国盟信息安全通报

2021 年 10 月 31 日第 244 期

全国售后服务中心

国盟信息安全通报

（第 244 期）

国际信息安全学习联盟

2021 年 10 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 402 个，其中高危漏洞 117 个、中危漏洞 231 个、低危漏洞 54 个。漏洞平均分值为 5.63。本周收录的漏洞中，涉及 0day 漏洞 334 个（占 83%），其中互联网上出现“libde265 堆缓冲区溢出漏洞（CNVD-2021-78426）、libde265 堆缓冲区溢出漏洞（CNVD-2021-78427）”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原创漏洞总数 7662 个，与上周（5750 个）环比增加 33%。

主要内容

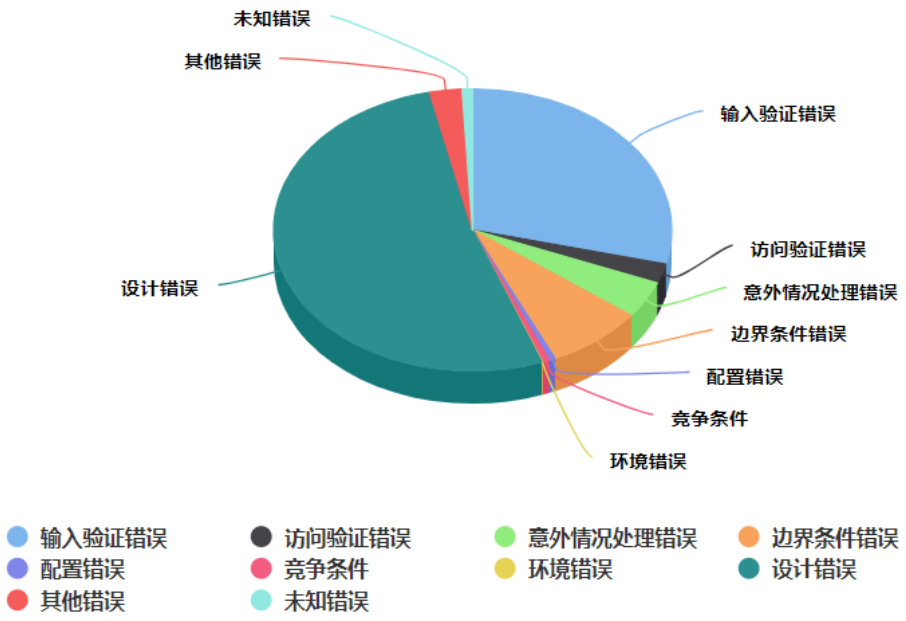
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

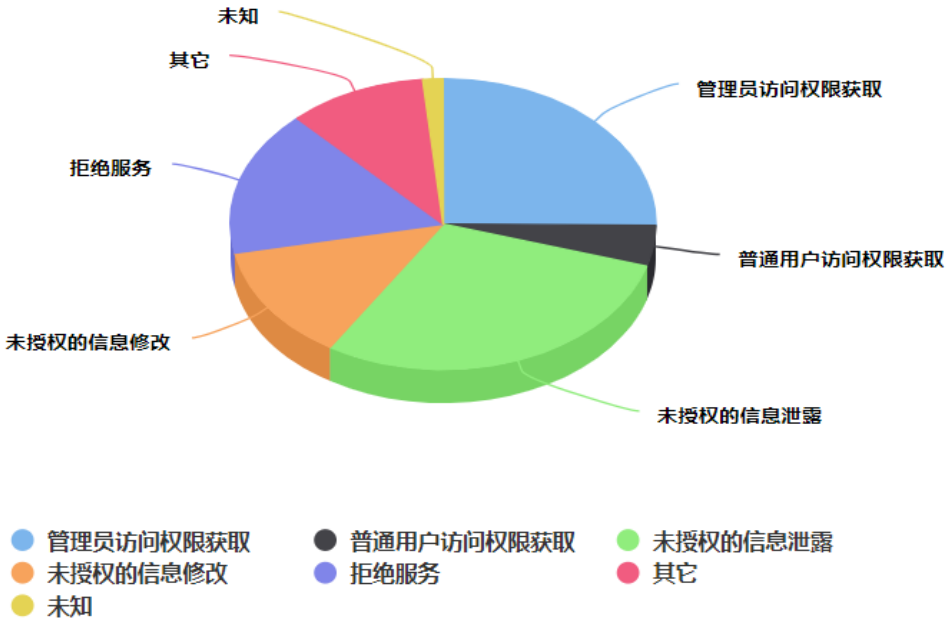
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 402 个，其中高危漏洞 117 个、中危漏洞 231 个、低危漏洞 54 个。漏洞平均分值为 5.63。本周收录的漏洞中，涉及 0day 漏洞 334 个（占 83%），其中互联网上出现“libde265 堆缓冲区溢出漏洞（CNVD-2021-78426）、libde265 堆缓冲区溢出漏洞（CNVD-2021-78427）”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的原创漏洞总数 7662 个，与上周（5750 个）环比增加 33%。

二、安全漏洞增长数量及种类分布情况

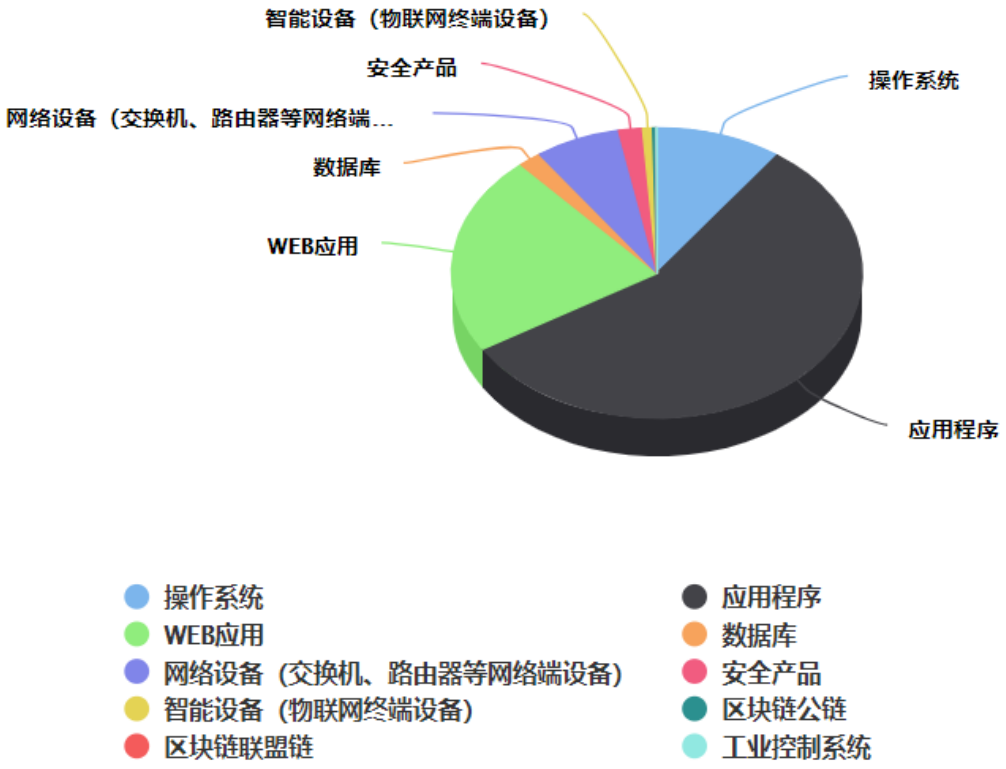
➢ 漏洞产生原因（2021 年 10 月 1 日—2021 年 10 月 31）



➢ 漏洞引发的威胁（2021 年 10 月 1 日—2021 年 10 月 31）



➢ 漏洞影响对象类型（2021 年 10 月 1 日—2021 年 10 月 31）



三、安全产业动态

➢ 把握数字经济发展趋势和规律 推动我国数字经济健康发展

2021 年 10 月 18 日下午，中共中央政治局就推动我国数字经济健康发展进行第三十四次集体学习。中共中央总书记习近平在主持学习时强调，近年来，互联网、大数据、云计算、人工智能、区块链等技术加速创新，日益融入经济社会发展各领域全过程，数字经济发展速度之快、辐射范围之广、影响程度之深前所未有，正在成为重组全球要素资源、重塑全球经济结构、改变全球竞争格局的关键力量。要站在统筹中华民族伟大复兴战略全局和世界百年未有之大变局的高度，统筹国内国际两个大局、发展安全两件大事，充分发挥海量数据和丰富应用场景优势，促进数字技术与实体经济深度融合，赋能传统产业转型升级，催生新产业新业态新模式，不断做强做优做大我国数字经济。

中国科学院院士、南京大学校长吕建教授就这个问题进行讲解，提出了工作建议。中央政治局的同志认真听取了他的讲解，并进行了讨论。

习近平在主持学习时发表了讲话。他指出，党的十八大以来，党中央高度重视发展数字经济，实施网络强国战略和国家大数据战略，拓展网络经济空间，支持基于互联网的各类创新，推动互联网、大数据、人工智能和实体经济深度融合，建设数字中国、智慧社会，推进数字产业化和产业数字化，打造具有国际竞争力的数字产业集群，我国数字经济发展较快、

成就显著。特别是新冠肺炎疫情暴发以来，数字技术、数字经济在支持抗击新冠肺炎疫情、恢复生产生活方面发挥了重要作用。

习近平强调，发展数字经济是把握新一轮科技革命和产业变革新机遇的战略选择。一是数字经济健康发展有利于推动构建新发展格局，数字技术、数字经济可以推动各类资源要素快捷流动、各类市场主体加速融合，帮助市场主体重构组织模式，实现跨界发展，打破时空限制，延伸产业链条，畅通国内外经济循环。二是数字经济健康发展有利于推动建设现代化经济体系，数字经济具有高创新性、强渗透性、广覆盖性，不仅是新的经济增长点，而且是改造提升传统产业的支点，可以成为构建现代化经济体系的重要引擎。三是数字经济健康发展有利于推动构筑国家竞争新优势，当今时代，数字技术、数字经济是世界科技革命和产业变革的先机，是新一轮国际竞争重点领域，我们要抓住先机、抢占未来发展制高点。

习近平指出，要加强关键核心技术攻关，牵住自主创新这个“牛鼻子”，发挥我国社会主义制度优势、新型举国体制优势、超大规模市场优势，提高数字技术基础研发能力，打好关键核心技术攻坚战，尽快实现高水平自立自强，把发展数字经济自主权牢牢掌握在自己手中。

习近平强调，要加快新型基础设施建设，加强战略布局，加快建设高速泛在、天地一体、云网融合、智能敏捷、绿色低碳、安全可控的智能化综合性数字信息基础设施，打通经济社会发展的信息“大动脉”。要全面推进产业化、规模化应用，重点突破关键软件，推动软件产业做大做强，提升关键软件技术创新和供给能力。

习近平指出，要推动数字经济和实体经济融合发展，把握数字化、网络化、智能化方向，推动制造业、服务业、农业等产业数字化，利用互联网新技术对传统产业进行全方位、全链条的改造，提高全要素生产率，发挥数字技术对经济发展的放大、叠加、倍增作用。要推动互联网、大数据、人工智能同产业深度融合，加快培育一批“专精特新”企业和制造业单项冠军企业。要推进重点领域数字产业发展，聚焦战略前沿和制高点领域，立足重大技术突破和重大发展需求，增强产业链关键环节竞争力，完善重点产业供应链体系，加速产品和服务迭代。

习近平强调，要规范数字经济发展，坚持促进发展和监管规范两手抓、两手都要硬，在发展中规范、在规范中发展。要健全市场准入制度、公平竞争审查制度、公平竞争监管制度，建立全方位、多层次、立体化监管体系，实现事前事中事后全链条全领域监管。要纠正和规范发展过程中损害群众利益、妨碍公平竞争的行为和做法，防止平台垄断和资本无序扩张，依法查处垄断和不正当竞争行为。要保护平台从业人员和消费者合法权益。要加强税收监管

和税务稽查。

习近平指出，要完善数字经济治理体系，健全法律法规和政策制度，完善体制机制，提高我国数字经济治理体系和治理能力现代化水平。要完善主管部门、监管机构职责，分工合作、相互配合。要改进提高监管技术和手段，把监管和治理贯穿创新、生产、经营、投资全过程。要明确平台企业主体责任和义务，建设行业自律机制。要开展社会监督、媒体监督、公众监督，形成监督合力。要完善国家安全制度体系。要加强数字经济发展的理论研究，就涉及数字技术和数字经济发展的问题提出对策建议。要积极参与数字经济国际合作，主动参与国际组织数字经济议题谈判，开展双多边数字治理合作，维护和完善多边数字经济治理机制，及时提出中国方案，发出中国声音。

习近平强调，数字经济事关国家发展大局，要做好我国数字经济发展顶层设计和体制机制建设，加强形势研判，抓住机遇，赢得主动。各级领导干部要提高数字经济思维能力和专业素质，增强发展数字经济本领，强化安全意识，推动数字经济更好服务和融入新发展格局。要提高全民全社会数字素养和技能，夯实我国数字经济发展社会基础。（来源：新华社）

➢ 加强网络文明建设 共筑美好精神家园

2021 年 10 月 27 日，中共中央党校《学习时报》在头版头条刊发中共中央宣传部副部长，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：

网络文明是伴随互联网发展而产生的新的文明形态，是现代社会文明进步的重要标志。党的十八大以来，以习近平同志为核心的党中央高度重视网络文明建设，党的十九届五中全会作出了“加强网络文明建设，发展积极健康的网络文化”的重要部署。近日，中共中央办公厅、国务院办公厅印发《关于加强网络文明建设的意见》（以下简称《意见》），进一步明确了网络文明建设的指导思想、工作目标、主要任务、保障措施。我们要切实把思想和行动统一到以习近平同志为核心的党中央决策部署上来，深入学习贯彻《意见》要求，加强网络文明建设，共筑美好精神家园，努力为全面建设社会主义现代化国家、实现第二个百年奋斗目标提供坚强思想保证、强大精神动力、有力舆论支持、良好文化条件。

深入学习贯彻习近平总书记重要讲话精神，充分认识加强网络文明建设的重大意义

习近平总书记站在人类社会进入信息时代的战略高度，多次就加强网络文明建设作出重

要论述、提出明确要求，深刻阐释了新的历史条件下为什么要加强网络文明建设、怎样加强网络文明建设的重大问题，为我们指明了前进方向、提供了根本遵循。我们要认真学习领会，切实增强推进网络文明建设的政治责任感、历史使命感、现实紧迫感。

加强网络文明建设是顺应信息时代潮流、提高社会文明程度的必然要求。习近平总书记指出：“纵观世界文明史，人类先后经历了农业革命、工业革命、信息革命。”当前，信息化、数字化、网络化、智能化发展日新月异，互联网全面融入经济社会发展和人民生产生活，已经成为信息传播的新渠道、经济发展的新引擎、文化繁荣的新载体、社会治理的新平台、国际合作的新纽带。网络文明建设作为社会主义精神文明建设的新兴领域和重要内容，对于提高社会文明程度的意义和作用更加凸显。这就要求我们必须把加强网络文明建设作为一项重要任务，高度重视网络空间的思想引领、价值感召、精神凝聚、文化滋养，努力用科学理论、先进文化、主流价值占领网络阵地，激发广大网民思想共振、情感共鸣、行动共进，推动社会文明程度不断得到新提升。

加强网络文明建设是坚持以人民为中心、满足亿万网民对美好生活向往的迫切需要。习近平总书记多次强调，网信事业发展必须贯彻以人民为中心的发展思想，让亿万人民在共享互联网发展成果上有更多获得感。目前，我国网民规模超过 10 亿，形成了全球最庞大的数字社会，网络空间已经成为亿万民众共同的精神家园。建设一个天朗气清、生态良好的网络空间，是广大网民的共同期待。近年来，网信部门针对群众反映强烈的突出问题，推动出台一系列法律法规，集中开展专项治理行动，网络生态得到明显改善。同时也要清醒地看到，

网络谣言、网络诈骗、网络信息泄露、网络侵犯个人隐私、网络黄赌毒、网络暴力等乱象仍时有发生，直接损害人民群众的合法权益。这就要求我们必须本着对人民负责的态度，把加强网络文明建设作为满足亿万网民对美好生活新期待的重要举措，大力发展积极健康的网络文化，滋养网络空间、净化网络生态，为营造清朗网络空间提供有力支撑。

加强网络文明建设是加快建设网络强国、全面建设社会主义现代化国家的重要任务。习近平总书记指出：“实现中国梦，是物质文明和精神文明均衡发展、相互促进的结果。没有文明的继承和发展，没有文化的弘扬和繁荣，就没有中国梦的实现。”加快建设网络强国，既要有过硬的核心技术、发达的基础设施、繁荣的数字经济、有力的安全保障，也要有丰富的网络服务、优质的网络内容、健康的网络文化、良好的网络生态。这就要求我们必须胸怀两个大局，把加强网络文明建设作为推动网信事业高质量发展、建设网络强国的重要内容，充分发挥网络文明在举旗帜、聚民心、育新人、兴文化、展形象等方面的积极作用，唱响主旋律、传播正能量、弘扬真善美，积极构建网上网下同心圆，不断巩固全党全国人民团结奋斗的共同思想基础，更好凝聚全面建设社会主义现代化国家的磅礴力量。

聚焦网络文明建设重点任务，全面推进文明办网、文明用网、文明上网、文明兴网

“十四五”时期是加强网络文明建设的关键时期。要坚持以习近平新时代中国特色社会主义思想为指导，深入贯彻落实习近平总书记关于网络强国的重要思想和关于精神文明建设的重要论述，聚焦《意见》明确的工作目标和重点任务，坚持正能量是总要求、管得住是硬道理、用得好是真本事，大力弘扬社会主义核心价值观，推动形成适应新时代网络文明建设要求的思想观念、文化风尚、道德追求、行为规范、法治环境、创建机制，实现网上网下文明建设有机融合、互相促进。

筑牢理论武装新阵地。坚持以习近平新时代中国特色社会主义思想统领互联网内容建设，牢牢把握正确的政治方向、舆论导向、价值取向，发挥网络传播优势，推动理想信念教育常态化制度化，让党的创新理论通过互联网“飞入寻常百姓家”。加快推进各类理论资源数字化、网络化、智能化传播和应用，推动大众化理论传播，打造内容鲜活、形式新颖的理论产品。创新开展网上正面宣传，加强网络传播手段建设和创新，不断提高新闻舆论传播力、引导力、影响力、公信力。围绕做大做强网络阵地，推动媒体融合向纵深发展，建好主流媒体移动传播平台，管好用好商业化、社会化互联网平台，形成网络正能量传播合力。

培育网络文化新风尚。把社会主义核心价值观体现到互联网信息服务和网络文化产品生产全过程，增强广大网民特别是青少年网民对社会主义核心价值观的认同感。加强党史、新中国史、改革开放史、社会主义发展史网上宣传，传播我们党在革命、建设、改革各个历

史时期取得的伟大成就，旗帜鲜明反对历史虚无主义等错误倾向。加强中华优秀传统文化丰富内涵和时代价值的网上宣传阐释，积极推动优秀传统文化和当代文化精品的数字化、网络化传播。丰富优质网络文化产品供给，引导创作积极健康、向上向善的网络文学、网络表演、网络影视剧、网络音视频、网络动漫、网络游戏等文化产品。加强互联网新技术创新运用，提高网络公共文化服务供给的普惠性和便捷性。

拓展道德建设新空间。着眼加强社会公德、职业道德、家庭美德、个人品德教育，广泛开展劳动模范、时代楷模、道德模范、最美人物、身边好人、优秀志愿者等典型案例和事迹网上宣传活动。弘扬网络诚信文化，不断健全完善网络诚信建设的体制机制、法规制度、渠道载体，努力构建人人参与、多元共治的网络诚信建设工作新格局。坚持以人为本、科技向善，深入实施网络公益工程，运用互联网广泛传播公益理念、善行义举、爱心榜样，广泛开展网络文明志愿服务和网络公益活动，深化拓展“互联网+公益”新模式，推动形成崇德向善、见贤思齐的网络文明环境。

构建网络行为新秩序。以完善网络文明规范为依托，在各类文明创建工作中鼓励制定出台有针对性的网络文明准则。以提升青少年网络素养为重点，引导青少年网民形成良好的安全意识、健康的用网习惯、必备的防护技能，采取有效手段防范青少年沉迷网络，坚决打击和制止网络欺凌。以压实平台主体责任为抓手，督促网站平台完善内部管理制度，加强平台社区规则、用户协议建设，健全内容审核机制，提高网络内容从业人员政治素质和业务能力。以强化互联网行业自律为基础，坚持经济效益和社会效益相统一，充分发挥行业组织引导督促作用，通过完善行业公约、开展社会评议等方式，广泛凝聚社会共识和行业力量。

营造综合治理新生态。加快建立健全网络综合治理体系，统筹推进系统治理、依法治理、综合治理、源头治理。广泛开展网络文明宣传活动，大力强化网络文明意识，引导广大网民积极投身网络文明建设。进一步规范网上内容生产、信息发布和传播流程，深入推进公众账号分级分类管理，加强中国互联网联合辟谣平台建设，健全全国网络辟谣联动机制。深入推进“清朗”“净网”系列专项行动，加大对网络暴力、“饭圈”乱象等网络不文明行为的整治力度，动员广大网民积极参与监督。加快制定修订相关法律法规，加强网络执法统筹协调，创新网络普法方式，增强公民法律意识和法治素养。

打造文明创建新品牌。有力推进群众性精神文明创建活动向网上延伸，加强网民网络文明素养实践教育基地建设，推动基层深入开展网络文明建设活动。精心组织实施网络文明品牌活动，积极打造中国网络文明理念宣介平台、经验交流平台、成果展示平台和国际网络文明互鉴平台。深入实施中国正能量“五个一百”网络精品征集评选展播工程、争做中国好网

民工程，持续打造“网络中国节”品牌，积极推进“阳光跟帖”行动，引导全社会提升网络文明素养、净化网络环境。

加强党对网络文明建设工作的领导，凝聚共建共享的强大合力

网络文明建设是一项涉及面广、综合性强的系统工程，要坚持党的集中统一领导，统筹谋划、全面部署、一体推进，充分发挥各地区各部门的积极性主动性创造性，广泛调动社会各界力量，共同建设网上美好精神家园。

强化组织领导，完善工作机制。各地区各部门要认真落实《意见》要求，把网络文明建设摆上重要议事日程，纳入全局工作谋划推进，加快建立党委统一领导、党政齐抓共管、有关部门各负其责、全社会积极参与的领导体制和工作机制。对于《意见》明确的网络文明建设各项工作任务，要坚持项目化推进，细化分解任务，扎实推进重大任务、重点工程有效开展，及时总结推广成功经验和创新做法，确保工作取得实效。

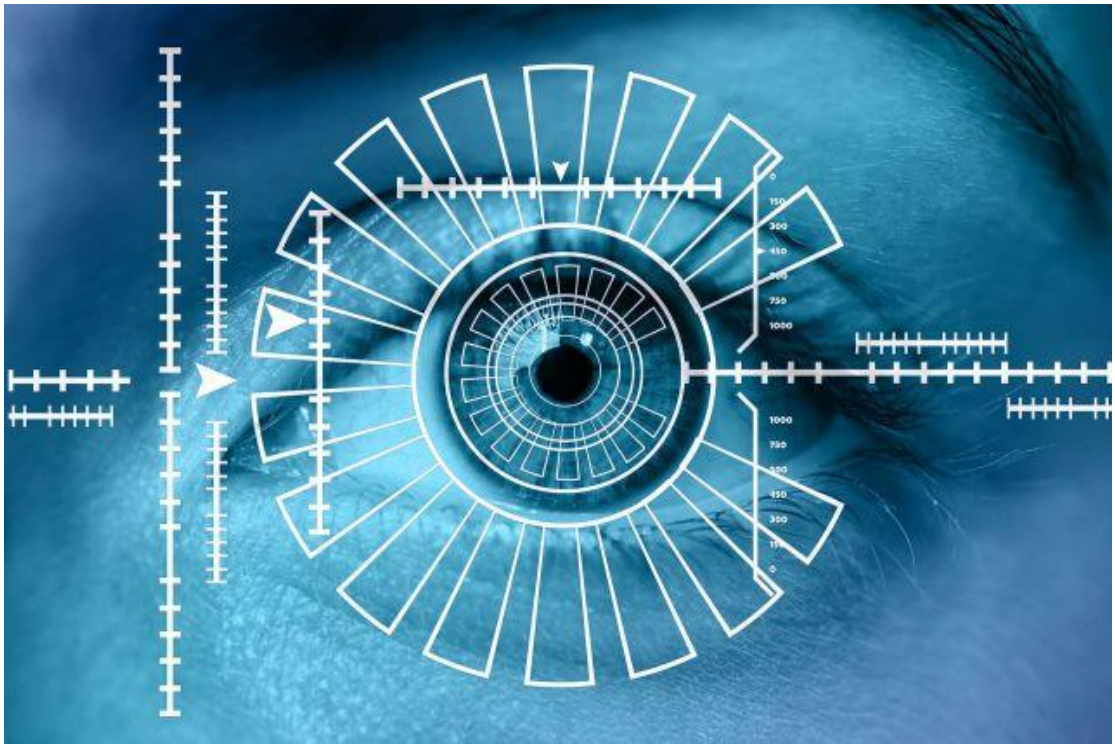
强化统筹协调，提升工作效能。各级网信办要与本级文明办密切配合，共同发挥好牵头抓总作用，同时充分发挥各有关部门的职能作用，加强对网络文明建设的组织指导和协调服务，做到定位明确、分工合理、优势互补、协同高效。要走好走实网上群众路线，通过互联网面对面、键对键、心贴心地宣传群众、引导群众、服务群众，吸引广大网民特别是青少年网民主动参与网络文明建设，构建起各方共建、成果共享的网络文明建设新格局。

强化支撑保障，夯实工作基础。进一步完善网络文明建设有关制度规定，确保政策的科学性、精准性、有效性。加大政策、项目等扶持力度，鼓励社会力量对网络文明建设提供财力物力支持。加强对工作规律的研究和把握，不断推动网络文明建设的内容形式、方法手段、渠道载体等创新，切实增强网络文明建设的针对性有效性和吸引力感染力。（来源:《学习时报》2021 年 10 月 27 日第 1 版）

➢ 密码，让百姓生活更安全

密码技术是保障网络与信息安全的核心技术和基础支撑，通过加密保护和安全认证两大核心功能，可以完整实现防假冒、防泄密、防篡改、抗抵赖等安全需求，在网络空间中扮演着“信使”“卫士”和“基因”的重要角色。信息化、网络化、数字化高度发达的今天，密码技术已经渗透到了社会生产生活各个方面，重要网络和信息系统、关键信息基础设施、数字化平台都离不开密码的保护。5G、物联网、云计算、大数据、人工智能、区块链、量子通

信、数字经济等新技术新业态都与密码紧密融合。密码与老百姓日常生活也息息相关，身份认证、消费支付、网络交易、个人信息保护、财产保护等，背后都有密码在发挥着作用，密码的应用可谓无处不在，有力维护了社会正常运转和交易秩序，保障了公民、法人和社会组织的合法权益。



——保障在线支付安全。网上支付、手机支付等在线支付方式已成为老百姓日常消费支付的主要方式。各大支付平台都使用密码技术实现用户身份认证、交易数据验签等功能，确保支付数据的机密性和完整性，保护用户资金等敏感信息不被盗用、输入的交易资料不被篡改，防止业务损失或服务中断，为保护消费者资金安全，防止欺诈、套现、洗钱等违法犯罪行为发挥了重要作用。

——助力“互联网+政务服务”。公积金管理部门利用密码技术，为个人办理公积金业务提供在线身份核实认证、各类申请表电子签名，实现公积金网办大厅全程电子化，查询、提取、贷款等业务全部线上办理，为存缴单位和职工提供优质、便捷、高效的服务。电子营业执照和电子印章利用密码技术，支持市场主体身份全国范围内的在线验证和识别，降低市场主体办事成本。自 2021 年 1 月起，北京市新开办企业可在获得电子营业执照的同时免费获得一套电子印章。

——服务居民医疗健康数据管理。卫生信息系统利用密码技术，实现各级卫生行政部门和各级各类医疗卫生机构及其工作人员的统一身份认证，有效满足了居民医疗健康数据的完整性保护、可信时间及责任认定等安全需求，在防止假冒身份、篡改信息、越权操作、否认

责任等方面发挥了重要作用。特别是在抗疫斗争中，通过采用密码技术，国家疾控数据直报、“防疫健康码”等实现了传输不中断、信息不泄露、数据无篡改，可靠电子签名及安全电子病历在医疗系统大量应用，为政府、社区、单位联防联控、复工复产提供了有力支撑。

——支撑智能电表安全快捷。智能电表采用商用密码对电力用户进行身份鉴别，对用电关键数据进行签名、加密，保障用电信息采集、用电控制、用户电力缴费等业务的顺利开展和安全可靠运行。目前，智能电表已经遍及千家万户，老百姓使用手机就可以查询电量、缴纳电费。方便快捷的背后，离不开密码技术的保护和支持。智能电表的广泛应用，在便利了群众日常生活的同时，对支持阶梯电价政策、推动节能减排也发挥了重要作用。

——便利高校毕业生就业升学。北京大学、清华大学等高校利用密码技术，将电子成绩单等传统纸质证明材料电子化，加盖基于密码技术的可靠电子签名及可信时间戳实现信息防伪，达成电子成绩单等证明材料互信互认，验证时间从之前的三周缩短至“秒级”，极大便利了广大毕业生办理就业、升学等业务。

密码赋能高质量发展，密码护航百姓生活。2019 年 10 月 26 日《中华人民共和国密码法》颁布以来，密码应用保障领域全面拓宽，产业生态持续繁荣壮大，科技创新成果显著，社会公众密码安全意识进一步增强，密码在维护国家安全、促进经济社会发展、保护人民群众利益中的作用日益凸显。

——密码应用保障领域全面拓宽。在公安、社保、交通、能源、水利、教育、广电、税务等领域，密码应用不断向纵深拓展，充分发挥了在保障国家网络与信息安全中的核心重要作用。银行卡、网上银行、移动支付、条码支付及非银行支付等各类电子支付中的密码应用不断深化。采用密码的身份证件、社会保障卡、应急广播、数字电视、不停车收费（ETC）系统、交通一卡通、增值税发票系统等实现规模化部署，密码在一大批国家和地方政务网络系统中得到广泛应用。

——密码产业生态持续繁荣壮大。密码从业单位数量和规模不断增大，密码应用与创新发展示范基地、行业密码应用研究中心和产业园区建设蓬勃开展。密码检测认证体系不断健全，为推动密码科学化规范化管理，促进密码产业健康有序发展提供了坚实支撑。市场监管总局与国家密码管理局联合发布一系列规范性文件，进一步明确商用密码检测认证工作原则、工作机制和实施要求。组织开展商用密码应用安全性评估试点，推进评估标准、技术、机构、人才支撑体系建设。全国电子认证服务机构签发的数字证书，广泛应用于金融、税务、教育、电信、电子商务以及电子政务等领域，产生了重大的社会效益和经济效益。

——密码学术交流和人才培养加速推进。密码学术交流繁荣发展，中国密码学会聚焦密

码技术新成果和新方向，搭建产学研交流平台，举办国际密码学术会议，发布《中国密码学发展报告》。2021 年 3 月，教育部正式将“密码科学与技术”列入新增普通高等学校本科专业目录，7 所高校从今年秋季开始招收密码本科生；“密码技术应用”专业已纳入职业教育专业目录。人力资源社会保障部会同市场监管总局、国家统计局发布新职业信息，将“密码技术应用员”确定为新职业。上述举措为有效满足社会密码人才应用需求，提升密码科技创新实力提供了坚实的人才支撑。

——社会公众密码安全意识进一步增强。各级密码管理部门深入贯彻《中华人民共和国密码法》要求，落实密码安全主体责任，健全完善密码安全管理工作机制，提高密码安全风险防范能力和水平。今年“4·15”全民国家安全教育日期间，国家密码管理局以“统筹发展和安全，筑牢维护国家安全的密码防线”为主题，在全国范围内组织开展密码安全宣传教育活动，各地区各部门精心准备、踊跃参与，有力提升了全社会的密码安全意识。

做好新时代的密码工作，事关人民切身利益。各级密码管理部门将深入践行“密码安全为人民”的理念，全面推进《中华人民共和国密码法》的贯彻实施，积极促进密码与数字经济、数字政府、数字社会的融合应用，不断筑牢密码安全防线，让百姓的生活更安全、更便捷，努力提升人民群众在网络空间的获得感、幸福感、安全感！（来源：人民日报）

➢ 共同筑牢网络安全防线——党的十八大以来网络安全发展成就综述

2021 年 10 月 11 日至 17 日，以“网络安全为人民，网络安全靠人民”为主题的 2021 年国家网络安全宣传周将在全国范围内统一举办，大力营造全社会共筑网络安全防线的浓厚氛围。

习近平总书记指出，没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。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，特别是关于网络安全工作“四个坚持”重要指示指引下，我国网络安全工作进入快车道，国家网络安全保障体系日益完善，网络安全防护能力显著提升，网络安全工作取得瞩目成就，广大人民群众在网络空间收获了满满的获得感、幸福感、安全感。

依法治网，确保互联网在法治轨道上健康运行

2021 年 8 月 20 日，十三届全国人大常委会第三十次会议表决通过《中华人民共和国个人信息保护法》。这部和人们数字生活息息相关的法律，回应了一系列社会关注的热点问题，

为进一步筑牢网络安全之基提供了强大法治保障。

网络空间不是“法外之地”。党的十八大以来，网络安全顶层设计和总体布局不断强化，网络安全“四梁八柱”基本确立。如今，从个人信息保护到关键信息基础设施安全保护，从网络安全审查到大数据安全管理，一批涵盖网络安全各个领域的重要制度相继建立并不断完善。

——法治思维贯穿网络安全工作的始终。近年来，从网络安全法、数据安全法、个人信息保护法等重要法律的人大立法，到《国家网络空间安全战略》《关键信息基础设施安全保护条例》等战略规划、法律法规的制定出台，再到《网络安全审查办法》《云计算服务安全评估办法》《汽车数据安全管理若干规定（试行）》等部门规章和规范性文件的发布实施，网络安全法律法规体系基本建立。

——网络安全国家标准体系日益完善。截至目前，制定发布 322 项国家标准，共有 12 项包含我国技术贡献和提案的国际标准发布。如今，相关标准在指导和规范网络安全工作、提升国际竞争力等方面的作用显著提升。

——网络安全应急能力建设不断加强。国家网络安全应急体系不断健全，与《国家网络安全事件应急预案》有效衔接，金融、能源、通信、交通等行业领域制修订本行业领域网络安全应急预案，安全防护体系不断完善，应急响应处置能力持续提升。

——健全网络安全审查制度。组织开展对关键信息基础设施采购网络产品和服务活动的网络安全审查，对滴滴、运满满、货车帮、BOSS 直聘等启动网络安全审查，有效防范采购活动、数据处理活动以及国外上市可能带来的国家安全风险。

——健全云计算服务安全评估制度。组织对面向党政机关和关键信息基础设施服务的云平台开展安全评估，加强云计算服务安全管理，防范云计算服务安全风险。截至目前，已有 56 家云平台通过云计算服务安全评估，同时对已通过评估的云平台开展持续监督。

依法管网、依法办网、依法上网，确保互联网在法治轨道上健康运行，如今我国互联网治理能力的法治化、科学化水平不断提升，网络安全治理格局日渐完善，网络安全防线不断筑牢。

网络安全为人民、网络安全靠人民

习近平总书记强调，国家网络安全工作要坚持网络安全为人民、网络安全靠人民。

互联网通达亿万群众，连接党心民心，网信事业发展必须坚持以人民为中心的发展思想，始终把实现好、维护好、发展好广大人民群众在网络空间的合法权益，作为网络安全工作的出发点和落脚点。

非法利用摄像头偷窥个人隐私画面、交易隐私视频、传授偷窥偷拍技术等侵害公民个人隐私的行为，人民群众深恶痛绝。今年 5 月以来，摄像头偷窥等黑产集中治理工作深入推进，截至 8 月，查获非法控制的网络摄像头使用权限 2.5 万余个，收缴窃听窃照器材 1500 余套，清理相关违规有害信息 2.2 万余条，下架违规产品 1600 余件，对存在隐私视频信息泄露隐患的 14 家视频监控 APP 厂商进行了约谈。

利用手机卡开卡环节恶意注册、出售网络账号的违法犯罪活动，往往成为下游电信网络诈骗、网络赌博等的源头。对此，今年以来“净网 2021”专项行动重拳出击，截至 9 月，共抓获违法犯罪人员 1.6 万余名，对其中 6700 余人采取刑事强制措施。2019 年以来，相关部门围绕网络黑产中的黑卡（手机卡、物联网卡）、黑号开展重点打击，网上黑卡数量连续两年降幅超 50%。

强制授权、过度索权、超范围收集个人信息……在小小手机 APP 上，大量存在的违法违规收集使用个人信息问题的危害不可小觑。2019 年以来，APP 违法违规收集使用个人信息专项治理在全国范围内开展，对问题较为严重的 APP 进行了公开曝光，APP 运营者履行个人信息保护责任义务的能力和水平明显提升。……

党的十八大以来，针对网络安全领域特别是数据安全、个人信息保护、新技术新应用风险防范等各界关注、百姓关切的热点问题，相关部门切实回应焦点、打通堵点、解决难点，有力地维护了国家网络安全和人民群众合法权益。

维护网络安全也是全社会共同的责任。在如今的网络安全宣传教育过程中，网上宣传的理念、内容、形式、方法、手段等不断创新。自 2014 年举办首届国家网络安全宣传周以来，

各地区各部门多措并举、扎实推进，以百姓通俗易懂、喜闻乐见的形式，宣传网络安全理念、普及网络安全知识、推广网络安全技能，广泛开展网络安全进社区、进农村、进企业、进机关、进校园、进军营、进家庭等活动，有力推动了全社会网络安全意识和防护技能的提升，在全国范围内形成了共同维护网络安全的良好氛围。

筑牢数字安全屏障，让数字文明造福各国人民

当今世界正经历百年未有之大变局，新一轮科技革命和产业变革方兴未艾。随着大数据、人工智能、物联网、下一代通信网络等新技术新应用快速发展，我国网络安全技术产业发展日新月异、网络安全保障能力不断增强，同时也积极推进全球互联网治理体系变革，为筑牢数字安全屏障，让数字文明造福各国人民，作出中国贡献、体现大国担当。

网络空间的竞争，归根结底是人才竞争。习近平总书记指出，要坚持网络安全教育、技术、产业融合发展，形成人才培养、技术创新、产业发展的良性生态。

近年来网络安全学科建设和人才培养明显加快。2016 年 6 月，中央网信办、发改委、教育部等 6 部门联合印发《关于加强网络安全学科建设和人才培养的意见》，推动开展网络安全学科专业和院系建设，创新网络安全人才培养机制。中央网信办、教育部实施了一流网络安全学院建设示范项目，西安电子科技大学、北京航空航天大学等 11 所高校入选。

与之相应，网络安全技术产业快速发展，每年以 20%以上速度增长，产业增速全球领先。《中国网络安全产业白皮书（2020 年）》显示，2019 年我国网络安全产业规模达到 1563.59 亿元。如今，通过建设国家网络安全人才与创新基地，开展国家网络安全教育技术产业融合发展试验区建设，网络安全人才培养、技术创新、产业发展的良性生态正在加速形成。

网络安全是全球性挑战，没有哪个国家能够置身事外、独善其身，维护网络安全是国际社会的共同责任。

不久前，浙江乌镇再聚世界目光——来自全球 96 个国家和地区的 2000 多名嘉宾采用“线上+线下”相结合的方式共聚 2021 年世界互联网大会乌镇峰会。自 2014 年起，世界互联网大会已连续成功举办 8 届，习近平总书记关于全球互联网发展治理的“四项原则”“五点主张”“四个共同”赢得国际社会广泛赞同，网络空间命运共同体理念深入人心。

强化互联网国际治理和网络安全国际交流合作，推动建立多边、民主、透明的国际互联网治理体系。从《网络空间国际合作战略》的发布，到《全球数据安全倡议》的提出，今天的中国，不仅为推进全球网络安全治理体系变革提供“中国方案”，更以实际行动为构建网络空间命运共同体贡献中国力量，让互联网发展成果更好造福世界各国人民。（来源：人民日报）

四、政府之声

➢ 工信部公布《工业和信息化领域数据安全管理办法(试行)(征求意见稿)》

2021 年 9 月 30 日，工信部网站发布公开征求对《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》的意见。

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

访客预约 | RSS订阅
统一搜索
看新闻 找文件 查办事 提意见 查数据 要投诉

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管理办法（试行）（征求意见稿）》的意见

发布时间：2021-09-30 16:41 来源：网络安全管理局

为贯彻落实《数据安全法》等法律法规，加快推动工业和信息化领域数据安全管理工作制度化、规范化，提升工业、电信行业数据安全保护能力，防范数据安全风险，工业和信息化部研究起草了《工业和信息化领域数据安全管理办法（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2021年10月30日前反馈。

传真：010-66069561

邮箱：suntao@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管理办法（试行）（征求意见稿）》意见反馈”。

附件：1. 工业和信息化领域数据安全管理办法（试行）（征求意见稿）.pdf

征求意见稿提出，工业和信息化部建立工业和信息化领域重要数据和核心数据备案管理制度，统筹建设备案管理平台。备案内容包括数据的数量、类别、处理目的和方式、使用范围、主体责任、安全保护措施等基本情况，数据提供、公开、出境、承接，以及数据安全风险、事件处置等情况。

地方工业和信息化主管部门、通信管理局应当分别对本地区工业、电信行业重要数据和核心数据备案内容进行审核，对不符合有关备案要求的，应当督促企业及时完善并重新进行备案。此外，工业和电信数据处理者应当按照有关要求进行备案，备案内容发生变化的，应在三个月内报备变更情况，同时对整体备案情况进行更新。（来源：工业和信息化部）

- **《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》全文：**
- https://www.miit.gov.cn/jgsj/waj/gzdt/art/2021/art_d4793a2b8f664a6e91773243541b864f.html

➢ 人民银行中国银保监会发布《系统重要性银行附加监管规定（试行）》

2021 年 10 月 15 日，为完善我国系统重要性银行监管框架，明确系统重要性银行附加监管要求，央行会同银保监会制定了《系统重要性银行附加监管规定(试行)》(以下简称《附加监管规定》)正式发布。

《附加监管规定》共五章二十二条，包括总则、附加监管要求、恢复与处置计划、审慎监管和附则。作为去年底发布的《系统重要性银行评估办法》的补充，《附加监管规定》为实施系统重要性银行附加监管提供指导和依据。

对于规定出台的背景，人民银行、银保监会有关部门负责人答记者问时表示，从夯实我国银行体系健康发展基础的角度，需进一步完善系统重要性银行监管的基础性政策框架，要求系统重要性银行在落实各项微观审慎监管要求的基础上，满足更高的监管标准，提高其抗风险能力。与此同时，我国系统重要性银行名单发布，具体包括 6 家国有商业银行、9 家股份制商业银行和 4 家城市商业银行，共计 19 家银行。（来源：人民银行）

- **（系统重要性银行附加监管规定（试行）**
- **全文：**http://www.pbc.gov.cn/tiaofasi/144941/144957/4361118/index.html

➢ 国家网信办部署推进“清朗·互联网用户账号运营乱象专项整治行动”

2021 年 10 月 18 日，为切实解决账号运营存在的突出问题，国家互联网信息办公室召开“清朗·互联网用户账号运营乱象专项整治行动”全国视频工作会议，对相关工作进行专题部署。中央网信办副主任、国家网信办副主任盛荣华出席并讲话。

会议指出，今年以来，网信系统认真贯彻落实习近平总书记关于网络强国的重要思想，针对社会各界高度关注、人民群众反映强烈的突出问题，开展“清朗”系列专项整治，着力解决影响网络空间清朗生态的顽症痼疾，取得积极成效。账号运营乱象专项整治行动是“清朗”系列专项整治的重要内容，将坚持问题导向和效果导向，对即时通讯、新闻资讯、论坛社区、网络直播、知识问答、生活服务、电子商务、网络视频、网络游戏等各类网站平台账号乱象进行集中整治。

会议强调，专项整治行动要紧盯五类账号运营乱象：一是违法违规账号“转世”。加强账号注册管理，严禁已被依法依约关闭的账号以相同名称、相似名称等关联名称重新注册，对于已被关闭的账号主体，根据违法违规程度设置一定的禁止重新注册期限。二是互联网用户账号名称信息违法违规。坚决处置名称、昵称、头像、简介和封面等包含违法违规信息的账号，假冒仿冒党政军机关、企事业单位、新闻媒体等组织机构名称、标识以假乱真误导公众的账号，不具备经济、教育、医疗卫生、司法等领域专业资质仍从事专业领域信息内容生产的账号。三是网络名人账号虚假粉丝。严格管控网络名人账号异常涨粉行为，全面清理“僵尸”粉、机器粉，大力打击通过雇佣水军等方式的非自然涨粉行为，定期清理“僵尸”账号。

四是互联网用户账号恶意营销。从严处置利用社会时事“蹭热点”、发布“标题党”文章煽动网民情绪的账号；传播低俗、庸俗、媚俗内容的直播、主播账号；炒作明星八卦等泛娱乐化信息，引发网民互相攻击的账号；以知识传播名义歪曲解读国家政策，干扰公众认知的账号；“带节奏”操控评论，干扰真实舆论呈现的水军账号。五是向未成年人租售网络游戏账号。严格网络游戏账号实名注册和登记要求，清理向未成年人提供网络游戏账号的租售交易。此外，因机构调整等原因无法注销的政务号也将予以集中处置。

会议要求，专项整治行动要强化统筹协调，通过进一步加强账号注册、使用和管理全流程动态监管，督促网站平台严格落实主体责任，引导账号主体规范账号运营行为，营造清朗网络空间。（来源：中国网信网）

➢ 《中华人民共和国反电信网络诈骗法（草案）》发布

2021 年 10 月 19 日，十三届全国人大常委会第三十一次会议听取了全国人大常委会法工委副主任李宁所作的关于反电信网络诈骗法草案的说明。近年来，电信网络诈骗犯罪活动形势严峻，在刑事犯罪案件中占据很大比重。犯罪分子利用新型电信网络技术手段，钻管理上的漏洞，利用非法获取个人信息、网络黑灰产业交易等实施精准诈骗，组织化、链条化运作，跨境跨地域实施，严重危害人民群众获得感、幸福感、安全感。电信网络诈骗犯罪已经成为当前发案最高、损失最大、群众反映最强烈的突出犯罪，多发高发态势难以有效遏制，需要进一步完善制度，坚决打击治理，维护人民群众切身利益。

李宁介绍，制定专门法律是反电信网络诈骗工作实践的迫切需要。从实践情况看，反电信网络诈骗工作综合治理、源头治理方面的制度措施不够充分，金融、通信、互联网等行业治理存在薄弱环节，需要进一步建立完善各方面责任制度，形成协同打击治理合力；实践中一些好的做法和政策文件需要上升为法律规定；现有法律规定总体上较为分散，不够明确，针对性不强，各方面对于加强法律制度建设的需求较为迫切。李宁表示，制定反电信网络诈骗法统筹发展和安全，坚持精准防治和问题导向，强化系统观念、注重源头治理、综合治理，加强预防性法律制度建设，为打击遏制电信网络诈骗活动提供法治支撑。

草案共 39 条，分为 7 章，主要涵盖 6 方面内容：

一是反电信网络诈骗工作的基本原则。强调坚持系统观念，注重源头治理、综合治理，全面落实打防管控各项措施；规定各部门职责、企业职责和地方政府职责；加强协同联动工作机制建设。

二是完善电话卡、物联网卡、金融账户、互联网账号有关基础管理制度。落实实名制，规定电话卡、互联网服务真实信息登记制度，建立健全金融业务尽职调查制度；对办理电话卡、金融账户的数量和异常办卡、开户情形进行限制，防范开立企业账户风险；有针对性地完善物联网卡销售、使用监测制度。

三是支持研发电信网络诈骗反制技术措施，统筹推进跨行业、企业统一监测系统建设，为利用大数据反诈提供制度支持。规定金融、通信、互联网行业主管部门统筹推进相关跨行业、企业的统一监测系统建设，推进涉诈样本信息数据共享；要求互联网企业移送监测发现的嫌疑线索。

四是加强对涉诈相关非法服务、设备、产业的治理。治理改号电话、虚假主叫和涉诈非法设备；加强涉诈 APP、互联网域名监测治理；打击治理涉电信网络诈骗相关产业。

五是其他措施方面，建立涉案资金紧急止付、快速冻结和资金返还制度；防范个人信息被用于电信网络诈骗；有针对性加强宣传教育；对潜在受害人预警劝阻和开展被害人救助；加强治理跨境电信网络诈骗活动，规定特定风险防范措施和国际合作。

六是明确法律责任，加大惩处力度。加大惩处非法买卖、出租、出借电话卡、物联网卡、金融账户、互联网账号行为，实施惩戒措施；对违反本法规定依法追究刑事责任以及实施、帮助实施电信网络诈骗活动的法律责任作出衔接性规定。（来源：人民日报）

- **《中华人民共和国反电信网络诈骗法（草案）》全文：**
- http://www.npc.gov.cn/flcaw/userIndex.html?lid=ff8081817ca2554e017ca63b3a2f0a05

五、本期重要漏洞实例

➢ Microsoft 发布 2021 年 10 月安全更新

发布日期：2021-10-12

更新日期：2021-10-12

描述：10 月 12 日，微软发布了 2021 年 10 月份的月度例行安全公告，修复了多款产品存在的 77 个安全漏洞。受影响的产品包括：Windows 11（39 个）、Windows Server 2022（43 个）、Windows 10 21H1（41 个）、Windows 10 20H2 & Windows Server v20H2（44 个）、Windows 10 2004 & Windows Server v2004（44 个）、Windows 8.1 & Server 2012 R2（28 个）、Windows Server 2012（28 个）、Windows RT 8.1（27 个）和 Microsoft Office-related software（12 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-2021-36970	**Windows Print Spooler 欺骗漏洞**	重要 欺骗	Server, version 20H2 Server, version 2004 Server 2019 Windows 10 Windows 11 Server 2016 Server 2012 R2 Server 2012 Windows 8.1 Server 2022
CVE-2021-40449	**Win32k 权限提升漏洞**	重要 特权提升	Windows 11 Server 2022 Server, version 20H2 Server, version 2004 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2021-40469	**Windows DNS Server 远程代码执行漏洞**	重要 远程代码执行	Server 2022 Server, version 20H2 Server, version 2004 Server 2019 Server 2016 Server 2012 R2 Server 2012

CVE-2021-40461	**Windows Hyper-V 远程代码执行漏洞**	严重 远程代码执行	Windows 11 Server 2022 Server, version 20H2 Windows 10 Server, version 2004 Server 2019
CVE-2021-41340	**Windows Graphics Component 远程代码执行漏洞**	重要 远程代码执行	Windows 11 Server 2022 Server, version 20H2 Server, version 2004 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2021-40487	**Microsoft SharePoint Server 远程代码执行漏洞**	重要 远程代码执行	SharePoint Foundation 2013 SharePoint Server 2019 SharePoint Enterprise Server 2016
CVE-2021-40486	**Microsoft Word 远程代码执行漏洞**	严重 远程代码执行	Word 2016 Office Online Server Word 2013 Office Web Apps Server 2013 SharePoint Enterprise Server 2013 SharePoint Enterprise Server 2016 Office 2019 SharePoint Server 2019
CVE-2021-40485	**Microsoft Excel 远程代码执行漏洞**	重要 远程代码执行	Office LTSC 2021 Office LTSC for Mac 2021 Excel 2013 Excel 2016 365 Apps Enterprise Office 2019 SharePoint Enterprise Server 2013 Office Online Server Office 2019 for Mac
CVE-2021-40480	**Microsoft Office Visio 远程代码执行漏洞**	重要 远程代码执行	Office LTSC 2021 365 Apps Enterprise Office 2019

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

➢ IBM Sterling File Gateway 任意文件上传漏洞

发布日期：2021-10-19
受影响系统：
IBM Sterling File Gateway >=2.2.0.0，<=5.2.6.5_4
IBM Sterling File Gateway >=6.0.0.0，<=6.0.0.6
IBM Sterling File Gateway >=6.0.1.0，<=6.0.3.4
IBM Sterling File Gateway >=6.1.0.0，<=6.1.0.2
描述：

CVE(CAN) ID: CVE-2021-20584
IBM Sterling File Gateway 是一款用于在内部和外部合作伙伴之间传输文件的应用程序，可让您更加安全可靠地与贸易伙伴进行文件传输。
IBM Sterling File Gateway 2.2.0.0-5.2.6.5_4、6.0.0.0-6.0.0.6、6.0.1.0-6.0.3.4、6.1.0.0-6.1.0.2 版存在任意文件上传漏洞。该漏洞源于访问控制不当。远程攻击者可利用该漏洞上传任意文件。
建议：

厂商补丁：
IBM
厂商已发布了漏洞修复程序，请及时关注更新：
https://www.ibm.com/support/pages/node/6496751

➢ 多款 Cisco 产品拒绝服务漏洞

发布日期：2021-10-06
更新日期：2021-10-27
受影响系统：
Cisco TelePresence Collaboration Endpoint (CE) Software < 10.7.2
Cisco RoomOS Software < 10.7.1.2
描述：

CVE(CAN) ID: CVE-2021-34758
Cisco RoomOS Software 和 Cisco TelePresence Collaboration Endpoint Software 都是美国思科（Cisco）公司的产品。Cisco RoomOS Software 是一套用于 Cisco 设备的自动管理软件。该软件主要用于升级、管理 Cisco 设备的主板固件。Cisco TelePresence Collaboration Endpoint Software 是一套协作终端软件。
Cisco RoomOS Software 10.7.1.2 之前版本和 Cisco TelePresence Collaboration Endpoint Software 10.7.2 之前版本存在拒绝服务漏洞。该漏洞源于程序未对共享内存资源访问进行有效控制。攻击者可利用该漏洞破坏共享内存段并导致设备重新加载。
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tpce-rmos-mem-dos-rck
*>

建议：

厂商补丁：

Cisco

Cisco 已经为此发布了一个安全公告（cisco-sa-tpce-rmos-mem-dos-rck56tT）以及相应补丁：cisco-sa-tpce-rmos-mem-dos-rck56tT：Cisco TelePresence Collaboration Endpoint and RoomOS Software Denial of Service Vulnerability

链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tpce-rmos-mem-dos-rck56tT

➢ Mozilla Firefox 安全限制绕过漏洞

发布日期：2021-09-07

更新日期：2021-10-25

受影响系统：

Mozilla Firefox 92.0-1

描述：

CVE(CAN) ID: CVE-2021-38491

Mozilla Firefox 是美国 Mozilla 基金会的一款开源 Web 浏览器。

Mozilla Firefox 92.0-1 存在安全限制绕过漏洞。该漏洞源于 Mixed-Content-Blocking 未对不透明的来源进行检查。攻击者可利用该漏洞加载不透明来源的混合内容。

建议：

厂商补丁：

Mozilla

目前厂商已经发布了升级补丁以修复这个安全问题，详情请关注厂商主页：

https://www.mozilla.org/en-US/security/advisories/mfsa2021-38/

六、本期网络安全事件

➢ Facebook 史上最严重宕机 全网宕机近七小时市值蒸发千亿

2021 年 10 月 4 日早上 9 点，社交平台 Facebook 及旗下两大社交媒体 Instagram 和 WhatsApp 的网站和 App 出现集体宕机，波及社交服务的多个国家发生中断故障，直接影响用户达 15 亿。此外，在服务器宕机之后，Facebook 的运营和技术团队用了长达 7 个小时才将设备恢复，触发了全球用户的持续“不爽”和质疑。

而让大家更想不到的是，这次宕机除了波及社交业务的服务器，甚至连 Facebook 的企业端和内部服务也被曝出了全线崩溃，内部处理类似问题的员工之间也无法交流。在此次宕机事件发生几个小时之后，**Facebook 官方转而只能通过 Twitter(58.39, -3.59, -5.79%)官方账户发表正式声明：**“世界各地的一些人在访问 Facebook 应用程序时遇到了问题。我们正在努力尽快恢复正常，我们对给用户造成的不便，表示抱歉。”

据报道，监测网络状况的网站 DownDetector.com 显示，除了 Facebook 以外，Messenger、Instagram 和 WhatsApp 等 Facebook 旗下应用均出现故障，全球其他一些网站也出现网页宕机。受此消息影响，Facebook 股价一度跌至 5.9%，收跌 4.9%，创 6 月 3 日以来的四个月最低，市值一夜蒸发 643 亿美元（约合人民币 4147 亿元），目前总市值约 9000 亿美元。此次宕机影响了约 8500 万用户，为 Facebook 自 2008 年以来最严重的一次。对此，Facebook 官

方通过 Twitter 发表声明，承认产品出现故障，表示正在致力解决问题，尽快恢复服务。

值得注意的是，外媒报道，在宕机的近 7 个小时当中，据称有超过 15 亿 Facebook 用户的数据在黑客论坛上被出售。对于这一说法，Facebook 辟谣称，没有证据表明用户数据因宕机而被泄露。这次宕机的根本原因是错误的配置更改。（来源：互联网综合整理）

➢ 两程序员制作销售证券软件外挂 可侵入 84 家证券公司交易系统

2021 年 10 月 8 日，由中国检察网获悉，两名程序员因销售“通达信”API 接口被抓。起诉书显示，该 API 接口名为“TradeX”，可侵入由财富趋势承建、维护的 84 家证券公司交易系统。自 2017 年 3 月 29 日起，两名程序员通过销售通达信平台的 API 接口并提供后续服务，共发展客户 1240 名，收取销售服务费超 902 万元，共计非法获利超 583 万元。

据悉，通达信为国内知名证券行情软件，由财富趋势设计开发。公开信息显示，财富趋势于 2020 年 4 月 27 日在科创板上市，主营业务为面向证券公司等金融机构客户提供安全、稳定、可靠的金融软件解决方案,为其建设投资者行情交易终端、终端用户信息系统以及客户服务系统等，同时为终端投资者客户提供专业、高效的证券信息服务。

上海市普陀区人民检察院在起诉书中表示：经依法审查查明，2017 年 3 月至 2020 年 12 月，两名程序员宋某 1、宋某 2 为牟取非法利益，由宋某 1 负责对深圳**科技股份有限公司(以下简称“财富趋势”)为证券公司开发的“通达信”软件客户端中的通讯、控制模块进行

脱壳、篡改，剥离其中静态防御措施后，使用其自行开发的外挂主程序接管控制与通讯模块，重新搭建对外接口，使其得以调用“通达信”软件客户端通讯模块功能，后再通过镜像欺骗以及篡改等手段破坏动态反外挂模组，并将上述程序代码封装成可以通过证券公司交易系统安全检测的“TradeX”交易接口，侵入由财富趋势承建、维护的 84 家证券公司交易系统。

并由宋某 2 负责编写接口使用说明、开通接口授权文件及绑定证券账户，通过互联网对外向上海*甲科技有限公司(以下简称“上海**公司)及个人出售“TradeX”交易接口。经司法鉴定，“TradeX”具备自动化登陆证券账号、查询证券账号信息、证券账号持仓数据、进行证券交易的功能。经司法审计鉴定，宋某 1、宋某 2 通过销售通达信平台的 API 接口并提供后续服务，共发展客户 1240 名，收取销售服务费人民币 902 万余元。

截至目前，宋某 1 和宋某 2 共计非法获利 583 万余元，其中宋某 1 获利 411 万余元，宋某 2 获利 171 万余元。2020 年 12 月 30 日，二人分别被公安机关抓获，到案后均如实供述自己的罪行。

基于以上事实，上海市普陀区人民检察院认为，宋某 1、宋某 2 对外出售“Trade X”交易接口牟利，情节特别严重，已触犯刑法，应当以提供侵入计算机信息系统程序罪追究其刑事责任。但考虑到二人自愿认罪认罚、如实供述自己的罪行，可从宽处理、从轻处罚。且宋某 1 起主要作用，系主犯，宋某 2 起次要作用，系从犯，根据相关法律规定，应当对宋某 2 从轻或减轻处罚。最终，上海市普陀区人民检察院提起公诉，建议对宋某 1 判处有期徒刑四年，并处罚金;对宋某 2 判处有期徒刑二年六个月，并处罚金。（来源：和讯网）

➢ 每条 1000 美元！团伙非法获取 54 亿条公民个人信息

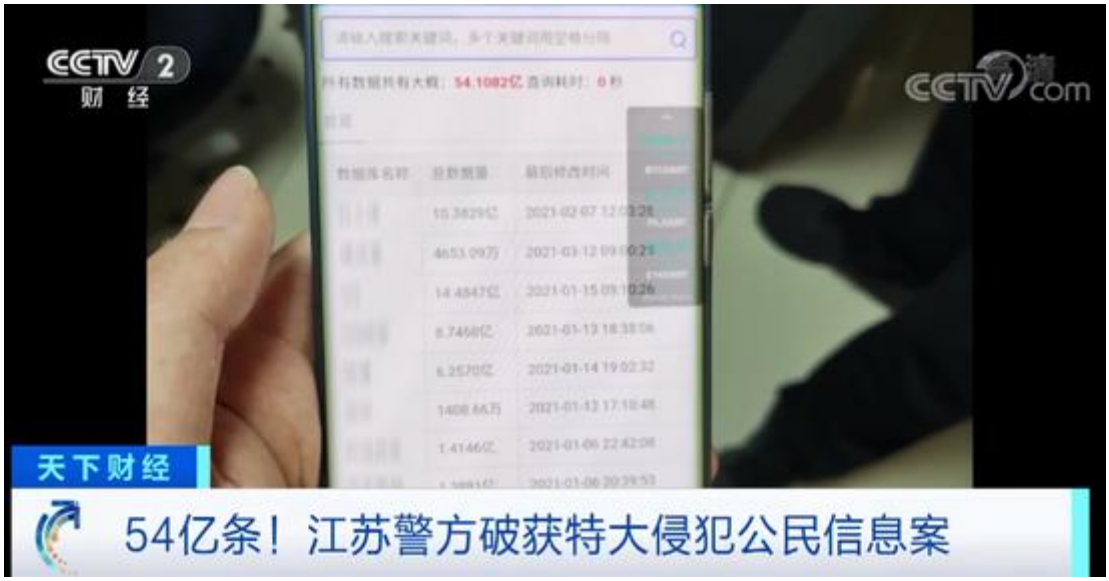
2021 年 10 月 22 日，近日，无锡警方成功破获了一起侵犯公民个人信息案，犯罪团伙非法获取医疗、出行、快递等公民信息，数据累计高达 54 亿多条，并通过"暗网"平台提供查询、出售服务。

今年 3 月，无锡锡山网安大队在网上巡查时发现，一名暗网卖家在暗网平台上为他人查询某大型社交网络平台账号关联的手机号码、个人信息等数据，并将查询信息以每条 1000 美元的价格出售。

无锡市锡山公安分局网安大队民警陆朋：我们对这个线索进行追踪，通过侦查，发现在贵州遵义，有一家网络公司可能与该案有关。我们深入侦查发现，该网络公司的法人何某，

他是具有一定的黑客技术的人员，深入侦查发现，他自己组建了一个社工库。

所谓"社工库"，就是黑客们将泄露的用户数据整合分析，然后集中归档的一个地方。办案民警告诉记者，何某本身对网络技术比较精通，他通过搭建具备查询功能的数据库，将数据库接口接入其公司开发的自用软件系统内，从而在暗网平台上为他人提供非法查询公民个人信息服务并以此获利。



无锡市锡山公安分局网安大队民警陆朋：他的信息来源一部分是他自己购买，还有一部分通过他的一些工作便利，比如他为贵州某医院搭建挂号 APP 的时候，通过数据直接导出功能，获取医院的就诊信息，还有通过给某机场搭建系统时，就导出一些航班信息。

经过缜密侦查，无锡警方于近日成功抓获涉嫌侵犯公民个人信息、非法获取计算机信息系统数据的何某、熊某等人，现场查扣涉案服务器 6 台、电脑 2 台，以及非法获取的各类公民个人信息 54 亿余条。目前，该案正在进一步处理中。**江苏无锡市公安局锡山分局网安大队民警陆朋：**它的信息，迄今为止应该是国内我们查获的，最大单体量的一个公民个人信息社工库。（来源：央视财经）

➢ Tesco 网站遭黑客攻击 使成千上万的顾客无法在线购买商品

2021 年 10 月 25 日，据英国《卫报》报道，Tesco 网站日前遭到黑客攻击，导致成千上万沮丧的购物者无法在英国最大的超市在线购买商品。这次故障使其食品杂货网站和应用程序连续第二天瘫痪，人们无法预订送货或修改现有订单。乐购每周收到 130 万份在线订单。

Tesco 的一位发言人说：“从昨天开始，我们的在线食品杂货网站和应用程序遇到了干扰。有人试图干扰我们的系统，这导致了网站搜索功能的问题。我们正在努力全面恢复所有服务，并对造成的不便表示歉意。”这名发言人补充说：“没有理由相信这个问题会影响到客户的数据，我们将继续采取持续行动，确保所有数据保持安全。”

Tesco 曾在 2014 年遭黑客攻击，当时在网上发布了 2000 多个包括密码在内的登录信息后，它被迫停用了在线客户账户。两年后，对 Tesco 财务部门的一次单独攻击导致 250 万英镑的损失。网络攻击已经变得越来越普遍，许多公司和其他组织已经成为全球的目标。今年夏天，世界上最大的巴西肉类加工企业 JBS 遭到网络攻击，迫使其在美国、澳大利亚和加拿大暂时停止生产。

购物者在社交媒体上表达了他们的挫败感。一些人发布了他们从超市收到的信息，告诉他们由于"当前的 IT 问题"，Tesco 目前无法访问或更改任何订单。**竞争对手 Asda 超市周六在 Twitter 上说：**你们好，希望我们能提供帮助。我们有空位，有些是当天或明天的，如果你去我们的网站或应用程序，它将允许你为你需要的物品下订单)。（来源：cnBeta ）

➢ 侵犯公民个人信息！浙江一行长遭禁业五年

2021 年 10 月 22 日，中国银行保险监督管理委员会官网公布的一则行政处罚决定书公告送达书透露，沈静冲时任中国建设银行余姚城建支行行长，侵犯公民个人信息案件的作案

当事人，对侵犯公民个人信息案件负有直接责任。

宁波银保监局表示：上述事实，有浙江省余姚市人民法院刑事判决书、中国建设银行宁波市分行案件信息确认报告、宁波银保监局案件调查事实确认书、行政处罚案件调查笔录等证据证明。 该公告显示，作为侵犯公民个人信息案件当事人，上述行为已触犯《中华人民共和国刑法》第二百五十三条的规定，违反了《银行业金融机构从业人员职业操守指引》（银监发〔2011〕6 号）第五条、第七条的规定，属于严重违反审慎经营规则的行为。

根据《中华人民共和国银行业监督管理法》第四十八条第（三）项规定，宁波银保监局决定对沈静冲予以**禁止从事银行业工作五年**的行政处罚。

宁波银保监局指出，如不服本行政处罚决定，可以在收到本处罚决定书之日起六十日内向中国银行保险监督管理委员会申请行政复议，也可以在收到本处罚决定书之日起六个月内向有管辖权的人民法院提起诉讼。复议、诉讼期间本决定不停止执行。

相关法律条文：《银行业金融机构从业人员职业操守指引》（银监发〔2011〕6 号）

第五条 从业人员应当具备岗位任职资格或能力，熟练掌握业务技能，自觉遵守行业自律制度和本单位规章制度，合规操作；对已发生的违法违规行为或尚未发生但存在潜在风险隐患的行为，应当按照相关报告制度规定，及时报告。

第七条 从业人员应当尊重客户，了解客户需求，依法保护客户权益和客户信息。从业人员应当对客户如实详细提示产品的特点和风险，切实保护客户权益；不得采取隐瞒或误导等不正当手段，损害客户权益。从业人员应当执行首问负责制，诚待客户，语言文明，举止大方，提供优质服务。从业人员不得因国籍、地区、肤色、民族、性别、年龄、宗教信仰、健康情况或其他因素等差异而歧视客户。

《中华人民共和国银行业监督管理法》

第四十八条　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。（来源：浙江在线）

➢ 韩国大面积断网韩国电信公司道歉：网络路径设置错误

2021 年 10 月 25 日，占据韩国网络市场半壁江山的电信运营商——韩国电信（KT）的有线、无线互联网服务从 25 日上午 11 时 20 分许出现约 1 小时 25 分钟的中断，在韩国各地引发混乱。

这次断网给韩国大量企业和个人造成极大困扰。据《韩国先驱报》（The Korea Herald）25 日报道，KT 的有线和无线互联网服务在 25 日上午 11 点左右突然中断，韩国 KT 用户无

法上网，打不了电话。证券公司的电子交易系统、医疗机构结算系统无法使用，韩国门户网站、商铺支付系统、企业业务系统等基于 KT 互联网的各项服务均出现瘫痪，即时通讯、视频会议、游戏和线上课程均受影响。韩国《中央日报》称，支付管理系统通常在宽带局域网（LAN）上运行。根据市场追踪机构 Smart Choice 的数据，KT 在韩国宽带互联网领域的市场份额最大，为 41.3%。

据报道，KT 曾在事故发生后发布公告称，公司网络当天上午 11 时许遭到大规模分布式拒绝服务攻击（DDoS），但两小时后又称本次网络瘫痪是因设置错误所致。

KT 在最新公告中表示：由于流量超负荷，起初推测遭受分布式拒绝服务攻击，但经缜密调查，发现该事故因设备更换过程中出现的设置错误所致，将与韩国政府一道进一步查明具体原因。报道称，KT 在事发后立即开展修复工作，大部分服务已于当天（25 日）中午起恢复正常，部分地区的修复工作出现延误。

韩国电信于 1981 年 12 月成立，1982 年 1 月 1 日正式运营。1991 年之前，韩国电信曾是韩国国内唯一的地方、国内长途及国际长途业务的供应商。上世纪 90 年代初，韩国政府在电信业引入市场竞争。在政策影响下，韩国有 3 家地方电信供应商，5 家国内长途业务供应商，以及多家国际长途业务供应商。韩国通信市场曾经历整合，KT 在 2009 年兼并当时韩国第二大移动运营商 KTF。目前，韩国拥有 3 家移动通信供应商，分别是 SK 电讯、韩国电信和 LG U+。（来源：综合整理）