# 国盟信息安全通报

2021 年 12 月 31 日第 246 期

全国售后服务中心

# 国盟信息安全通报

（第 246 期）

国际信息安全学习联盟

**2021 年 12 月 31 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 588 个，其中高危漏洞 203 个、中危漏洞 303 个、低危漏洞 82 个。漏洞平均分值为 5.70。本周收录的漏洞中，涉及 0day 漏洞 193 个（占 33%），其中互联网上出现“News Portal Project SQL 注入漏洞（CNVD-2021-102010）、Belloo SQL 注入漏洞”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 19707 个，与上周（10886 个）环比增加 81%。

# 主要内容



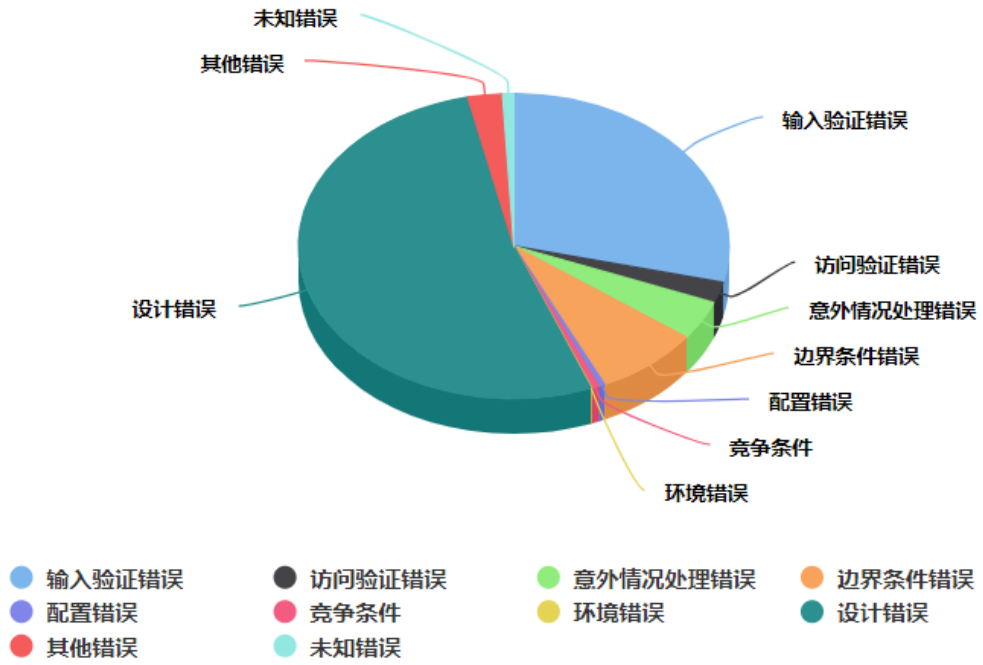
**注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。**

# 一、概述

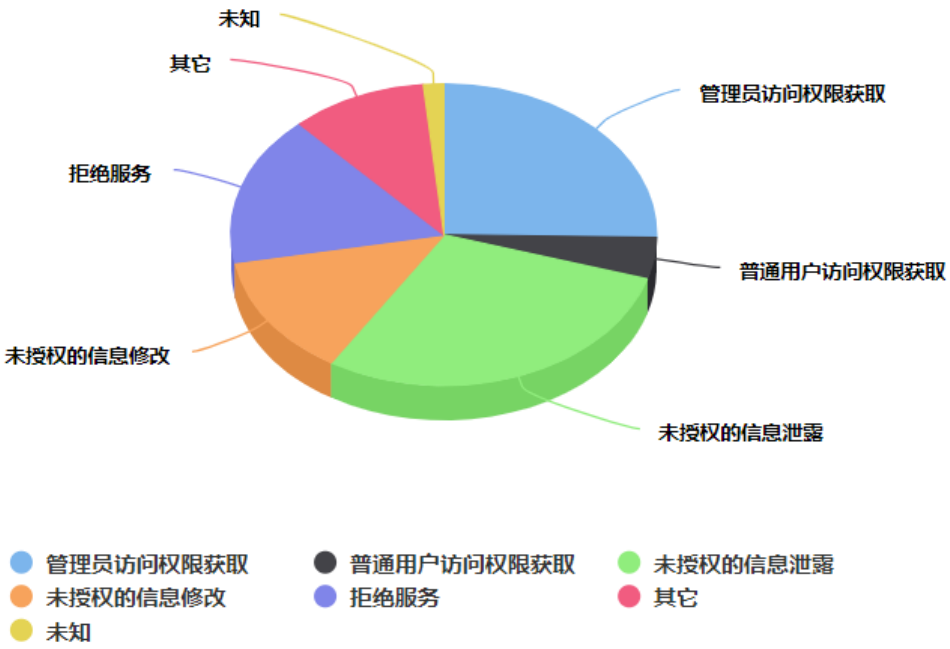
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 588 个，其中高危漏洞 203 个、中危漏洞 303 个、低危漏洞 82 个。漏洞平均分值为 5.70。本周收录的漏洞中，涉及 0day 漏洞 193 个（占 33%），其中互联网上出现“News Portal Project SQL 注入漏洞（CNVD-2021-102010）、Belloo SQL 注入漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 19707 个，与上周（10886 个）环比增加 81%。

# 二、安全漏洞增长数量及种类分布情况

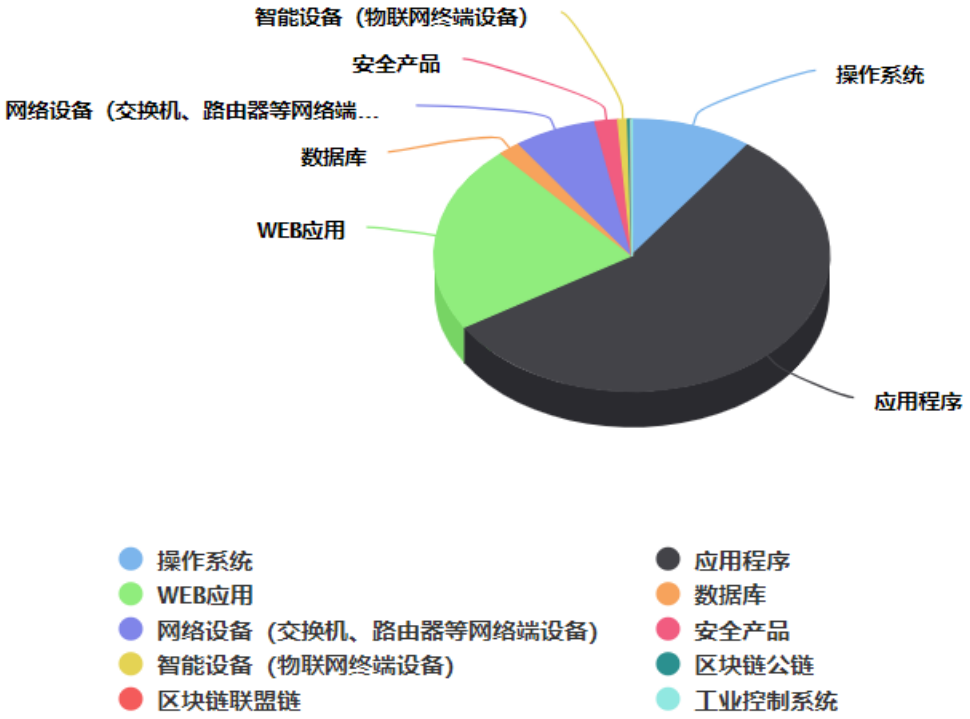
➢ **漏洞产生原因（2021 年 12 月 1 日—2021 年 12 月 31）**



## ➢ 漏洞引发的威胁（2021 年 12 月 1 日—2021 年 12 月 31）




## ➢ 漏洞影响对象类型（2021 年 12 月 1 日—2021 年 12 月 31）



# 三、安全产业动态

## ➢ 隐私泄露之风当休矣 个人信息保护任重道远

备受瞩目的《中华人民共和国个人信息保护法》落地满一个月，我们的个人信息还在“裸奔”吗？记者调研发现，买房信息泄露、App 过度收集信息、视频平台索要会员照片等现象仍然出现在我们身边。多位专家认为，我国对个人信息的保护工作不断完善，但是隐私泄露难以在短时间内“急刹车”，进一步保护个人信息仍任重道远。

个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。随着我国市场化程度的不断加深，以及互联网、大数据、云计算的广泛应用，公民个人信息保护已成为一个日益严峻的课题。

国家移动互联网应用安全管理中心数据显示，11 月 1 日以来，有 44 款 App 被发现隐私不合规，其中不乏多点、亚马逊购物等安装量超过千万次的热门 App。在消费者服务平台上，11 月以来涉及个人信息泄露的投诉五花八门：手机号遭泄露被乱发快递、某平台授信后半小时内接到 4 个境外贷款诈骗电话、从未注册过的 App 发送额度短信、商家偷偷用个人信息刷单、视频平台索取会员的个人照片等等。

个人信息泄露不仅意味着我们会收到大量骚扰电话和短信，更可能成为滋生网络犯罪的温床。据最高人民法院有关部门负责人介绍，19.16%的网络诈骗案件具有精准诈骗的特征，即不法分子获取公民个人信息后有针对性地实施诈骗，极大地提高了诈骗得逞的可能性。据

媒体报道，有相当数量的人在一些虚假贷款 App 或网站上提交了包括姓名、身份证照片、个人资产证明、银行账户、地址等在内的大量个人隐私信息，造成了较为严重的信息泄露和经济损失。

事实上，我国对公民个人信息保护力度不断加大，并通过立法加强对公民个人信息进行保护。《中华人民共和国民法典》、《中华人民共和国网络安全法》等法律明确对个人信息的法律保护。作为保护个人信息的专门立法，落地月余的《中华人民共和国个人信息保护法》更是被寄予厚望。为何线上线下仍有不少平台机构有恃无恐？究其原因主要是：违法惯性不可能一朝改变，一些违法企业已经尝到了靠违法违规收集使用个人信息建立业务线甚至直接售卖个人信息的甜头；执法过程中仍有模糊地带，不少用户难以判定必要信息、敏感信息，给 App 肆无忌惮地超限收集用户隐私留有可乘之机；法律法规仍需细化，在数据的归集、加工、流动等方面进一步健全相关法规。

个人信息保护法的施行掷地有声，不仅凸显了我国严管侵犯个人隐私行为的坚定决心，也是对保护个人信息的郑重声明。公民个人信息保护有赖于法律体系的整体完善，不仅需要针对各种类型的犯罪行为不断健全法律法规，提升监测和侦破的技术手段，还需要加强全社会法律意识和监督意识，重点把控相关企业和机构的规范水平，从源头遏制住对公民个人信息的侵犯，提升全社会信息安全水平。执法是最好的普法，要及时对典型案例进行通报，在提高群众法律意识的同时，对盗取个人信息的违法分子形成威慑。期待通过常态化、制度化的监管，切实守住公民个人信息安全这道关口，推动个人信息保护法更好贯彻落实。（来源：民主与法制时报）

## ➢ 立足百年大党奋斗新起点 谱写网络强国建设新篇章

2021 年 12 月 17 日，中共中央党校《学习时报》在头版头条刊发中央宣传部副部长、中央网络安全和信息化委员会办公室主任、国家互联网信息办公室主任庄荣文署名文章。全文转发如下：

**全文转发如下：**

党的十九届六中全会是在我们党成立一百年之际，党领导人民实现第一个百年奋斗目标、向着实现第二个百年奋斗目标迈进的重大历史关头召开的，时机特殊、议题重大，在党的历史上具有重要里程碑意义。全会审议通过了《中共中央关于党的百年奋斗重大成就和历史经

验的决议》（以下简称《决议》）和《关于召开党的第二十次全国代表大会的决议》，习近平总书记在全会上发表了重要讲话。全会取得的重大成果、作出的重大部署，必将对推动全党统一思想、统一意志、统一行动，团结带领全国各族人民以史为鉴、开创未来，埋头苦干、勇毅前行，在新时代更好坚持和发展中国特色社会主义、实现中华民族伟大复兴产生重大而深远的影响。

深入学习宣传贯彻党的十九届六中全会精神，是当前和今后一个时期全党全国的重要政治任务，也是全国网信系统的头等大事。汲取百年奋斗伟力，开启新的伟大征程，我们必须深入学习宣传贯彻党的十九届六中全会精神，汲取百年奋斗历史经验，把握信息革命时代潮流，奋力谱写网络强国建设新篇章。

**深刻认识全会精神的重大历史意义，全面把握党领导人民百年奋斗的初心使命，进一步增强做好网信工作的责任感和使命感。**不忘初心，方得始终。一百年来，我们党团结带领中国人民进行的一切奋斗、一切牺牲、一切创造，都是在践行为中国人民谋幸福、为中华民族谋复兴的初心使命，这是党的历史发展的主题主线和主流本质。全会《决议》站在实现中华民族伟大复兴的历史高度，分新民主主义革命时期、社会主义革命和建设时期、改革开放和社会主义现代化建设新时期、中国特色社会主义新时代四个历史时期，对党的百年奋斗重大成就进行了全面总结、精辟概括，指出党和人民百年奋斗，书写了中华民族几千年历史上最恢宏的史诗。《决议》指出，马克思主义信仰、共产主义远大理想、中国特色社会主义共同理想，是中国共产党人的精神支柱和政治灵魂，也是保持党的团结统一的思想基础。理想信念是共产党人精神上的“钙”，共产党人如果没有理想信念，精神上就会“缺钙”，就会得“软骨病”。

面向新时代新征程，我们要进一步坚定理想信念、牢记初心使命，进一步增强历史自觉、历史自信、历史责任，努力从苦难辉煌的党的百年奋斗历程中、从源远流长的人类历史演进

中、从波澜壮阔的全球风云变迁中、从蓬勃发展的信息时代大潮中，深刻领会网信工作肩负的历史使命，深刻把握网信工作“从哪里来、到哪里去”的重大课题，自觉把网信工作置身重要战略机遇期、置身“两个大局”中去谋划部署，以永不懈怠的精神状态和一往无前的奋斗姿态，加快推进网络强国建设，创造无愧于历史的新业绩。

**深刻认识全会精神的重大政治意义，全面把握“两个确立”的精神实质，进一步增强做到“两个维护”的思想自觉、政治自觉、行动自觉。**党的十八大以来，以习近平同志为核心的党中央团结带领人民，推动党和国家事业取得历史性成就、发生历史性变革，实现中华民族伟大复兴进入了不可逆转的历史进程。实践充分证明，万山磅礴必有主峰，船重千钧掌舵一人。有习近平总书记掌舵领航，党和人民事业就有了定盘星、主心骨，面对惊涛骇浪就能够“稳坐钓鱼船”。党确立习近平同志党中央的核心、全党的核心地位，确立习近平新时代中国特色社会主义思想的指导地位，是全党全军全国各族人民共同心愿，这也是我们总结新时代这段历史的最大政治成果、最重要实践经验、最宝贵历史财富，对于新时代党和国家事业发展具有根本性、决定性、历史性意义。

党的十八大以来，习近平总书记作为党中央的核心、全党的核心，亲自领导和直接推动网信事业发展，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，在于习近平新时代中国特色社会主义思想特别是习近平总书记关于网络强国的重要思想的科学指引。面向新时代新征程，我们要始终把“两个确立”作为最执着的政治信念、最深刻的政治领悟、最坚定的政治立场、最重要的政治原则，牢牢把握网信工作显著的政治特征和网信部门鲜明的政治属性，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，不折不扣贯彻落实习近平总书记重要指示批示精神和党中央决策部署，确保网信事业始终沿着正确政治方向和道路前进。

**深刻认识全会精神的重大理论意义，全面把握马克思主义中国化的最新成果，进一步深学细悟笃行习近平新时代中国特色社会主义思想。**党的百年历史，就是一部不断推进马克思主义中国化的历史，就是一部不断推进理论创新、进行理论创造的历史。全会《决议》强调，习近平新时代中国特色社会主义思想是当代中国马克思主义、二十一世纪马克思主义，是中华文化和中国精神的时代精华，实现了马克思主义中国化新的飞跃。《决议》用“十个明确”进一步对习近平新时代中国特色社会主义思想的核心内容作了系统概括，指出习近平同志对关系新时代党和国家事业发展的一系列重大理论和实践问题进行了深邃思考和科学判断，就新时代坚持和发展什么样的中国特色社会主义、怎样坚持和发展中国特色社会主义，建设什

么样的社会主义现代化强国、怎样建设社会主义现代化强国，建设什么样的长期执政的马克思主义政党、怎样建设长期执政的马克思主义政党等重大时代课题，提出一系列原创性的治国理政新理念新思想新战略，是习近平新时代中国特色社会主义思想的主要创立者。

党的十八大以来，习近平总书记从信息化发展大势和国内国际大局出发，就网信工作提出了一系列新思想新观点新论断，系统回答了为什么要建设网络强国、怎样建设网络强国等一系列重大理论和实践问题，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。这一重要思想，是习近平新时代中国特色社会主义思想的重要组成部分，是我们党管网治网实践经验的理论总结，是引领我国网信事业发展的行动指南。面向新时代新征程，我们要全面强化思想引领，始终坚持以习近平新时代中国特色社会主义思想特别是习近平总书记关于网络强国的重要思想武装头脑、指导实践、推动工作，更加深入学习领会蕴含其中的丰富内涵、精神实质、实践要求，努力从中把握网信工作的方向思路、目标任务、方法途径，做到学思用贯通、知信行统一，切实将科学理论的强大思想伟力转化为推进网络强国建设的巨大实践动力。

**深刻认识全会精神的重大实践意义，全面把握党百年奋斗的历史经验，进一步探索网信工作规律、完善中国特色治网之道。**全会《决议》以宏阔的历史视角，用“十个坚持”全面总结了党领导人民进行伟大奋斗积累的宝贵历史经验，系统阐释了党永葆青春活力的“成功密码”。这“十个坚持”的历史经验是系统完整、相互贯通的整体，揭示了党和人民事业不断成功的根本保证，揭示了党始终立于不败之地的力量源泉，揭示了党始终掌握历史主动的根本原因，揭示了党永葆先进性和纯洁性、始终走在时代前列的根本途径，进一步深化了我

们党对共产党执政规律、社会主义建设规律、人类社会发展规律的认识。这些经过长期实践积累的宝贵经验，既是“过去我们为什么能够成功”的深刻总结，更是“未来我们怎样才能继续成功”的行动指南，激励着我们以更加昂扬的姿态迈进新征程、建功新时代。

党的十八大以来，以习近平同志为核心的党中央从进行具有许多新的历史特点的伟大斗争出发，高度重视互联网、大力发展互联网、积极运用互联网、有效治理互联网，推动网信事业从夯基垒台到积厚成势、从发展起步到不断壮大，在攻坚克难中迈出坚实步伐，在开拓创新中取得重大突破，取得历史性成就、发生历史性变革。在这个过程中，形成了一系列管网治网的规律性认识，探索走出了一条中国特色治网之道，一些重要理论和实践成果都写入了《决议》。面向新时代新征程，我们要深入总结党的十八大以来党领导网信工作的实践经验，把握管网治网工作规律，深化网信领域重大理论和实践问题研究，深入推进网信领域理念思路、工作内容、方式手段、体制机制等全方位创新，进一步探索中国特色治网之道，形成更加成熟、更加完备、更加定型的中国特色治网模式，努力使网信工作体现时代性、把握规律性、富于创造性，不断增强网信事业发展的动力和活力。

**深刻认识全会精神的重大时代意义，全面把握以史为鉴、开创未来的重要要求，进一步以网络强国建设助力实现中华民族伟大复兴。**胸怀千秋伟业，百年只是序章。全会在全面总结党的百年奋斗重大成就和历史经验的基础上，面向新时代新征程，展望了我们国家和民族发展的美好前景，对走好实现第二个百年奋斗目标新的赶考之路提出要求，号召全党要牢记中国共产党是什么、要干什么这个根本问题，以咬定青山不放松的执着奋力实现既定目标，以行百里者半九十的清醒不懈推进中华民族伟大复兴。这些重要要求发出了奋进新时代的动员令、吹响了建功新时代的集结号，对于全党更加坚定、更加自觉地践行初心使命，更好坚持和发展中国特色社会主义，具有重大意义。

习近平总书记多次强调，建设网络强国的战略部署要与“两个一百年”奋斗目标同步推进。全会站在党长期执政的高度，准确把握信息时代的“时”与“势”，把“过不了互联网这一关就过不了长期执政这一关”这一重大论断写进《决议》，充分体现了党中央对网信工作的高度重视和殷切期望。面向新时代新征程，我们要深刻把握全会就网信工作作出的新论断新部署新要求，增强锚定既定奋斗目标、意气风发走向未来的勇气和力量，进一步明确网信工作的时代方位、职责使命、路径选择，聚焦党中央部署的重大事项、网信领域面临的重大问题、制约事业发展的突出障碍，有效防范化解网信领域各类风险隐患，加快实施“十四五”网信发展规划，持续做好习近平新时代中国特色社会主义思想网上宣传工作，扎实做好迎接服务保障党的二十大工作，持续推进网信领域科技自立自强，迈出信息化发展新步伐，

筑牢网络安全新屏障，塑造网络空间国际合作新格局，推动网信工作高质量发展，以网络强国建设的新进展新成效为全面建设社会主义现代化国家、实现中华民族伟大复兴的中国梦提供强大网上舆论支持、可靠网络安全保障和有力信息化支撑。（来源：学习时报）

## ➢ 为数据安全提供基础性法律保障

随着互联网、大数据、人工智能等蓬勃发展，各类数据迅猛增长、海量聚集，对国家治理、社会发展、人民生活都产生了深刻影响。数据已经成为一种新的生产要素，与此相关的数据安全问题也日益凸显。今年 9 月 1 日，《中华人民共和国数据安全法》开始施行，这为我国数据安全提供了基础性法律保障。深入理解和贯彻实施数据安全法，对于更好维护数据安全、充分发挥数据效能具有重要意义。

**体现践行总体国家安全观的要求。**习近平总书记强调：“把国家安全贯穿到党和国家工作各方面全过程，同经济社会发展一起谋划、一起部署，坚持系统思维，构建大安全格局”。数据安全是国家安全的重要组成部分。数据安全法确立和完善了数据安全保护管理的各项基本制度，形成了我国保障数据安全的顶层设计，在数据安全领域践行了总体国家安全观的要求。比如，规定国家建立数据分类分级保护制度，根据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、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护；国家建立集中统一、高效权威的数据安全风险评估、报告、信息共享、监测预警机制；等等。这些规定对于保障数据安全，

维护国家主权、安全、发展利益具有重要意义。

**坚持发展与安全并重。**近年来，我国积极推进数字产业化、产业数字化，引导数字经济和实体经济深度融合，推动经济高质量发展。“十四五”规划和 2035 年远景目标纲要提出“加快数字化发展，建设数字中国”，强调“打造数字经济新优势”。同时，将统筹发展和安全纳入“十四五”时期我国经济社会发展的指导思想，并列专篇作出战略部署。这就要求我们在充分发挥数据资源作为未来基础资源和创新引擎作用、加快发展数字经济的同时，牢牢守住数据安全的底线。数据安全法坚持发展与安全并重，明确鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以数据为关键要素的数字经济发展。数据安全法还设“数据安全与发展”专章，规定国家实施大数据战略、支持开发利用数据提升公共服务的智能化水平、支持数据开发利用和数据安全技术研究、推进数据开发利用技术和数据安全标准体系建设等内容，为支持、促进数据安全与发展提供法治保障。

**强化个人和组织主体责任。**保障数据安全，切实维护个人、组织的合法权益，关键是立足数据安全工作实际，着力解决数据安全领域的突出问题，明确并严格落实包括个人和组织在内的各类数据处理活动主体的安全保护义务与责任。数据安全法设“法律责任”专章，细化了数据处理活动主体承担责任的具体情形和责任形式，为数据处理活动主体设置了行为底线，增强了数据安全法的规范效力。比如，数据安全法规定，开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。开展数据处理活动的个人、组织不履行这一义务，由有关主管部门责令改正，给予警告，可以并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款。这些规定，有利于引导数据处理活动主体更加自觉采取合法、正当方式开展数据处理活动，夯实保障数据安全的社会根基。（来源：人民日报）

## ➢ 个人金融信息保护面临的困难与对策研究

随着信息技术在社会各个领域的普及应用，个人信息采集的广度和深度不断拓展，个人信息运用趋于电子化、规模化和产业化，信息流动更是突破地域和行业限制。与此同时，受利益驱使，不法分子通过泄露、冒用、倒卖等手段利用个人的金融信息进行非法牟利，对个人金融信息侵害的非法行为甚至已经演化为产业链模式，不但侵害客户的合法权益,扰乱市

场经济秩序,严重危害社会经济正常发展。本文对个人金融信息保护重要意义进行了阐述，全面分析个人金融信息保护工作面临的困难和挑战，并对加强个人金融信息保护提出建议。

**个人金融信息保护的必要性**

**1.加强个人金融信息保护是维护国家金融安全的必然要求。**金融是现代经济的核心，金融安全是国家安全的重要组成部分。互联网经济的迅猛发展，在极大便利社会民生的同时，也催生了大量个人信息泄露事件，致使垃圾信息、骚扰电话、精准诈骗时有发生，由此带来的侵权违法活动呈多发态势。个人金融信息泄露，不仅对人民群众财产安全和金融行业资金及声誉造成威胁，也严重侵扰了公民的日常生活，甚至危及社会的长治久安。因此，要从源头上推进金融安全综合治理必须加强个人金融信息保护。


**2.加强个人金融信息保护是保障金融消费者合法权益的重要体现。**随着社会进步和经济发展，个人金融信息除了具有人格权属性外，也渐渐体现出财产权属性。保护个人金融信息安全是衡量金融业消费者权益保护水平的重要标尺，是金融业担负的一项重要社会职责，也是依法维护金融消费者权益的重要举措。《网络安全法》《个人信息保护法》《征信业管理条例》等一系列法律法规和规章制度的出台，标志着我国个人金融信息保护立法驶入了快车道。

**3.加强个人金融信息保护是促进数字经济创新发展的现实需要。**金融信息应用是现代金融发展的基础，电子技术是现代金融运行的主要手段。在此背景下，金融企业掌握信息资源的数量以及对信息资源的利用水平，直接关系到自身的行业地位、盈利水平、贡献程度和未来发展。因此，只有加强个人金融信息保护，才能增强客户信心、维护企业良好声誉，保持

市场竞争力，才能为企业持续创新发展奠定坚实基础。

**4.加强个人金融信息保护是防范网络诈骗的重要手段。**网络诈骗案件一般不受时间空间的限制，具有高技术和强隐蔽性，很难发现案件线索和证据，当前主要是以预防为主。因此，加强个人金融信息保护工作，已成为防范和打击金融诈骗案件的重要关口，金融机构有责任和义务采取有效措施加强个人金融信息保护，防止信息泄露。

**个人金融信息保护工作面临的困难**

**1.法规制度仍有短板。**个人信息已成为公民人格权的重要组成部分，对个人权利保护是法律体系核心内容之一。多年来，我国从民事、行政、刑事等各个层面不断完善个人信息保护相关法律法规，2021 年 8 月通过的《个人信息保护法》更是构建了个人信息保护完整框架，为金融机构加强个人金融信息保护、防范打击非法侵害个人金融信息提供了法律基础。但现行的个人金融信息保护法律制度还存在诸多不足，主要表现在可操作性差、分散于不同的制度要求中、对信息主体的权利保护不够充分。

**2.行业监管力度亟待加强。**近年来，央行等金融监管部门陆续下发了《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》《个人金融信息保护技术规范》《个人存款账户实名制管理规定》《个人信用信息基础数据库管理暂行办法》等多份加强个人金融信息保护的通知和规范，但仍有一些金融机构在执行过程存在措施不到位的情况，主要表现在保护领域不全和重管理轻保护两个方面。

**3.金融机构对个人金融信息管理较薄弱。**一是组织机构不健全，缺少管理部门，金融机构一般由多个部门行使个人金融信息保护的权力。未设置专职个人信息保护岗位，导致个人信息保护工作经常陷于无人问津或“打乒乓球”的尴尬境地；二是未建立完整的个人信息使用全过程管理机制，导致难以准确监测和查询个人信息使用的全过程；三是缺乏对外包厂商和人员的管控机制，不能很好的将个人信息保护职责划分清楚并纳入厂商准入标准以及项目合同中，对外包厂商及工作人员进行有效约束。

近年来，金融机构不断通过创新产品、优化服务、探索新型合作等措施，加快信息化进程，推进智能化银行建设。然而个人金融信息保护的理念传导、措施落实还不够到位，个人信息保护缺乏应有的统一管理，信息数据面临外部黑客攻击和病毒感染等诸多风险。

**4.技术管控能力手段不足。**一是个人金融信息关联系统管理较为分散、技术相对落后。部分金融机构个人金融信息的各类管理系统较为零散，管控技术不足，防控手段单一，给个人金融信息保护带来一定困难。二是部分金融机构对敏感数据的使用及相关操作行为缺少系统、充分、高效的监督与审查，缺少自动化数据脱敏机制，给个人金融信息的安全有效传输

使用带来较大风险。三是随着移动通讯技术和互联网应用的快速发展，APP 已成为日常生活中不可的组成部分，但部分金融类 APP 非授权收集信息、超范围收集信息、无隐私协议等现象屡见不鲜，加之非法份子利用病毒、木马和仿冒钓鱼等恶意盗取个人金融信息，故意泄露或非法出售个人信息，使得 APP 成为名副其实的“重灾区”。

**5.消费者自我保护意识淡薄。**在金融和科技融合发展的背景下，加强个人金融信息保护、防范信息泄露和权益侵犯迫在眉睫。金融消费者人数众多，年龄结构和知识水平存在很大差异，对于保护个人金融信息的认知程度也不尽相同，对个人金融信息的重要性、金融信息保护相关细节、个人金融信息等合法权益被侵犯后的解决途径等问题普遍缺乏了解，风险防范意识较为薄弱。

**加强个人金融信息保护的对策建议**

**1.健全个人金融信息保护系统化法规框架。**相关部门应深入贯彻依法治国方略，以《个人信息保护法》为基础，建立健全系统化的个人金融信息保护法规制度，明确金融机构严格按照法律法规的要求收集、保存、使用、销毁个人金融信息，防止信息泄露和滥用。完善金融业个人金融信息管理机制，加强对于保存、使用个人金融信息的组织进行有效监督，发生信息泄露事件要严肃追究法律责任，同时进一步完善相关赔偿制度。

**2.加大个人金融信息保护监管力度。**金融监管部门在做好个人金融信息保护顶层设计的同时，也要加大监管力度，监督各项制度要求的顺利实施。一是提升金融标准指导能力，完善个人金融信息保护监管的标准和规则，切实发挥标准的规范指导作用；二是提升金融业数字化监管能力，建立健全风险防控治理体系，强化数据共享趋势下个人金融信息数据治理，

促进数据资源有效整合和规范利用；三是推进移动金融 APP 备案全覆盖，从提升安全防护、加强个人信息保护、提高风险监测能力、健全投诉处理机制、强化行业自律等方面划定红线、加强监管，提升线上金融服务渠道安全应用水平，保障移动金融领域的数据合法合规使用。

**3.推进金融机构个人金融信息保护规范管理。**金融机构应不断加强个人金融信息保护防御体系建设，规范个人金融信息保护管理。一是规范系统开发流程，将信息安全覆盖系统全生命周期，定期开展渗透测试，提升信息系统防恶意攻击的水平；二是规范个人信息保护风控系统建设，建立覆盖账户安全、网络诈骗、虚假营销、信贷欺诈、非法集资、网络赌博等多种风险模型，通过量化策略实现大批次支付交易日监测功能，在满足消费者对金融服务“线上化、场景化、个性化、体验化”需求的同时，主动实现风险交易止付，为客户安全交易保驾护航；三是加强外包风险管控，从战略、法律、合规等方面进行外包风险识别和控制，规范外包服务内容和责任划分，不断提升自主掌控能力和外包风险管理水平。

**4.加强个人金融信息全生命周期技术管控。**一是加强信息收集管理。通过建设运行信息采集资产管理系统，内置敏感数据发现规则，实现从大量数据库表中自动发现敏感数据，形成数据资产及敏感信息清单，为银行数据资产与敏感数据管理提供技术支撑；二是加强数据脱敏流通。探索部署双节点数据脱敏设备，形成“A 节点数据抽取、脱敏，B 节点数据发放”的模式，在符合物理隔离要求前提下解决银行在生产环境网络与测试环境数据流通问题；三是加强金融 APP 管控。采用高等级 API 和安全 SDK 减少代码的攻击面，对 APP 和服务器进行必要的安全加固，利用加密存储和传输技术保障个人金融信息的安全可靠。

**5.增强消费者自我保护意识。**涉及个人金融信息的侵权事件和犯罪层出不穷,金融消费者作为信息主体更应从增强自我保护意识做起，在日常生活做好以下几点：一是妥善保管身份证、银行卡、网银介质等，不要随意透露身份证号、银行卡号、账户密码、安全码、短信验证码等信息；二是要正确使用支付工具,谨慎点击或扫描不明链接、二维码等；三是发现个人金融信息被非法收集、传播或使用时，及时向金融管理部门或行政执法部门举报投诉，维护自身合法权益。（来源：金融电子化）

# 四、政府之声

## ➢ 央行发布《金融数据安全数据安全评估规范》（征求意见稿）

2021 年 12 月 3 日，全国金融标准化技术委员会网站消息，《金融数据安全数据安全评估规范》（征求意见稿）已发布并公开征求意见。据了解，该标准适用于金融业机构开展金融数据安全评估使用，并为第三方安全评估机构等单位开展金融数据安全检查与评估工作提供参考。


当前金融业机构数据泄露、滥用、篡改等安全威胁的影响已逐步从机构内转移扩大至行业间，甚至影响国家安全、社会秩序、公众利益与金融市场稳定。如何在满足金融业务基本需求的基础上，指导各相关机构规范金融数据安全管理，强化金融行业数据资源保护能力，切实保障金融数据安全流动，已成为当前亟待解决的问题。与此同时，在大数据时代的背景下，数据安全问题层出不穷，而当前金融业机构数据安全管理能力尚处于参差不齐的状态，金融业机构数据安全意识明显落后于快速发展的应用需求及应用技术，金融行业整体数据安全管理仍有待进一步统筹协调。

该标准围绕金融数据安全分级及其生命周期安全要求，主要从金融数据的安全管理评估、安全保护评估、安全运维评估三个方面明确评估内容，并对评估结果的判定原则和判定方式等进行说明，为金融业机构开展数据安全评估工作提供参考。（来源：金融标准化技术委员会）

- **《金融数据安全数据安全评估规范》等 2 项金融行业标准（征求意见稿）全文：**
- https://www.cfstc.org/jinbiaowei/2929444/2982369/index.html

## ➢ 工业和信息化领域数据安全风险信息报送与共享工作指引（试行）征求意见

2021 年 12 月 22 日，为加强工业和信息化领域数据安全风险信息获取、分析、研判和预警工作，及时掌握工业和信息化领域数据安全整体态势，提高数据安全风险处置能力， 工业和信息化部近日研究起草《工业和信息化领域数据安全风险信息报送与共享工作指引(试行)》(以下简称《工作指引》)，并面向社会公开征求意见。

中华人民共和国工业和信息化部
Ministry of Industry and Information Technology of the People's Republic of China

工业和信息化部 | 新闻动态 | 政务公开 | 政务服务 | 公众参与 | 工信数据 | 专题专栏

首页 > 工业和信息化部 > 机关司局 > 网络安全管理局 > 工作动态

公开征求对《工业和信息化领域数据安全风险信息报送与共享工作指引（试行）（征求意见稿）》的意见

发布时间：2021-12-22 16:49　来源：网络安全管理局

为贯彻落实《中华人民共和国数据安全法》等法律法规，加强工业和信息化领域数据安全风险信息获取、分析、研判和预警工作，及时掌握工业和信息化领域数据安全整体态势，提高数据安全风险处置能力，工业和信息化部研究起草了《工业和信息化领域数据安全风险信息报送与共享工作指引（试行）（征求意见稿）》（见附件），拟以规范性文件形式印发，现面向社会公开征求意见。如有意见或建议，请于2022年1月22日前反馈。

传真：010-66069561

邮箱：zhanghong@miit.gov.cn

地址：北京市西城区西长安街13号工业和信息化部网络安全管理局（邮编：100804）。请在信封上注明“《工业和信息化领域数据安全风险信息报送与共享工作指引（试行）（征求意见稿）》意见反馈”。

按照《工作指引》，数据安全风险信息，是指通过检测、评估、信息搜集、授权监测等手段获取的，包括但不限于数据泄露、数据篡改、数据滥用、违规传输、非法访问、流量异常等数据安全风险：一、数据泄露，包括但不限于数据被恶意获取，或者转移、发布至不安全环境等相关风险；二、数据篡改，包括但不限于造成数据破坏的修改、增加、删除等相关风险；三、数据滥用，包括但不限于数据超范围、超用途、超时间使用等相关风险；四、违规传输，包括但不限于数据未按照有关规定擅自进行传输等相关风险；五、非法访问，包括但不限于数据遭未授权访问等相关风险；六、流量异常，包括但不限于数据流量规模异常、流量内容异常等相关风险；七、其他信息，包括由相关政府部门组织授权监测的暴露在互联网上的数据库、大数据平台等数据资产信息，以及有关单位掌握的威胁数据安全的其他风险信息等。

《工作指引》指出，风险信息报送，是指有关单位向工业和信息化部、地方工业和信息化主管部门、地方通信管理局报送数据安全风险信息的行为。风险信息共享，是指经工业和

信息化部、地方工业和信息化主管部门、地方通信管理局审核、授权后，向有关部门、单位告知风险提示的行为。风险信息报送与共享工作坚持“及时、客观、准确、真实、完整”的原则，不得迟报、瞒报、谎报。

同时，工业和信息化部(网安局)鼓励部系统各单位、安全企业、数据处理者、科研院所、行业组织等单位开展风险信息报送，遴选支撑服务能力强、技术水平高、报送信息质量优的单位建立风险直报单位名录，并实施名录动态管理。地方工业和信息化主管部门、地方通信管理局应当组织开展本地区风险报送单位遴选、推荐等工作，建立本地区风险报送单位名录，并加强名录管理。

工业和信息化部(网安局)根据数据安全风险影响范围等情况，分别开展以下风险信息共享和通报工作：一、对于可能影响社会公众的风险信息，可通过部网站等渠道通报；二、对于区域性的风险信息，通报至有关地方工业和信息化主管部门或者地方通信管理局；三、对于能够确定具体通报单位的，同时向该单位主体及其所在地工业和信息化主管部门或者通信管理局通报。（来源：工信部网络安全管理局）

- **《工业和信息化领域数据安全风险信息报送与共享工作指引（试行）》全文：**
- https://www.miit.gov.cn/gzcy/yjzj/art/2021/art_9ed695f19c9f42f882bfdad9ba5ea0e7.html

## ➢ 中央网络安全和信息化委员会印发《“十四五”国家信息化规划》

2021 年 12 月 27 日，中央网络安全和信息化委员会印发《“十四五”国家信息化规划》（以下简称《规划》），对我国“十四五”时期信息化发展作出部署安排。《规划》是“十四五”国家规划体系的重要组成部分，是指导各地区、各部门信息化工作的行动指南。

《规划》指出，“十四五”时期，信息化进入加快数字化发展、建设数字中国的新阶段。加快数字化发展、建设数字中国，是顺应新发展阶段形势变化、抢抓信息革命机遇、构筑国家竞争新优势、加快建成社会主义现代化强国的内在要求，是贯彻新发展理念、推动高质量发展的战略举措，是推动构建新发展格局、建设现代化经济体系的必由之路，是培育新发展动能，激发新发展活力，弥合数字鸿沟，加快推进国家治理体系和治理能力现代化，促进人的全面发展和社会全面进步的必然选择。

《规划》强调，要深入贯彻党的十九大和十九届二中、三中、四中、五中、六中全会精神，坚持以习近平新时代中国特色社会主义思想特别是习近平总书记关于网络强国的重要思

想为指导，紧紧围绕统筹推进“五位一体”总体布局和协调推进“四个全面”战略布局，坚定不移贯彻新发展理念，坚持稳中求进工作总基调，以推动高质量发展为主题，以建设数字中国为总目标，以加快数字化发展为总抓手，发挥信息化对经济社会发展的驱动引领作用，推动新型工业化、信息化、城镇化、农业现代化同步发展，加快建设现代化经济体系；以深化供给侧结构性改革为主线，进一步解放和发展数字生产力，加快构建以国内大循环为主体、国内国际双循环相互促进的新发展格局；以改革创新为根本动力，完善创新体系和发展环境，激发创新活力，增强发展动能；以满足人民日益增长的美好生活需要为根本目的，统筹发展和安全，推进国家治理体系和治理能力现代化，加强数字社会、数字政府、数字民生建设，让人民群众在信息化发展中有更多获得感幸福感安全感，为开启全面建设社会主义现代化国家新征程、向第二个百年奋斗目标进军提供强大动力。


《规划》提出，要坚持党的全面领导，坚持以人民为中心，坚持新发展理念，坚持深化改革开放，坚持系统推进，坚持安全和发展并重。到 2025 年，数字中国建设取得决定性进展，信息化发展水平大幅跃升。数字基础设施体系更加完备，数字技术创新体系基本形成，数字经济发展质量效益达到世界领先水平，数字社会建设稳步推进，数字政府建设水平全面提升，数字民生保障能力显著增强，数字化发展环境日臻完善。

《规划》围绕确定的发展目标，部署了 10 项重大任务，一是建设泛在智联的数字基础设施体系，二是建立高效利用的数据要素资源体系，三是构建释放数字生产力的创新发展体系，四是培育先进安全的数字产业体系，五是构建产业数字化转型发展体系，六是构筑共建

共治共享的数字社会治理体系，七是打造协同高效的数字政府服务体系，八是构建普惠便捷的数字民生保障体系，九是拓展互利共赢的数字领域国际合作体系，十是建立健全规范有序的数字化发展治理体系，并明确了 5G 创新应用工程等 17 项重点工程作为落实任务的重要抓手。

《规划》根据《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》中主要目标和重点内容，把基础能力、战略前沿、民生保障等摆在了优先位置，确定了全民数字素养与技能提升、企业数字能力提升、前沿数字技术突破、数字贸易开放合作、基层智慧治理能力提升、绿色智慧生态文明建设、数字乡村发展、数字普惠金融服务、公共卫生应急数字化建设、智慧养老服务拓展等 10 项优先行动。

《规划》从加强组织领导、健全政策体系、强化队伍建设、规范试点示范、强化战略研究和加强舆论宣传等 6 个方面保障实施，确保目标任务落到实处。（来源：中国网信网）

- **《“十四五”国家信息化规划》**
- **全文：**http://www.cac.gov.cn/2021-12/27/c_1642205314518676.htm

## ➢ 公安部：加强统一领导统筹力量资源深入推进公安网络安全和信息化工作

2021 年 12 月 25 日，公安部网络安全和信息化领导小组会议召开，国务委员、公安部部长、部网络安全和信息化领导小组组长赵克志主持会议并讲话。会议强调，要深入贯彻落实习近平总书记关于网络安全和信息化工作的重要指示精神，增强“四个意识”、坚定“四个自信”、做到“两个维护”，加强统一领导，统筹力量资源，深入推进公安网络安全和信息化工作，更好履行党和人民赋予的新时代职责使命。

会议指出，党的十八大以来，以习近平同志为核心的党中央从发展中国特色社会主义、实现中华民族伟大复兴中国梦的战略高度，系统部署和全面推进网络安全和信息化工作，习近平总书记多次作出重要指示、提出明确要求，为我们做好网络安全工作指明了前进方向、提供了根本遵循。我们要认真学习领会、坚决贯彻落实，切实把思想和行动统一到习近平总书记重要指示精神和党中央决策部署上来，进一步加强和改进公安网络安全和信息化工作。健全部网络安全和信息化领导机构，是加强对公安网络安全和信息化工作统一领导的重要举措，是积极适应形势变化有效应对网络安全风险的迫切需要，是全面提升公安网络安全和信息化工作水平的重要保障。要充分认识健全部网络安全和信息化领导机构的重要意义，统筹

公安网络建设发展和安全保障，统筹公安机关内部资源力量，加强统筹规划和协调指导，全面提升公安网络安全和信息化水平，坚决维护网络空间安全。


中华人民共和国公安部
The Ministry of Public Security of the People's Republic of China

首 页　机构设置　警务信息　办事服务　警民互动　请输入关键字

当前位置：首页 > 警务信息 > 公安要闻 > 正文

公安部网络安全和信息化领导小组会议召开
加强统一领导　统筹力量资源
深入推进公安网络安全和信息化工作

时间：2021年12月26日　字体：大 中 小　分享到：

公安部网络安全和信息化领导小组会议12月25日召开，国务委员、公安部部长、部网络安全和信息化领导小组组长赵克志主持会议并讲话。会议强调，要深入贯彻落实习近平总书记关于网络安全和信息化工作的重要指示精神，增强“四个意识”、坚定“四个自信”、做到“两个维护”，加强统一领导，统筹力量资源，深入推进公安网络安全和信息化工作，更好履行党和人民赋予的新时代职责使命。

会议强调，要以落实党委网络安全责任制为抓手，深入推进公安网络安全和信息化工作。要坚持统筹发展和安全，加强统筹协调，统一谋划、统一部署、统一推进、统一实施公安网络安全和信息化工作，切实下好工作“一盘棋”，着力形成整体工作格局。要紧紧围绕公安“十四五”发展规划，认真研究谋划公安网络安全和信息化基础战略，明确基本要求和主要目标、工作任务和保护措施，切实筑牢公安网络和信息安全屏障。要强化科技创新能力建设，深化公安大数据建设应用，积极推广智慧警务新模式，着力助推公安工作质量变革、效率变革、动力变革。要坚持统筹国内国际两个大局、网上网下两个战场，充分发挥各部门各警种职能作用，整合各种力量资源手段，切实形成维护网上政治安全工作合力。要加强《关键信息基础设施安全保护条例》的宣传解读和贯彻落实工作，进一步增强风险意识、强化底线思维，扎实做好关键信息基础设施安全保护工作，为推动经济社会发展、建设网络强国提供有力安全保障。要切实加强对公安网络安全和信息化工作的统一领导，明确工作任务，细化工作方案，统筹推进各项工作。各成员单位要认真履行工作职责，密切协作配合，确保公安网络安全和信息化各项工作措施落到实处。

公安部党委书记、分管日常工作的副部长、部网络安全和信息化领导小组常务副组长王小洪出席会议并讲话。部党委委员、副部长、部网络安全和信息化领导小组副组长林锐出席会议。领导小组成员单位主要负责同志参加会议。（来源：中华人民共和国公安部）

# 五、本期重要漏洞实例

## ➢ Microsoft 发布 2021 年 12 月安全更新

发布日期：2021-12-14

更新日期：2021-12-14

描述：12 月 14 日，微软发布了 2021 年 12 月份的月度例行安全公告，修复了多款产品存在的 64 个安全漏洞。受影响的产品包括：Windows 11（29 个）、Windows Server 2022（29 个）、Windows 10 21H1（30 个）、Windows 10 20H2 & Windows Server v20H2（30 个）、Windows 10 2004 & Windows Server v2004（30 个）、Windows 8.1 & Server 2012 R2（21 个）、Windows Server 2012（21 个）、Windows RT 8.1（21 个）和 Microsoft Office-related software（6 个）。利用上述漏洞，攻击者可以绕过安全功能限制，获取敏感信息，提升权限，执行远程代码，或发起拒绝服务攻击等。在此，提醒广大 Microsoft 用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

| CVE 编号 | 公告标题 | 最高严重等级和漏洞影响 | 受影响的软件 |
|---|---|---|---|
| CVE-2021-43215 | iSNS 服务器内存损坏漏洞 | 严重<br>远程代码执行 | Windows 11<br>Server 2022<br>Server, version 20H2<br>Server, version 2004<br>Server 2019<br>Windows 10<br>Server 2016<br>Server 2012 R2<br>Server 2012<br>Windows 8.1 |
| CVE-2021-43880 | Windows Mobile Device Management 权限提升漏洞 | 重要<br>特权提升 | Windows 11 |
| CVE-2021-43217 | Windows Encrypting File System (EFS) 远程代码执行漏洞 | 严重<br>远程代码执行 | Windows 11<br>Server 2022<br>Server, version 20H2<br>Server, version 2004<br>Server 2019<br>Windows 10<br>Server 2016<br>Server 2012 R2<br>Server 2012<br>Windows 8.1 |
| CVE-2021-43233 | Remote Desktop Client 远程代码执行漏洞 | 严重<br>远程代码执行 | Windows 11<br>Server 2022<br>Server, version 20H2<br>Server, version 2004<br>Server 2019 |

| | | | |
|---|---|---|---|
| | | | Windows 10<br>Server 2016<br>Server 2012 R2<br>Server 2012<br>Windows 8.1 |
| CVE-2021-43240 | NTFS Set Short Name 提升权限漏洞 | 重要<br>特权提升 | Windows 11<br>Server 2022<br>Server, version 20H2<br>Server, version 2004<br>Windows 10 |
| CVE-2021-41333 | Windows Print Spooler 权限提升漏洞 | 重要<br>特权提升 | Windows 11<br>Server 2022<br>Server, version 20H2<br>Server, version 2004<br>Server 2019<br>Windows 10<br>Server 2016<br>Server 2012 R2<br>Server 2012<br>Windows 8.1 |
| CVE-2021-43883 | Windows Installer 权限提升漏洞 | 重要<br>特权提升 | Windows 11<br>Server 2022<br>Server, version 20H2<br>Server, version 2004<br>Server 2019<br>Windows 10<br>Server 2016<br>Server 2012 R2<br>Server 2012<br>Windows 8.1 |
| CVE-2021-42309 | Microsoft SharePoint Server 远程代码执行漏洞 | 重要<br>远程代码执行 | SharePoint Server Subscription Edition<br>SharePoint Foundation 2013<br>SharePoint Enterprise Server 2016<br>SharePoint Server 2019 |
| CVE-2021-43256 | Microsoft Excel 远程代码执行漏洞 | 重要<br>远程代码执行 | Excel 2016<br>Excel 2013<br>Office Web Apps Server 2013<br>Office Online Server<br>365 Apps Enterprise<br>Office LTSC 2021 |

**来源**：https://msrc.microsoft.com/update-guide/releaseNote/2021-Dec

## ➢ 关于 Apache Log4j2 存在远程代码执行漏洞的安全公告

**发布日期**：2021-12-10
**更新日期**：2021-12-10
**受影响系统**：
漏洞影响的产品版本包括：Apache Log4j2 2.0 - 2.15.0-rc1
**描述**：

---

CNTA-2021-0032
2021 年 12 月 10 日，国家信息安全漏洞共享平台（CNVD）收录了 Apache Log4j2 远程代码执行漏洞（CNVD-2021-95914）。攻击者利用该漏洞，可在未授权的情况下远程执行代码。目前，漏洞利用细节已公开，Apache 官方已发布补丁修复该漏洞。CNVD 建议受影响用户立即更新至最新版本，同时采取防范性措施避免漏洞攻击威胁。
Apache Log4j 是一个基于 Java 的日志记录组件。Apache Log4j2 是 Log4j 的升级版本，通过重写 Log4j 引入了丰富的功能特性。该日志组件被广泛应用于业务系统开发，用以记录程序输入输出日志信息。
2021 年 11 月 24 日，阿里云安全团队向 Apache 官方报告了 Apache Log4j2 远程代码执行漏洞。由于 Log4j2 组件在处理程序日志记录时存在 JNDI 注入缺陷，未经授权的攻击者利用该漏洞，可向目标服务器发送精心构造的恶意数据，触发 Log4j2 组件解析缺陷，实现目标服务器的任意代码执行，获得目标服务器权限。CNVD 对该漏洞的综合评级为“高危”。
**建议**：

---

目前，Apache 官方已发布新版本完成漏洞修复，CNVD 建议用户尽快进行自查，并及时升级至最新版本：https://github.com/apache/logging-log4j2/releases/tag/log4j-2.15.0-rc2

建议同时采用如下临时措施进行漏洞防范：

1）添加 jvm 启动参数-Dlog4j2.formatMsgNoLookups=true；

2）在应用 classpath 下添加 log4j2.component.properties 配置文件，文件内容为 log4j2.formatMsgNoLookups=true；

3）JDK 使用 11.0.1、8u191、7u201、6u211 及以上的高版本；

4）部署使用第三方防火墙产品进行安全防护。建议使用如下相关应用组件构建网站的信息系统运营者进行自查，如 Apache Struts2、Apache Solr、Apache Druid、Apache Flink 等，发现存在漏洞后及时按照上述建议进行处置。

附：参考链接：https://github.com/apache/logging-log4j2/releases/tag/log4j-2.15.0-rc2

## ➢ Google Chrome CORS 策略执行不当漏洞

**发布日期：**2021-11-15
**更新日期：**2021-12-29
**受影响系统：**
Google Google Chrome < 96.0.4664.45
**描述：**

---

CVE(CAN) ID: CVE-2021-38019
Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。
Google Chrome 96.0.4664.45 之前版本的 CORS 组件存在策略执行不当漏洞。攻击者可利用该漏洞通过特制的 HTML 页面泄露跨源数据。
**建议：**

---

厂商补丁：
Google
---
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://chromereleases.googleblog.com/2021/11/stable-channel-update-for-desktop.html

## ➢ Bentley View 越界写入漏洞

**发布日期：**2021-12-07
**更新日期：**2021-12-24
**受影响系统：**
Bentley Systems Bentley Systems Bentley View < 10.16.02
**描述：**

---

CVE(CAN) ID: CVE-2021-34903
Bentley Systems Bentley View 是美国 Bentley Systems 公司的一个免费查看器。
Bentley View 10.16.02 之前版本在解析 BMP 文件时存在越界写入漏洞。攻击者可利用该漏洞执行任意代码。
<*来源：Mat Powell（Trend Micro Zero Day Initiative）
**建议：**

---

厂商补丁：
Bentley Systems
---
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://www.bentley.com/en/common-vulnerability-exposure/BE-2021-0002

# 六、本期网络安全事件

## ➢ 因信息安全等严重违反审慎经营规则，北京银行及 3 人被罚

2021 年 11 月 30 日，上海银保监局的罚单显示，北京银行上海张江支行因“信息安全和员工行为管理严重违反审慎经营规则”，**被罚 50 万元，同时，相关人员被罚警告或禁止从事银行业工作终身**。

| 行政处罚决定书文号 | | | 沪银保监罚决字〔2021〕175号 |
|---|---|---|---|
| 被处罚当事人姓名或名称 | 个人姓名 | | —— |
| | 单位 | 名称 | 北京银行股份有限公司上海张江支行 |
| | | 主要负责人 | 史松才 |
| 主要违法违规事实 | | | 2017年6月至2019年1月，该支行信息安全和员工行为管理严重违反审慎经营规则。 |
| 行政处罚依据 | | | 《中华人民共和国银行业监督管理法》第四十六条第（五）项 |
| 行政处罚决定 | | | 责令改正，并处罚款50万元 |
| 作出处罚决定的机关名称 | | | 中国银行保险监督管理委员会上海监管局 |
| 作出处罚决定的日期 | | | 2021年11月19日 |

| 行政处罚决定书文号 | | | 沪银保监罚决字〔2021〕176号 |
|---|---|---|---|
| 被处罚当事人姓名或名称 | 个人姓名 | | 秦舟波 |
| | 单位 | 名称 | —— |
| | | 主要负责人 | —— |
| 主要违法违规事实 | | | 2017年6月至2019年1月，北京银行上海张江支行信息安全和员工行为管理严重违反审慎经营规则。秦舟波对上述行为负责直接管理责任。 |
| 行政处罚依据 | | | 《中华人民共和国银行业监督管理法》第四十八条第（二）项 |
| 行政处罚决定 | | | 警告 |
| 作出处罚决定的机关名称 | | | 中国银行保险监督管理委员会上海监管局 |
| 作出处罚决定的日期 | | | 2021年11月19日 |

| 行政处罚决定书文号 | | | 沪银保监罚决字〔2021〕178号 |
|---|---|---|---|
| 被处罚当事人姓名或名称 | 个人姓名 | | 丁圣敏 |
| | 单位 | 名称 | —— |
| | | 主要负责人 | —— |
| 主要违法违规事实 | | | 2017年6月至2019年1月，北京银行上海张江支行信息安全和员工行为管理严重违反审慎经营规则。丁圣敏对上述行为负直接责任。 |
| 行政处罚依据 | | | 《中华人民共和国银行业监督管理法》第四十八条第（三）项 |
| 行政处罚决定 | | | 禁止从事银行业工作终身 |
| 作出处罚决定的机关名称 | | | 中国银行保险监督管理委员会上海监管局 |
| 作出处罚决定的日期 | | | 2021年11月19日 |

| 行政处罚决定书文号 | | | 沪银保监罚决字〔2021〕177号 |
|---|---|---|---|
| 被处罚当事人姓名或名称 | 个人姓名 | | 诸佳斌 |
| | 单位 | 名称 | —— |
| | | 主要负责人 | —— |
| 主要违法违规事实 | | | 2017年6月至2019年1月，北京银行上海张江支行信息安全和员工行为管理严重违反审慎经营规则。诸佳斌对上述行为负直接责任。 |
| 行政处罚依据 | | | 《中华人民共和国银行业监督管理法》第四十八条第（三）项 |
| 行政处罚决定 | | | 禁止从事银行业工作终身 |
| 作出处罚决定的机关名称 | | | 中国银行保险监督管理委员会上海监管局 |
| 作出处罚决定的日期 | | | 2021年11月19日 |

**《中华人民共和国银行业监督管理法》第四十六条规定：**银行业金融机构有下列情形之一，由国务院银行业监督管理机构责令改正，并处二十万元以上五十万元以下罚款；情节特别严重或者逾期不改正的，可以责令停业整顿或者吊销其经营许可证；构成犯罪的，依法追究刑事责任：

（一）未经任职资格审查任命董事、高级管理人员的；（二）拒绝或者阻碍非现场监管或者现场检查的；（三）提供虚假的或者隐瞒重要事实的报表、报告等文件、资料的；（四）未按照规定进行信息披露的；（五）严重违反审慎经营规则的；（六）拒绝执行本法第三十七

条规定的措施的。

**《中华人民共和国银行业监督管理法》第四十八条规定：**银行业金融机构违反法律、行政法规以及国家有关银行业监督管理规定的，银行业监督管理机构除依照本法第四十四条至第四十七条规定处罚外，还可以区别不同情形，采取下列措施：

（一）责令银行业金融机构对直接负责的董事、高级管理人员和其他直接责任人员给予纪律处分；（二）银行业金融机构的行为尚不构成犯罪的，对直接负责的董事、高级管理人员和其他直接责任人员给予警告，处五万元以上五十万元以下罚款；（三）取消直接负责的董事、高级管理人员一定期限直至终身的任职资格，禁止直接负责的董事、高级管理人员和其他直接责任人员一定期限直至终身从事银行业工作。

从此次北京银行相关人员的处罚结果看，直接责任人所受处罚比直接管理人更重。同时，值得关注的是，此次对于北京银行上海张江支行及相关员工的处罚，都是针对其 2017 年 6 月至 2019 年 1 月的违规行为。 近几年来，银保监会等监管机构多次对银行较长时间之前的违规行为进行处罚，于银行及从业人员也需要而更加重视业务经营行为的合规性。（来源：互联网综合整理）

## ➢ 2.2 亿会员私密聊天记录随便看 世纪佳缘致歉

2021 年 12 月 7 日，据报道，记者以应聘的形式卧底进入世纪佳缘网线下一家门店。经半个月调查发现，培训上岗后，该门店即为上述记者开通了后台权限，而通过世纪佳缘网后台可以随意查看用户个人信息，包括会员浏览的异性照片记录、聊天记录等。世纪佳缘此举是为了对用户进行“精准营销”。

此外，还有相关人士透露，即使工作人员看到“杀猪盘”套路诈骗，也要无视，避免用户举报公司侵犯个人隐私。另外，调查还发现，世纪佳缘还存在部分销售人员会故意注册成为其他婚恋平台会员或者参加线下相亲活动，以套取客户资源这类恶意竞争行为。

**12 月 7 日晚间在媒体发布调查报道之后世纪佳缘在其官微上致歉**

**世纪佳缘致歉声明称：**为更好的为用户提供更加精准的匹配和介绍，业务层面上向公司部分一线工作人员开放部分用户信息让一线的工作人员(红娘)积极发现用户的问题和实际需求，从而更好的服务用户。但在实际工作中出现了滥用职权查阅用户信息的严重违规行为，公司负有不可推卸的责任。目前公司已经在后台开始去除此功能。致歉声明显示目前世纪佳缘正在进行三项整改：1、报道中提及的门店即日起整改，全员再度深入学习相关法律法规以及公司的规章制度，考核通过后再上岗。2、对调查中发现的相关责任人员按公司规定予以处罚。3、全国各门店全面开展会员信息安全保护的培训和教育工作。（来源：澎湃新闻）

## ➢ 沃尔沃汽车证实服务遭到入侵导致“有限数量”的研发信息被盗

2021 年 12 月 11 日，瑞典汽车制造商沃尔沃(Volvo)刚刚披露，其部分服务器遭到了未知攻击者的入侵，导致部分研发信息被盗。**Volvo 在公告中写道：**“沃尔沃汽车已经意识到某个文件存储库被第三方非法访问”。截至目前的调查证实，该公司“有限数量”的研发资产在黑客入侵期间被盗。参考周五早些时候相关信息得出的结论，该公司的运营可能会受到一定的影响。

事情发生后，沃尔沃汽车公司表示已向有关部门进行了通报，目前正携手第三方专家展开深入调查。参考当前可用的信息，该公司认为本次事件不会对其汽车或个人数据的安全或保障造成影响。

而后 Bleeping Computer 报道称，虽然该公司没有披露更多细节，但 Snatch 勒索软件团伙已经宣布对本次攻击事件负责。

据悉，该勒索软件站点于 11 月 30 日在其数据泄露站点上添加了一个条目，内容涉及侵入 VolvoCars 的服务器并窃取文件。除了附有被盗文件的屏幕截图，该组织还放出了所谓的 35.9MB 文件。本月初，Bleeping Computer 曾试图与 VolvoCars 取得联系，以了解攻击背后的更多细节，但当时该公司未予进一步置评。（来源：易车讯）

## ➢ 菲律宾两大银行遭黑客入侵 部分客户存款被盗

2021 年 12 月 13 日，据菲律宾《世界日报》报道，菲律宾中央银行行长陆诺 12 月 12 日表示，央行正在监控社群媒体用户投诉银行帐户遭黑客入侵事件激增的现象，并与消费者银行合作，以补偿等方法解决问题。陆诺说，央行正和菲律宾最大的银行金融银行(BDO)和友联银行(Unionbank of the Philippines，UBP)合作，采取包括偿还款项在内的补救措施。他在声明中表示：“菲律宾央行将尽一切努力确保金融系统安全、完整，并保护金融消费者。”

上周末，菲律宾社交媒体上突然盛传金融银行一些客户的存款被黑客盗取，有报道称，这些钱被转移到友联银行的一些账户上并用以购买虚拟货币。有部分客户表示，自己开设的 BDO 帐户被黑客犯罪分子入侵，每个帐户窃取 25000 至 50000 不等的金额。初步信息显示，这是网络攻击诈骗的一种形式，账户持有人被骗以验证他们在 BDO 中拥有账户，但被骗资金转移到的账户都是 UnionBank(联合银行)账户。根据受害者的说法，来自 BDO 的现金，未经自己授权的情况下，被转移给骗子的联合银行账户。

许多受害者群体已经浮出水面，他们在脸书上组成了一个受害者声援群组，群组成员们分享了他们对所发生事件的经历。多名受害群组的成员表示，这不是网络钓鱼攻击，成员们保证，他们中的任何人都没有点击消息、短信或电子邮件中的链接，即网络黑客无法通过钓鱼手段获得他们的详细信息，即便如此，自己账户内的金额仍然莫名减少。

群组中的一名受害者 James Sarmiento 是最早报告该事件的受害者之一，他说他在 12 月 9 日凌晨 3 点左右损失了 10 万比索。“总而言之，我们都有未经授权的交易，从我们的 BDO 账户到另一个银行账户——Unionbank 账户，而且还在继续。”在脸书的聊天中，Sarmiento 说：“令人担忧的是，我们非常确定这些是 BDO 方面的安全漏洞，而不是由于我们的疏忽。”

根据众多报案人提供的信息，网络安全专家倾向于认为，这是一次利用某种未知系统漏洞，似乎能够轻松绕过以前被认为是铁一般的安全措施，如 OTP，SMS，发起针对 BDO 的网络安全攻击。

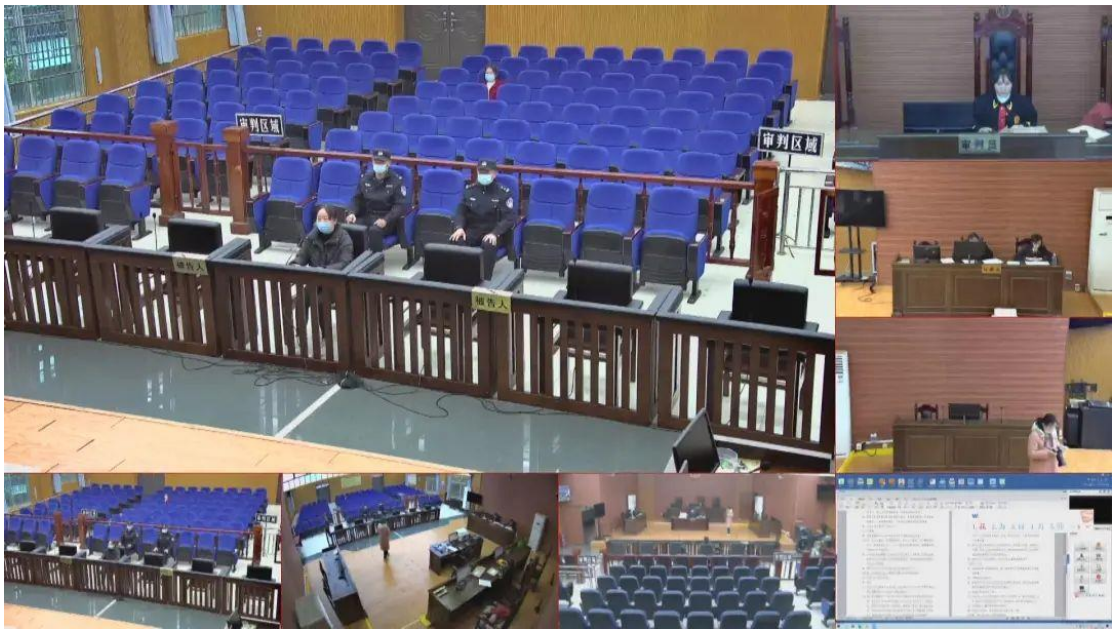
**BDO 在一份声明中表示：**正在调查每个案件并将对受影响的人做出回应，并承诺对于因黑客攻击造成的储户损失，提供赔偿。同时作为紧急预案，已强制所有用户统一更改 BDO 网银的密码，减少因为数据库漏洞产生的攻击风险。

而联合银行总裁埃德温·包蒂斯塔 (Edwin Bautista) 告诉媒体，其客户账户是从 BDO 账户接收资金的银行之一。包蒂斯塔说，有不到 10 个从 BDO 账户接收资金的联合银行账户已经被冻结，并补充说银行正在对允许使用其账户进行犯罪活动的用户，采取法律措施。截止周日晚间发稿为止，两家银行尚未能够估计有多少资金被非法转移及购买数字货币。如何防范潜在的网银使用风险，菲律宾银行家协会敦促菲律宾的网银用户“鉴于我们周围的网络犯罪事件数量不断增加，要更加警惕”。（来源：安全学习那些事儿 ）

## ➢ 通讯营业厅业务员贩卖公民个人信息被判刑 6 个月

2021 年 12 月 20 日，广西富川瑶族自治县人民法院开庭审理了被告人王某某侵犯公民个人信息罪一案。

被告人王某某在富川某营业厅上班，日常负责给客户办理各类通讯业务。2020 年 10 月，被告人王某某经他人介绍加入“淘宝特价注册 7 元秒结”、“淘宝首购 20 下载注册 10 元补贴秒结群”等微信群。2020 年 10 月到 2021 年 7 月，被告人王某某利用其系某移动通讯代理商及员工身份，在给客户办理业务时，未经过客户同意，使用客户手机和号码下载并注册特定渠道的抖音、淘宝、拼多多等手机软件，同时开通客户手机软件地理位置访问权限。注册成功后，被告人王某某将手机型号、手机编号等信息发送至特定微信群或某微信账号，以此方式将公民信息贩卖他人，期间共获利 10423.5 元。2021 年 7 月 6 日，被告人王某某被抓获归案。




在此过程中，许多客户甚至并未意识到自己的个人信息已经被侵犯，他们因为被告人王某某是营业厅的业务员而放松警惕，交由对方用自己的手机操作，在案发后被问起“业务员是否在你的手机上安装了什么软件”，很多人都回答“我不知道”，不知道营业员什么时候安装，营业员也并未告知安装的是什么软件。

富川法院经审理认为，被告人王某某违反国家有关规定，将提供服务过程中获得的公民个人信息出售给他人，情节严重，其行为已触犯《中华人民共和国刑法》第二百五十三条之一第二款的规定，构成侵犯公民个人信息罪。鉴于被告人王某某到案后如实供述犯罪事实且

认罪认罚，有主动退出违法所得并缴纳罚金的悔罪表现，考虑犯罪情节较轻，对其从轻处罚、适用缓刑对所居住社区没有重大不良影响，富川法院依法以侵犯公民个人信息罪，判处被告人王某某有期徒刑六个月，缓刑一年，并处罚金人民币一万元，并对退出违法所得予以没收，上缴国库。

**法官提醒：**随着网络科技的进步，手机已经不再是简单的通讯工具，还存储着通讯、储值、购物等许多重要的个人信息，广大市民在办理业务时，如遇到以上情况，应问明来意，不要轻易将手机交由他人，以免信息泄露，造成不必要的人身财产损失。（来源：法律资讯网）

## ➢ 离职高管利用公司管理漏洞转账上百次，盗走老东家 736 万元

2021 年 12 月 25 日，一名高管离职后，利用公司管理漏洞给自己转账，他摇身一变成了“百万富翁”。日前，浙江宁波警方破获一起盗窃案，这名离职高管蚂蚁搬家式地转账上百次，偷走“老东家”账户内的 736 万元。

今年 7 月，警方接到宁波某电子商务有限公司报案，称 2018 年 2 月至 2020 年 7 月，该公司在某电商平台开设店铺的企业支付宝账户中大量资金被他人盗取。浙江宁波市公安局江北分局洪塘派出所民警汤炳称：报案人怀疑他们公司里面一个员工，我们对于这个线索进行了深入调查，调取了这个人名下一些银行卡的流水，包括支付宝的流水、微信的流水。经过对证据资料进行核查，警方确认该公司前任高管夏某有重大作案嫌疑。


浙江宁波市公安局江北分局洪塘派出所民警汤炳：因为这个嫌疑人的轨迹飘忽不定，这给我们抓捕工作造成了一定的难度。

民警最终在杭州富阳区的一个出租房内将夏某抓获。据夏某交代，他在公司担任高管期间，发现公司**网络店铺绑定的企业支付宝账户存在漏洞，可以利用自己的账户和密码提取账户里的资金**。离职前，夏某尝试提取了几次资金，公司没有发现。离职后，夏某胆子也慢慢大了起来，每当花销不够时，他就登录公司系统进行转账。

浙江宁波市公安局江北分局洪塘派出所民警汤炳：每次金额比较小，每次转个三四万元，然后转了上百余次，最后一共盗走了公司 730 多万元。目前，夏某因涉嫌盗窃罪被公安机关移送起诉。（来源：央视财经）