律责任相衔接的

体系化规定。违反本办法，给他人造成损害的，依法承担民事责任；构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由网信等有关主管部门依据各自职责依照有关法律法规予以处理。（来源：中国网信网）

- **网络直播营销管理办法（试行）**
- **全文：**http://www.cac.gov.cn/2021-04/22/c_1620670982794847.htm

➢ 工信部：强化互联网市场竞争监管，加大力度保护用户个人信息

2021 年 4 月 20 日，工信部新闻发言人、信息通信管理局局长赵志国在国务院新闻办公室举行的新闻发布会上，针对记者提出的如何对待互联网企业垄断和不正当竞争现象的问题，作出如下回应：近年来我国互联网创新活跃，有力推动了数字经济的繁荣发展，同时资本无序扩张、平台强制二选一，违规过度收集使用个人信息等问题时有发生，引发了社会广泛的关注。工业和信息化部对此高度重视，结合我部职责，多年来持续加强互联网行业管理，维护市场秩序，保障用户权益，强化跨部门的协同，努力营造良好的发展环境。

近期，党中央、国务院就推动平台经济规范健康持续发展作出了工作部署，工业和信息化部坚决贯彻落实党中央、国务院的决策部署，下一步将立足主责主业，重点推动以下工作：

一是引导互联网企业加大科技创新的力度，鼓励头部企业参与国家的重大战略、重大工程，在 5G、云计算、人工智能、工业互联网等方面加大投入，推动数字产业化、产业数字化的发展，补短板、锻长板，助力提升我国科技核心竞争力。二是加强互联网行业市场的竞争监管，加大合规调查评估的力度，摸底筛查平台企业合规的情况，开展行业不正当竞争的专项整治行动，重点整治恶意屏蔽、强制捆绑、流量劫持、违规经营等扰乱市场竞争秩序的行为，加强信用管理，实施失信惩戒，打造公平开放的市场发展环境。三是加大用户个人信息的保护力度，持续开展 APP 侵犯用户权益问题的专项整治工作，充分利用法律、行政、技术等监管的手段，打好“组合拳”，形成一批典型案例，通报一批违规应用，处罚一批违规企业，取得标志性的成果。四是强化互联网协同监管和联合惩戒，加强协调配合，跨部门联合开展互联网领域专项的整治工作，强化信息共享和联动处置，形成治理的合力。完善联合执法惩戒机制，充分发挥技术优势，依法严厉查处违法违规互联网的相关应用。（来源：国新网）

五、本期重要漏洞实例

➢ IBM WebSphere Application Server XML 外部实体注入漏洞

发布日期：2021-04-20
更新日期：2021-04-23
受影响系统：
IBM Websphere Application Server 9.0
IBM Websphere Application Server 8.5
IBM Websphere Application Server 8.0
IBM Websphere Application Server 7.0
描述：

CVE(CAN) ID: CVE-2021-20454
IBM WebSphere Application Server（WAS）是美国 IBM 公司的一款应用服务器产品。该产品是 JavaEE 和 Web 服务应用程序的平台，也是 IBMWebSphere 软件平台的基础。
IBM WebSphere Application Server 7.0、8.0、8.5 和 9.0 版本在处理 XML 数据时存在 XML 外部实体注入漏洞。远程攻击者可利用该漏洞泄露敏感信息或消耗内存资源。
<*链接：https://www.ibm.com/support/pages/node/6445481
建议：

厂商补丁：
IBM

IBM 已经为此发布了一个安全公告（6445481）以及相应补丁:
6445481：Security Bulletin: WebSphere Application Server is vulnerable to an XML External Entity (XXE) Injection vulnerability (CVE-2021-20454)
链接：https://www.ibm.com/support/pages/node/6445481

➢ Cisco SD-WAN vManage Software 信息泄露漏洞

发布日期：2021-04-21
更新日期：2021-04-23
受影响系统：
Cisco SD-WAN vManage Software < 20.5.1
描述：

CVE(CAN) ID: CVE-2021-1491
Cisco SD-WAN vManage 是美国思科（Cisco）公司的一款可提供软件定义网络功能的软件。该软件为网络虚拟化的一种方式。
Cisco SD-WAN vManage Software 20.5.1 之前版本的 web 管理界面存在信息泄露漏洞。该漏洞源于文

件范围限制不足。经过身份认证的远程攻击者可通过在文件系统上创建特定的文件引用利用该漏洞从底层操作系统的文件系统读取任意文件。
<*来源：Johnny Yu (Walmart Security)
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-info-disclos-
*>
建议：

厂商补丁：
Cisco

Cisco 已经为此发布了一个安全公告（cisco-sa-vmanage-info-disclos-gGvm9Mfu）以及相应补丁：
cisco-sa-vmanage-info-disclos-gGvm9Mfu：Cisco SD-WAN vManage Software Information Disclosure Vulnerability
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-info-disclos-gGvm9Mfu

➢ 多款 Mozilla 产品内存错误引用漏洞

发布日期：2021-04-19
更新日期：2021-04-21
受影响系统：
Mozilla Firefox < 88
Mozilla Thunderbird < 78.10
Mozilla Firefox ESR < 78.10
描述：

CVE(CAN) ID: CVE-2021-23995
Mozilla Firefox 是一款开源 Web 浏览器。Mozilla Firefox ESR 是 Firefox(Web 浏览器)的一个延长支持版本。Mozilla Thunderbird 是一套从 Mozilla Application Suite 独立出来的电子邮件客户端软件。Firefox 88 之前版本、Firefox ESR 78.10 之前版本和 Thunderbird 78.10 之前版本的 Responsive Design Mode 存在内存错误引用漏洞。攻击者可利用该漏洞导致任意代码执行。
<*来源：Irvan Kurniawan
链接：https://www.mozilla.org/en-US/security/advisories/mfsa2021-16/
建议：

厂商补丁：
Mozilla

Mozilla 已经为此发布了一个安全公告（mfsa2021-16）以及相应补丁：
mfsa2021-16：Mozilla Foundation Security Advisory 2021-16
链接：https://www.mozilla.org/en-US/security/advisories/mfsa2021-16/

➢ Linux kernel 越界写入漏洞

发布日期：2021-03-07
更新日期：2021-04-21
受影响系统：
Linux kernel <= 5.11.3
描述：

CVE(CAN) ID: CVE-2021-27365
Linux kernel 是美国 Linux 基金会的开源操作系统 Linux 所使用的内核。
Linux kernel 5.11.3 及之前的版本存在越界写入漏洞。该漏洞源于 iSCSI 数据结构未执行适当的长度限制或检查，且可能超过 PAGE_SIZE 值。攻击者可利用该漏洞发送与 iSCSI 关联的长度为最大值的 Netlink 消息。
建议：

厂商补丁：
Linux

目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：
https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=f9dbdf97a5bd92b1a49cee3d591b55b11fd7a6d5

六、本期网络安全事件

➢ 运营商内鬼偷取公民信息赚近九千万，静默期号码也可注册出售

2021 年 4 月 21 日，据媒体报道，今年 2 月广州警方接到市民反映，某通讯营运公司“客服人员”来电以手机积分即将过期为由，要求客户尽快用积分兑换礼品。随后“客服人员”会用短信将链接发到用户手机里。而所谓的优惠换购，其实是不法之徒在偷偷收集公民个人信息。广州市公安局民警称，当用户进入由“客服人员”提供的换购链接进行选购时，支付页面会要求用户提供手机号、银行卡号、身份证号等超过正常收集范围的信息。通过此手段掌握了公民个人信息后，不法分子就去注册大量微信账号，出售给他人用于从事网络诈骗等犯罪活动。

据了解，该犯罪团伙共有 9 名成员，其中 5 人是某通信运营商公司的内部员工。自 2020 年 10 月至 2021 年 1 月，该团伙窃取公民信息，偷开、倒卖微信号 250 万个，涉案 972 宗，非法获利 8700 万元。目前该团伙人员已全部落网。

运营商漏洞：“静默期”号码可注册、出售

记者梳理发现，运营公司内部人员窃取公民信息，偷开、倒卖账号已非首次。据报道，今年 4 月 2 日，宁波警方破获一起特大电信诈骗案。嫌疑人刘某作为华南某通信运营商网管中心负责人，利用运营商系统内权限将 900 余万条号码出售给向非法短信接口团伙。该团伙用这些号码注册微信实施网络诈骗，涉及被骗资金 400 余万元。

值得注意的是，一个手机号只能注册一个微信账号，不法分子是如何利用买来的号码成功注册大量新微信号的？

据办理该案件的广州民警介绍，运营商一般会提前半年从工信部门获得一批号码段，这批号段的手机号码未实名注册和激活，半年之后再推向市场销售。而运营商公司的“内鬼”们，通过内部渠道批量获取了这些未开通手机号的验证码，然后通过内部软件批量化注册大量微信号。据悉，半年之后，这些被注册了微信的手机号销售到市场，于是出现有人开办新卡却发现已经被注册微信号的情况。

独立电信分析师付亮对记者表示，偷取公民信息的“内鬼”是钻了运营商监管的“空子”。“这些号码是前任机主抛弃后被运营商回收的，从运营商回收号码到再次售出，其中有 4 个月以上的‘静默期’。在此期间该号码保存在运营商的仓库中无法使用。”付亮解释。他还指出，用处在“静默期”的号码注册微信号再贩卖出去，原则上并不涉及机主的用户隐私。因为不法分子相当于是用第三方信息注册的微信，与前机主无关，与再买到该账号的后机主也无关。这种行为的主要危害在于将账号出售给不法分子从事诈骗活动，从而造成财产损失。

内鬼抓住了运营商监管不严的漏洞，能在‘静默期’里通过内部渠道偷取到账号，并用内部软件批量注册。直到有用户反映，拿到的新号码已经被开过微信了，才引起运营商的重视展开自我复查。”付亮说。

专家：应明确权责，实现业务全流程可追溯

为什么公民信息遭运营商内鬼偷取事件频频发生？应如何解决？对此，北京师范大学网络法治国际中心执行主任、博导、中国互联网协会研究中心副主任吴沈括总结了公民信息泄露事件中“内鬼”频发的三个原因。

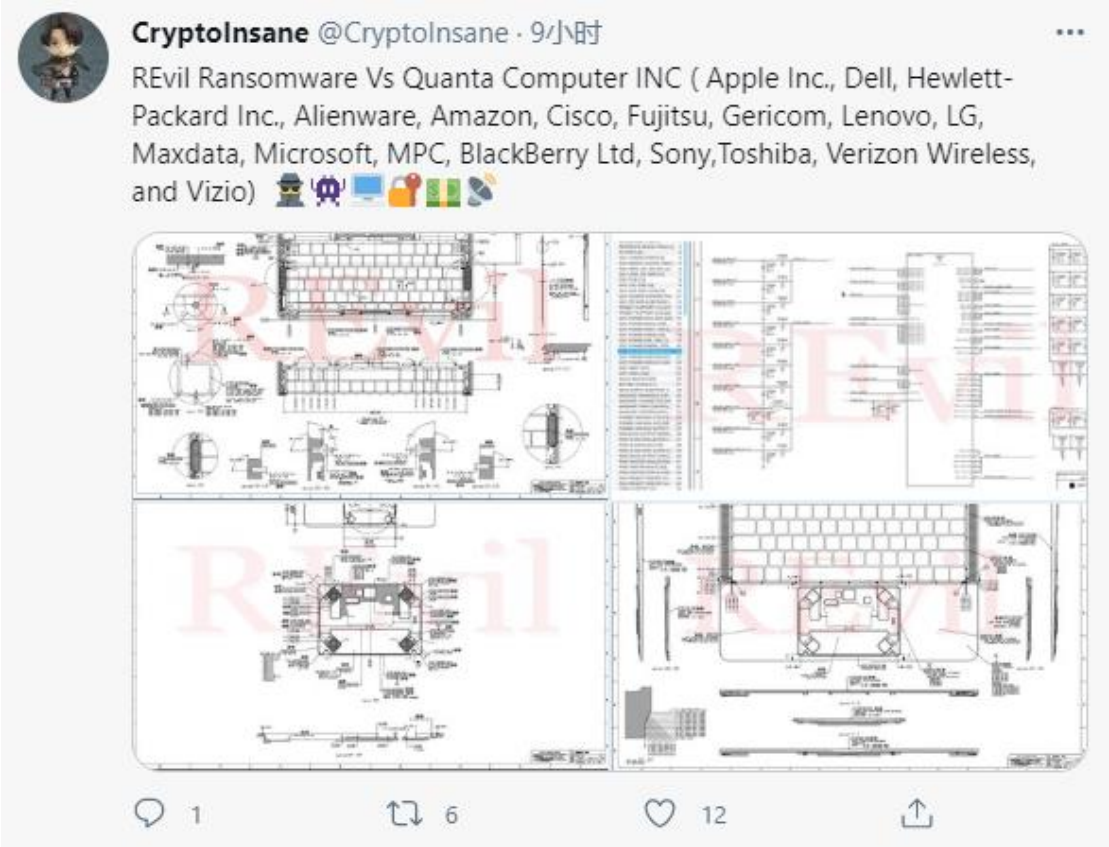
第一，相比外部人员，他们和数据资产的距离更近，有业务方便，容易得手；第二，“内鬼”往往是企业外部黑产的重点围猎对象，被“拉下水”的几率更高；第三，个别企业设定的不合理业绩要求往往间接促使内部人员为了满足考核要求去铤而走险。他还指出，这类问题的应对思路应是多方共治的多策并举。“首先，要推动企业内部建立清晰有效的‘定岗定责定人’制度，实现业务操作全流程的可追溯、可审计，确保‘数据-业务-人员’的严格匹配。其次，应鼓励支持建立面向社会大众的投诉举报激励机制，发挥社会力量的外部监督作用。再者，强化典型监管执法案例和司法裁判案例，以案说法，为数据业务运营和民众维权提供清晰的指引。”

从监管角度来看，付亮认为运营商应尽快填补“漏洞”。他强调，要定期对账号数据展开常规性核查，检测是否存在异常性使用现象，从根源上扼杀通过注册贩卖微信号实施网络

诈骗的苗头。此外，谈及“运营商内鬼偷取公民信息”一事，浙江垦丁律师事务所联合创始人麻策直言，个人信息的泄露最难防的并不在外部，而是内部泄露风险。公司在运营中应通过培训加强员工网络安全意识，明确个人信息分级分类权限，特别对批量化的导出下载等敏感事件进行预警，避免公司“内鬼”带来风险。（来源：互联网综合整理）

➢ 苹果代工厂广达遭黑客勒索：称窃取苹果机密索要巨额赎金

2021 年 4 月 21 日，臭名昭著的 REvil 勒索病毒又盯上了全球最大的大笔记本代工厂。据外媒报道，周二，REvil 黑客组织公开宣称，入侵了著名笔记本代工厂广达电脑(Quanta Computer)，称窃取了苹果的设计蓝图，索要 5000 万美元(约合人民币 3.25 亿元)赎金。据悉，广达电脑成立于 1988 年，是全球第一大笔记型电脑研发设计制造公司。与包括苹果、戴尔、惠普、黑莓等数十家全球大型科技公司有着密切的合作关系。今天，苹果公司刚刚召开了新品发布会。而 REvil 黑客组织也刚好在这个时间宣称窃取了苹果的产品设计蓝图，并且表示还将公布一些窃取的设计蓝图。



该黑客组织要求苹果公司在 5 月 1 日前“回购”这些被盗文件，否则将会每天都在其泄

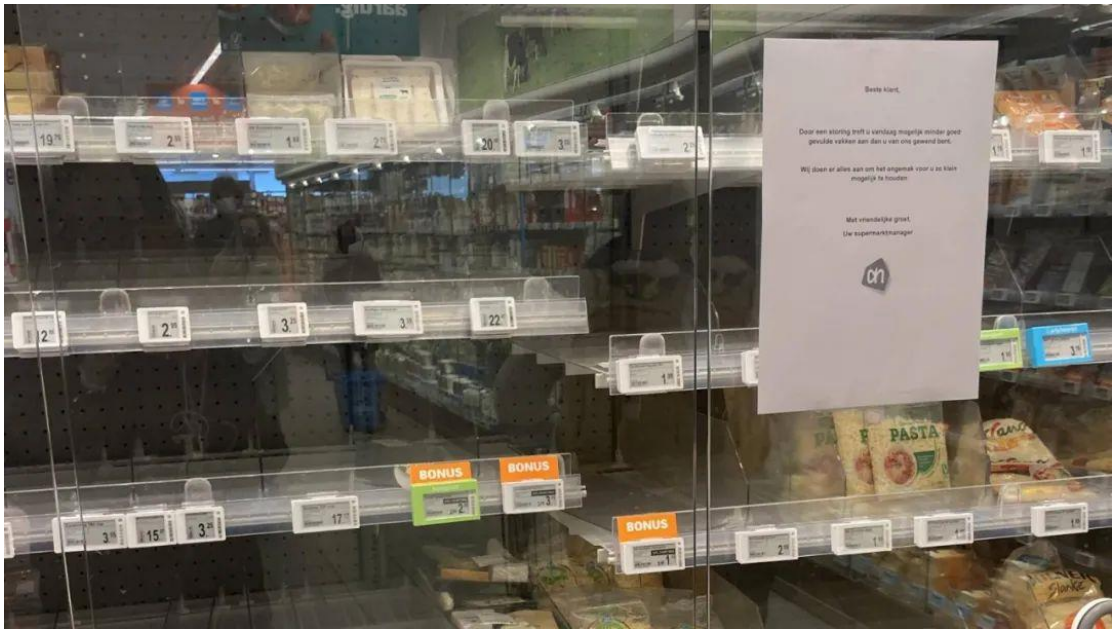
密网站公布部分这些机密文件。此外，该团伙还向广达电脑索取了 5000 万美元的赎金，要求其在 4 月 27 日前来赎回这些被盗数据。报道称，广达拒绝支付相关赎金。

不过，从目前泄露的设计蓝图来看，似乎是 Macbook 的设计图，并不是十分重要的设计。值得一提的是，在上个月，REvil 黑客组织攻击了全球著名 PC 制造商宏碁，并公布了疑似宏碁内部资料的截图，可以看到财务报表、流水账单、银行交易等等敏感信息，同样索要了 5000 万美元的赎金。

广达发布声明表示：已与多家外部公司技术专家合作，共同处理此次针对广达少部分服务器的网络攻击，日常营运未受影响。广达还称，已于第一时间启动信息安全防御机制，并进行网络攻击的清查，少数受到影响的内部服务均已恢复运作。（来源：快科技）

➢ 黑客攻击物流公司致供应链中断,荷兰超市奶酪短缺

2021 年 4 月 15 日，据今日俄罗斯电视台 14 日报道，荷兰一家大型物流公司遭到黑客的勒索软件攻击，导致该国供应链中断，继而引发奶酪等商品短缺，荷兰许多超市的货架上空空如也。



Bakker Logistiek 是荷兰国内规模最大的物流服务商之一，专门为荷兰各超市提供恒温仓储与食品运输服务。就在上周，Bakker Logistiek 公司遭遇勒索软件攻击，业务网络上的设备被对方加密，食品运输与配送体系也随之瘫痪。

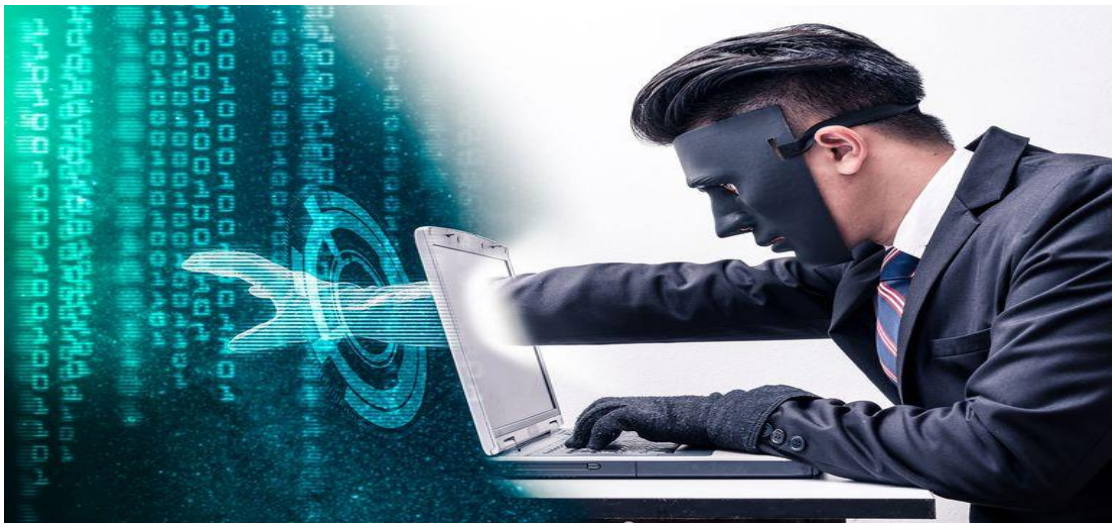
该公司主管 Toon Verhoeven 就此事接受采访时表示，“我们无法正常接收客户订单，也

搞不清现有商品存放在仓库内的哪些区域。我们的仓库非常巨大，逐一排查根本就不现实。我们还有大量配送货车，但由于统筹调度工作根本无法手动完成，目前的运输业务也无法正常运转。”此次事件给荷兰最大的连锁超市 Albert Heijn 直接带来连锁反应，包括奶酪在内的多种食品暂时无法供应。

货品短缺迫使 Albert Heijn 在其官方网站上发布通告，提醒客户独立包装的奶酪已经出现供应问题。该超市在官网上写道，“由于技术故障，采用独立包装的奶酪货品供应受限。物流服务商正努力解决问题并尽快恢复供应。对于由此带来的不便，我们深表歉意。”Bakker Logistiek 公司表示可以使用备份副本恢复受到影响的系统，并已经开始与客户方面协调以恢复配送业务。目前还不清楚勒索软件团伙是如何针对 Bakker Logistiek 发动攻击的，但 Verhoeven 在采访中提到，他们猜测攻击方是通过最近披露的微软 Exchange 服务的 ProxyLogon 漏洞掌握了系统访问权限。Bakker Logistiek 公司并不是全球首家遭遇勒索软件攻击的仓储物流运营商。去年 11 月，国际恒温仓储运营商 Americold 同样遭遇勒索软件攻击，期间电话系统、电子邮件、库存管理与订单履行等均受到影响。（来源：环球时报）

➢ 魔蝎科技非法缓存两千万条数据，被判侵犯个人信息罚三千万

2021 年 4 月 15 日，一年多前，杭州、上海多家数据科技公司接连被查，一时间大数据行业人人自危，纷纷关闭旗下的爬虫服务。近日，首批被查的杭州魔蝎科技公司（下称“魔蝎科技”）相关案件迎来一审判决。判决结果显示，魔蝎科技犯侵犯公民个人信息罪，判处罚金三千万元。公司法人周某某被判有期徒刑三年，缓刑四年；技术总监袁某被判有期徒刑三年，缓刑三年。



魔蝎公司非法存储个人信息两千万余条

据此前报道，据魔蝎科技官网（现已无法打开）介绍，魔蝎科技成立于 2016 年，是国内领先的大数据智能风控服务供应商，为 2000 多家银行、消费金融、保险、互联网金融等客户提供精准营销评分模型、反欺诈、多维度用户画像、授信评分、贷后预警、催收智能运筹等全面风险管理服务。

法院审理查明，魔蝎科技会将其开发的前端插件嵌入网贷平台 A**中。网贷平台用户使用网贷平台的 App 借款时，需要在魔蝎科技提供的前端插件上输入其通讯运营商、社保、公积金、淘宝、京东、学信网、征信中心等网站的账号、密码。

经过用户授权后，魔蝎科技的爬虫程序即代替用户进入其个人账户，利用各类爬虫技术，爬取（复制）上述企、事业单位网站上贷款用户本人账户内的通话记录、社保、公积金等各类数据，并按与用户的约定提供给网贷平台用于判断用户的资信情况，并从网贷平台获取每笔 0.1 元至 0.3 元不等的费用。

尽管魔蝎科技在和个人贷款用户签订的《数据采集服务协议》中明确告知，“不会保存用户账号密码，仅在用户每次单独授权的情况下采集信息”，但其仍在服务器上采用技术手段长期保存用户各类账号和密码。截至 2019 年 9 月案发时，以明文形式非法保存的个人贷款用户各类账号和密码条数多达 2000 万余条。

根据两高《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》，非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息 50 条以上即可入罪。

西湖法院认为，魔蝎科技以其他方法非法获取公民个人信息，情节特别严重，其行为已构成侵犯公民个人信息罪，判处罚金人民币三千万元；被告人周某某犯侵犯公民个人信息罪，判处有期徒刑三年，缓刑四年，并处罚金人民币 50 万元；被告人袁某犯侵犯公民个人信息罪，判处有期徒刑三年，缓刑三年，并处罚金人民币 30 万元。（来源：隐私护卫队）

➢ 男子用技术手段恢复女方微信记录并散布 涉侵犯隐私被拘 6 日

2021 年 4 月 16 日，浙江台州临海市公安局近日侦破一起侵犯隐私案件。一男子因情感问题发生纠纷，用技术手段恢复女方微信聊天记录，且发至微信朋友圈和女方母亲及女方未婚夫母亲，构成侵犯隐私，被行政拘留 6 日。

4 月 16 日从台州警方人士处获悉，事发后，警方在杭州将该男子抓获，因涉嫌侵犯个

人隐私，其被行拘 6 日。稍早前，网传一份由临海市公安局出具的行政处罚书显示，现查明 3 月 21 日 23 时许，违法行为人张某峰与被侵害人项某醒因情感问题发生纠纷，遂用技术手段将项某醒手机内的微信聊天记录恢复，后将部分微信聊天记录发送至微信朋友圈、项某醒母亲及项某醒未婚夫母亲。违法行为人张某峰的行为已构成侵犯隐私，且情节较重。

以上事实有违法行为人张某峰的陈述和申辩、被侵害人项某醒的陈述、证人证言、归案经过、接受证据清单、身份信息等证据证实。如不服本决定，可以在收到本决定书之日起六十日内向临海市人民政府申请行政复议或者在六个月内依法向临海市人民法院提起行政诉讼。

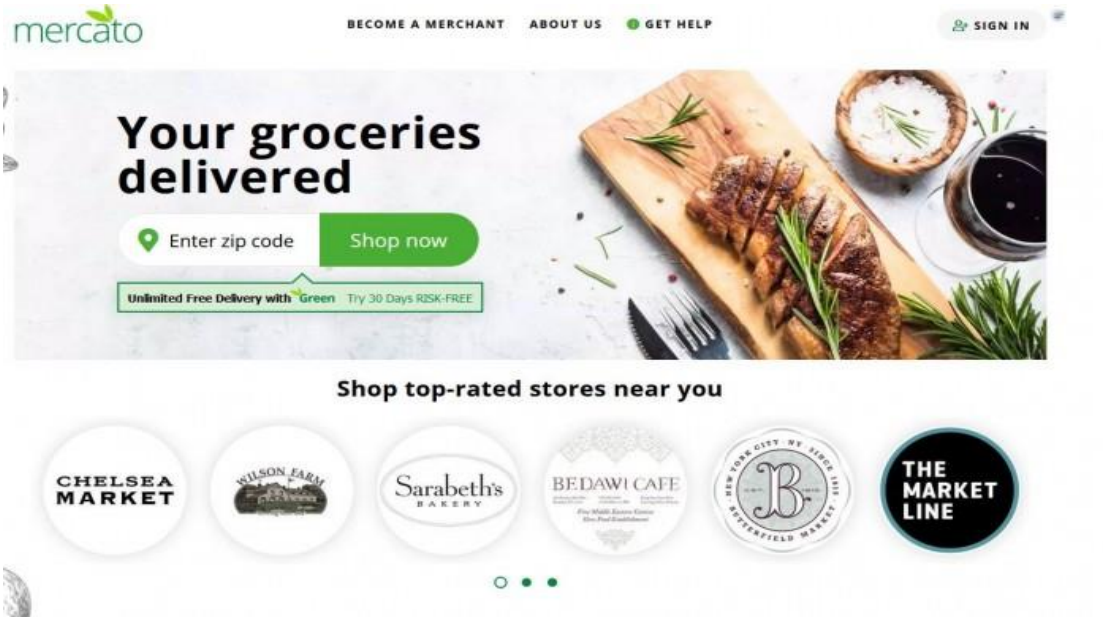
该行政处罚书显示，根据《中华人民共和国治安管理处罚法》第四十二条第(六)项之规定，决定给予张某峰行政拘留 6 日的行政处罚。该份行政处罚书盖有临海市公安局的印章，落款时间为 2021 年 4 月 8 日，有被处罚人张某峰签字及手印。（来源：澎湃新闻）

➢ 配送平台 Mercato 发生数据泄漏 却没向用户发出提醒

2021 年 4 月 15 日，援引外媒 TechCrunch 报道，在线杂货配送初创公司 Mercato 在今年 1 月发生了用户数据泄漏事件，导致数万用户的个人隐私被窃取。导致泄漏的原因是公司托管在亚马逊云端的一个云存储桶被攻击，且没有受到保护。在事件发生之后该公司只是修复了这些数据，但没有向用户发出提醒。

Mercato 成立于 2015 年，主要帮助超过 1000 家小型杂货店和专业食品店提供取餐

和配送服务，用户不需要注册 Instacart 或亚马逊 Fresh 等送货服务。Mercato 在波士顿、芝加哥、洛杉矶和纽约开展业务，并在这些地区设有办公场所。



根据外媒 TechCrunch 获得的一份数据副本，该副本中包含了 7 万份订单，时间是在 2015 年 9 月至 2019 年 11 月的，包括了客户姓名和电子邮件地址、家庭地址和订单详情。每条记录还有用户用于下单的设备的 IP 地址。该数据集还包括公司高管的个人资料和订单细节。

目前还不清楚安全漏洞是如何发生的，因为亚马逊云上的存储桶默认是私有的，也不清楚公司是什么时候得知这一曝光事件的。公司需要向州检察长披露数据泄露或安全漏洞，但在法律要求的地方，比如加州，还没有发布通知。该数据集在加州有超过 1800 名用户，是该州数据泄露通知法规定的触发强制披露所需人数的三倍多。（来源：cnbeta）