国盟信息安全通报

2021 年 09 月 30 日第 243 期

全国售后服务中心

国盟信息安全通报

（第 243 期）

国际信息安全学习联盟

2021 年 9 月 30 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 420 个，其中高危漏洞 128 个、中危漏洞 253 个、低危漏洞 39 个。漏洞平均分值为 5.79。本周收录的漏洞中，涉及 0day 漏洞 314 个（占 75%），其中互联网上出现“WordPress Modern Events Calendar 远程代码执行漏洞、ToaruOS 权限提升漏洞”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原创漏洞总数 4843 个，与上周（5176 个）环比减少 6%。

主要内容

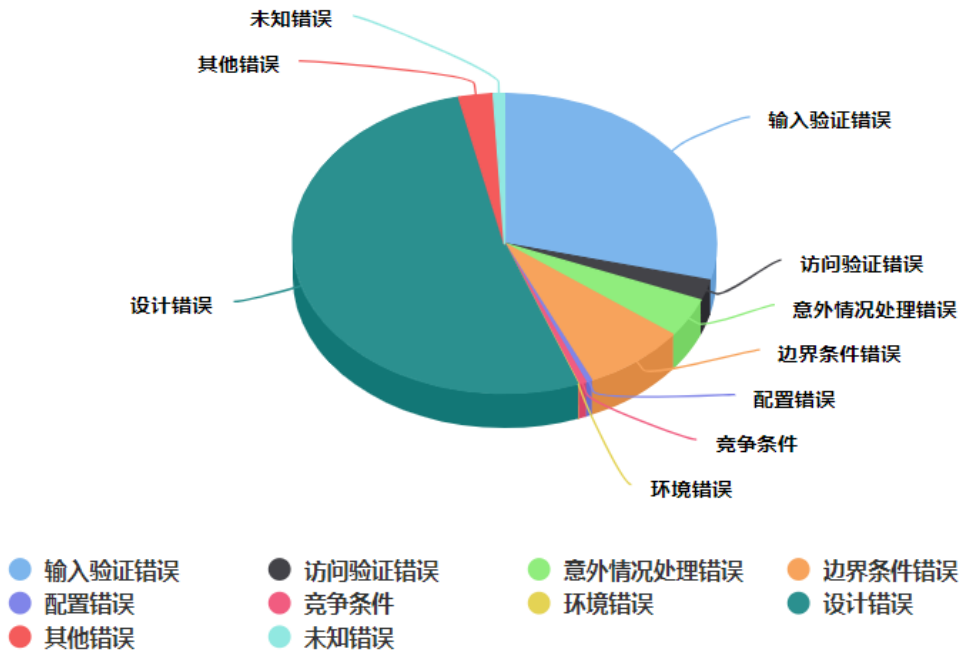
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

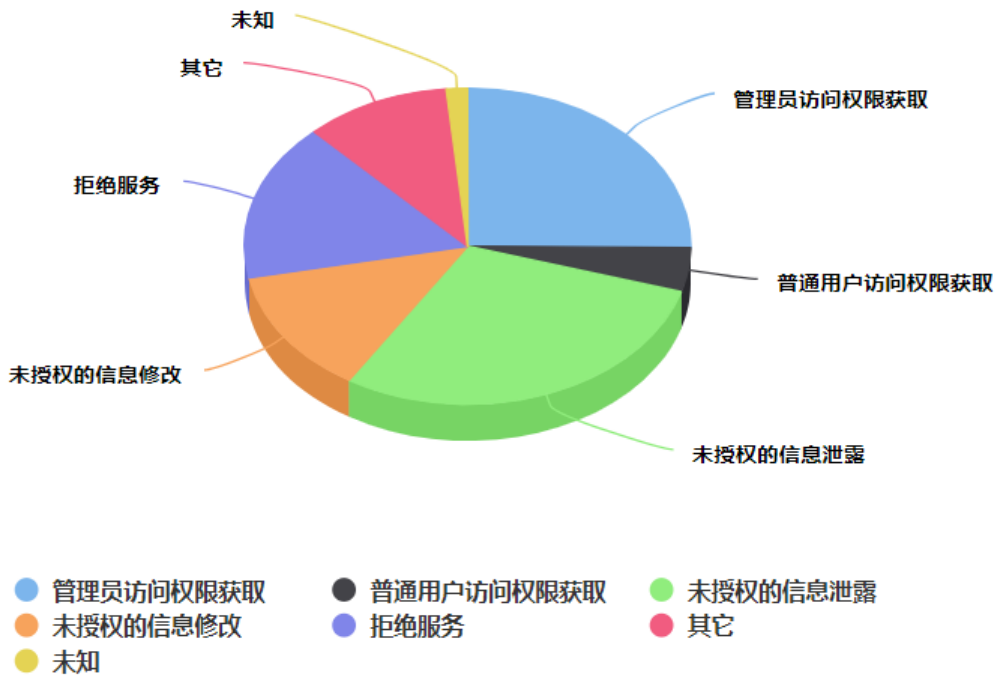
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 420 个，其中高危漏洞 128 个、中危漏洞 253 个、低危漏洞 39 个。漏洞平均分值为 5.79。本周收录的漏洞中，涉及 0day 漏洞 314 个（占 75%），其中互联网上出现“WordPress Modern Events Calendar 远程代码执行漏洞、ToaruOS 权限提升漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的原创漏洞总数 4843 个，与上周（5176 个）环比减少 6%。

二、安全漏洞增长数量及种类分布情况

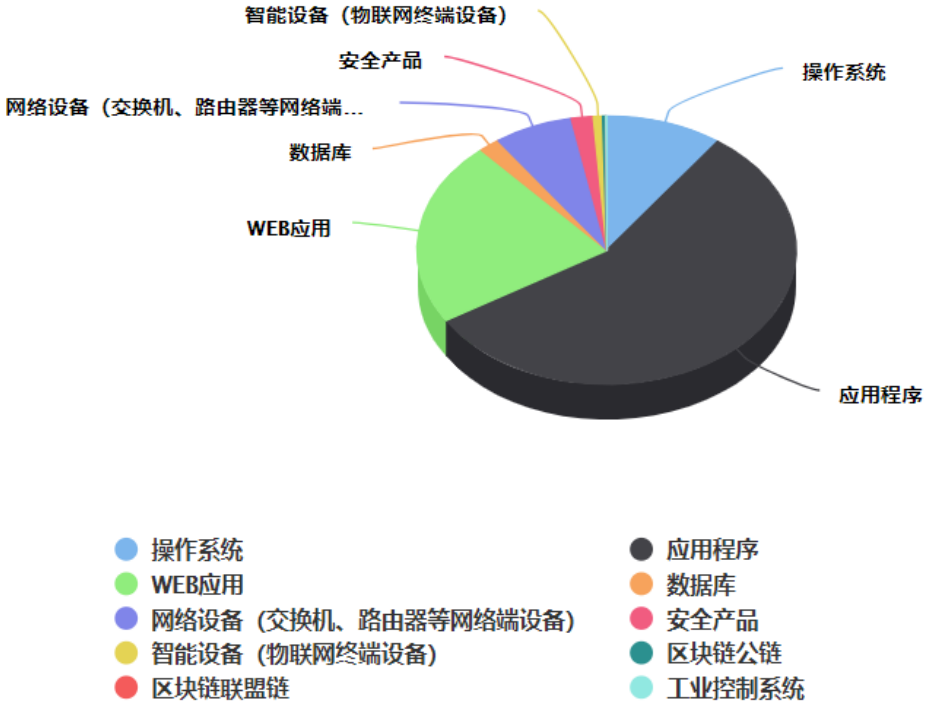
➢ 漏洞产生原因（2021 年 9 月 1 日—2021 年 9 月 30）



➢ 漏洞引发的威胁（2021 年 9 月 1 日—2021 年 9 月 30）



➢ 漏洞影响对象类型（2021 年 9 月 1 日—2021 年 9 月 30）



三、安全产业动态

➢ 奋力谱写网络强国建设精彩华章 我国网信事业发展成就综述

习近平总书记高度重视网络安全和信息化工作，提出一系列具有开创性意义的新思想新观点新论断，形成了习近平总书记关于网络强国的重要思想。在这一重要思想指引下，我国网信事业取得积极进展和瞩目成就。

积极构建安全清朗的精神家园

聪者听于无声，明者见于未形。“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。”习近平总书记高瞻远瞩的话语，为推动我国网络安全体系的建立，树立正确的网络安全观指明了方向。”

深刻把握信息化发展大势，积极应对网络安全挑战。党的十八大以来，中央网信办会同相关部门以总体国家安全观为指导，不断完善网络安全工作顶层设计和总体布局。出台网络安全法、数据安全法、个人信息保护法、《关键信息基础设施安全保护条例》《国家网络空间安全战略》等网络安全法律法规战略，印发《关于加强网络安全学科建设和人才培养的意见》《关于加强国家网络安全标准化工作的若干意见》等政策文件，不断夯实国家网络安全工作根基；

自 2014 年以来，十部门共同连续举办国家网络安全宣传周，有效提升全民网络安全意识和防护技能，“网络安全为人民，网络安全靠人民”的理念深入人心；

我国网络安全创新发展取得积极成效，2020 年网络安全产业规模超过 1700 亿元，较 2015 年翻了一番，年均增速超过 15%。网络空间是亿万民众共同的精神家园。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，不符合人民利益。

坚持“正能量是总要求、管得住是硬道理、用得好是真本事”，有关部门密切配合、协同发力，网上正能量更强劲、主旋律更高昂，网络空间日益清朗。

2021 年“清朗”系列专项行动重点整治未成年人网络环境、整治 PUSH 弹窗新闻信息突出问题、整治网上文娱及热点排行乱象等 8 方面内容，在全网开展“大扫除”，有效遏制网络乱象滋生蔓延；加强网上网下文化市场监管，“护苗 2021”专项行动中，仅 7 至 8 月，全国累计查缴少儿类非法出版物 52.3 万件，查删网络有害信息 12.6 万余条；《“抵制网络谣言 共建网络文明”倡议书》发布，倡导全社会共管共治网络谣言，共建共享网络文明。

信息化发展适应人民新期待

线上办公、视频会议、网络直播、云游博物馆……当前，信息技术发展日益蓬勃，“数字红利”加快释放，互联网深度融入百姓生活。

“网信事业发展必须贯彻以人民为中心的发展思想，把增进人民福祉作为信息化发展的出发点和落脚点”。习近平总书记为信息化发展指明方向。”

“十四五”规划和 2035 年远景目标纲要提出，适应数字技术全面融入社会交往和日常生活新趋势，促进公共服务和社会运行方式创新，构筑全民畅享的数字生活。

适应人民新期待，党的十八大以来，《国家信息化发展战略纲要》《“十三五”国家信息化规划》等战略规划出台，相关部门紧抓落实，信息化建设工作取得重要进展。

信息基础建设规模全球领先——我国已建成全球最大光纤网络、4G 和 5G 独立组网网

络；截至 2021 年 6 月，我国网民规模为 10.11 亿，互联网普及率达 71.6%，庞大的网民规模为推动我国经济高质量发展提供强大内生动力。

信息技术创新能力持续提升——基础性、通用性技术研发取得重要进展，5G、人工智能、高性能计算、量子计算等领域取得一批重大科技成果。

数字经济发展活力不断增强——当前新一轮科技革命和产业变革突飞猛进，带动经济发展加速迈向数字经济新阶段。2020 年，数字经济核心产业增加值占 GDP 比重达到 7.8%，数字经济质量效益明显提升；大数据产业规模达 718.7 亿元，同比增长 16.0%，增幅领跑全球大数据市场。

信息技术助力弥合数字鸿沟——截至 2020 年底，全国中小学互联网接入率达到 100%，远程医疗协作网覆盖 2.4 万余家医疗机构。互联网应用适老化水平及特殊群体的无障碍普及不断推进，健康码适老化相关功能已覆盖全国至少 3000 万老年群体。一串串亮眼数字的背后，亿万人民在信息化建设的不断推进下拥有了更多获得感、幸福感、安全感。

推动全球互联网发展治理迈向更高水平

当信息化革命浪潮席卷全球经济格局、利益格局、安全格局，各国在全球互联网治理体系中休戚与共。

习近平总书记深刻指出，国际网络空间治理应该坚持多边参与、多方参与，发挥政府、国际组织、互联网企业、技术社群、民间机构、公民个人等各种主体作用。

党的十八大以来，我国不断深化网络空间国际交流合作，积极参与互联网国际技术标准制定、网络基础设施建设和网络空间国际治理体系建设，共同推动全球互联网发展治理迈向

更高水平。

从《网络空间国际合作战略》的发布，到 G20 杭州峰会《二十国集团数字经济发展与合作倡议》的签署，再到发起“中非携手构建网络空间命运共同体倡议”……中国不断深化网络空间国际合作，推动世界各国共同搭乘互联网和数字经济发展的快车。

自 2014 年起世界互联网大会已连续 7 年成功举办，关于全球互联网发展治理的“四项原则”“五点主张”“四个共同”等中国智慧，得到国际社会特别是广大发展中国家的广泛认同，网络空间命运共同体等重要理念深入人心。

金秋九月，水乡乌镇再次汇聚世界目光。以“迈向数字文明新时代——携手构建网络空间命运共同体”为主题的 2021 年世界互联网大会乌镇峰会即将在这里举行。这场全球互联网界的盛事，将继续引领全球互联网领域的合作发展；中国智慧、中国方案将再次为世界发展注入更多新活力。（来源：新华社）

➢ 让互联网更加互联畅通

如今，互联网应用早已深度融入人们的日常生活，在沟通信息、优化服务等方面发挥着重要作用。与此同时，一些互联网平台之间存在的技术限制、利益排挤、互相屏蔽等问题，也给用户带来麻烦与困扰。比如，不少网友都有过类似经历：在社交平台给好友分享一个网址链接，却显示“无法打开”，需要手动复制链接后跳转至系统浏览器才能访问。平台之间互设壁垒、信息不能直接共享，不仅影响使用体验、损害用户权益，还扰乱市场秩序、妨碍公平竞争，不利于互联网行业和平台经济规范健康持续发展。

最近，工信部有关业务部门召开“屏蔽网址链接问题行政指导会”，提出有关即时通信软件的合规标准，要求限期内各平台必须按标准解除屏蔽，否则将依法采取处置措施。在国务院新闻办举办的新闻发布会上，工信部相关负责人表示，企业要按照整改要求，务实推动即时通信屏蔽网址链接等不同类型的问题分步骤、分阶段得到解决。对此，相关企业迅速表态，将在以安全为底线的前提下，分阶段分步骤地实施。

保障合法的网址链接正常访问，是互联网发展的基本要求。互联网的一个重要价值就在于，通过降低准入门槛，让获取信息、抵达用户更加便捷。在一个突破时空边界的平台上，企业能够以更高效便捷的方式开拓市场、服务客户，进而激励创新、促进竞争。从某种意义上说，互联网的活力源泉就是开放。得益于互联互通的开放生态，创新业态不断涌现，平台

经济快速发展，消费者福利持续增进。正因如此，整治屏蔽网址链接问题，实质上就是打通近些年互联网平台之间形成的断点堵点，推动互联网平台回归互联互通的轨道。

不同的互联网平台之所以相互屏蔽，归根到底是企业将流量思维凌驾于用户权益之上。移动互联网时代，注意力成为稀缺资源。各平台为争夺流量、保持用户黏性，便倾向于通过屏蔽竞争对手链接的方式、打造相对封闭的平台生态，导致互联网空间壁垒丛生、相互割裂。短期来看，屏蔽外链，聚拢了流量，换取了利益；但长远来看，则是屏蔽了便捷，丢失了口碑。平台企业应该认识到，互联互通是互联网行业高质量发展的必然要求，只有让用户安全顺畅使用互联网，才有利于增强自身竞争能力，也才能真正赢得市场认可。

推动形成互通开放、规范有序、保障安全的互联网发展环境，既是行业所向、大势所趋，也须多方联动、久久为功。在前期开展 APP 专项治理基础上，工信部于今年 7 月启动了为期半年的互联网行业专项整治行动，其中就包含整治恶意屏蔽网址链接等问题。在自查整改过程中，一些企业仍存在认识与行动脱节、落实举措不到位的情况。实现互联互通任重道远，对于监管部门而言，应加强督查检查，确保问题整改到位；作为平台企业，也应压实主体责任，积极顺应趋势，主动拆除壁垒，变流量思维为用户思维，以实际行动维护开放的互联网生态。

开放、共享，可谓互联网的基因。敞开胸怀、破除壁垒，让互联网更加互联畅通，共同促进互联网行业形成包容开放共享的良好生态，我们就能推动平台经济健康发展、行稳致远。

（来源：人民日报）

➢ 《个人信息保护法》：构筑新时代个人信息权益保护的安全防护网

《中华人民共和国个人信息保护法》即将于 2021 年 11 月 1 日起正式施行，这标志着我国个人信息保护立法体系进入新的阶段。个人信息保护的相关制度在《网络安全法》就已经有了专章规定，其后的《民法典》人格权编和《数据安全法》也先后规定了涉及个人信息的具体保护制度。相较于前述立法活动，《个人信息保护法》的出台为个人信息权益保护、信息处理者的义务以及主管机关的职权范围提供了全面的、体系化的法律依据。个人面对非法收集和处理个人信息的侵权行为能够获得更具体、更多样的救济方式，权利保障范围涵盖个人信息收集、存储、使用、加工、传输、提供、公开、删除等多个环节以及敏感个人信息处理、个人信息跨境提供等特定场景。个人信息权益得到切实有效的制度保障，也为信息产业明确了经营行为的合法性边界，与《国家安全法》《网络安全法》《民法典》和《数据安全法》等法律法规共同构建起个人信息保护的法治堤坝。

一、个人信息处理活动的基本原则框架：合法、正当、必要与诚信

《个人信息保护法》的出台可谓是顺应人民群众最迫切的利益诉求。在数字经济时代，个人与网络信息服务提供者之间存在明显的信息鸿沟，为了能够获得相应的信息服务使用权限，个人不得不“主动”提供自己的个人信息，但是却无法真正知晓自己的个人信息究竟将如何被处理以及谁将拥有自己的个人信息。更有甚者，个人信息买卖已然成为完整的黑灰产

业链条，个人的财产安全和人身安全受到严重威胁。为了充分保护个人信息权益，同时也是为了规范个人信息处理活动，促进信息产业发展，《个人信息保护法》顺势而为，明确了个人信息处理活动应当以合法、正当、必要和诚信作为基本原则，即任何类型和任何阶段的个人信息处理行为均应当满足这些原则性要求，即便现行立法没有明确规定特定个人信息处理行为是否满足法定义务，如若相关行为违背合法、正当、必要和诚信四项基本原则之一，也应当承担相应的民事法律责任，情节严重的，应当承担刑事责任。换言之，这四项基本原则构成了《个人信息保护法》的内容主线：第一，合法性原则要求个人信息处理行为应当满足法律法规规定，这里的“法”并不单一局限于《个人信息保护法》，还包括《网络安全法》《数据安全法》《民法典》《刑法》《关键信息基础设施安全保护条例》等法律法规。第二，正当性原则要求个人信息处理行为应当符合立法宗旨和法律价值，不得以谋求自身利益而侵害其他个人的个人信息权益。在实践中，部分 APP 运营者在用户注册阶段以不显著、不直接的方式向用户展示个人信息处理的目的、范围和方式等重要信息，这种行为显然违背了正当性原则。第三，必要性原则要求个人信息的收集范围和处理方式应当仅以实现相应的信息服务功能和业务目的为必要。该原则强有力地回应了当下社会对 APP 运营者肆意收集处理个人信息行为的担忧和质疑，避免个人为获取相应信息服务而被动提供个人信息的问题恶化。例如，地图导航类 APP 运营者的个人信息收集范围仅应当以地理位置信息为限，职业、工资、旅游偏好等其他与地图导航功能无关的个人信息显然不在“与处理目的直接相关”的范围之内。第四，诚信原则强调个人信息处理者不得利用自身的优势地位侵害个人信息权益。一方面，个人信息处理者应当诚实信用地按照约定的处理目的和范围处理个人信息；另一方面，个人信息处理者不应当故意隐瞒、有意淡化事关个人信息权益的提示说明事项。

二、个人信息权益保护方式：权利与义务的一体化

在欧盟《通用数据保护条例》出台之后，全球各国个人信息立法曾一度或多或少受到欧盟个人数据权利体系的理论影响，删除权、更正权、查询权等具体权利似乎成为个人信息保护领域的“制度范本”。我国《个人信息保护法》则立足于中国本土实践，向全世界提供了全新的个人信息保护思路：重视个人信息权益的实质性保护，以权利与义务的一体化要求为导向。从《个人信息保护法》的第四章和第五章内容来看，个人在个人信息处理活动中享有查阅、复制、更正、补充、请求删除个人信息等具体权利。并且，个人信息处理者也应当积极履行法定义务，确保个人权利能够有效实现，倘若个人信息处理者设置各种不合理非必要的维权程序、客服流程等“维权门槛”，既违背了个人信息处理行为的基本原则，也构成了法定义务履行不充分。

个人在个人信息处理活动中行使权利有两个前提条件：第一，个人对个人信息处理应当享有充分知情权和决定权。所谓的知情权是指个人有权知晓其个人信息的收集处理目的、范围和方式，并且这种知情应当是以清晰易懂的显著方式予以实现。换言之，如果个人信息处理者为避免承担法律责任将所有个人信息处理事项事无巨细地向用户直接展示，又或是以小号字体、密集文字排版等方式告知用户个人信息处理活动，则显然构成对个人信息知情权的实质侵害。第二，个人在实现知情权之后应当能够独立自主地决定是否提供个人信息以及决定个人信息的实际处理范围和方式。在实践中，部分用户即便知晓个人信息处理的相关事项，但囿于使用特定信息服务的需要以及行业内格式合同的泛滥，用户无力决定个人信息的具体处理方式。为了解决此类问题，《个人信息保护法》明确个人有权限制或限制对其个人信息处理。此外，决定权也有其例外情形。

三、充足的安全感：国家机关全方位保护个人信息

《个人信息保护法》提供的个人信息保护路径并不局限权利与义务的一致性要求，还包括专门的国家机关履行个人信息保护职责，提供全方位的个人信息保护和救济方式。《个人信息保护法》所提供的充足安全感既来自于国家机关处理个人信息的特别规定，也来源于国家机关履行职责的专门规定。一方面，《个人信息保护法》规定国家机关处理个人信息同样应当遵守法律、行政法规规定的权限和程序。个人信息权益受到前所未有的重视，即便个人信息处理者是国家机关，其收集处理范围和限度同样不得超出履行法定职责之需要。并且，

国家机关处理个人信息之前，应当依照规定，履行告知义务。另一方面，《个人信息保护法》明确规定了国家网信部门负责统筹协调个人信息保护工作和相关监督管理工作。国务院有关部门依照本法和有关法律、行政法规的规定，在各自职责范围内负责个人信息保护和监督管理工作。具体而言，除了日常熟知的个人信息保护宣传教育，接受、处理与个人信息保护相关的投诉、举报，调查、处理违法处理个人信息等活动之外，还包括个人信息保护评估、个人信息跨境传输安全评估、第三方安全认证体系、个人信息保护技术标准制定等具体领域的工作内容。此外，为了切实解决近期出现的“监控偷拍人脸识别”“大数据杀熟”等社会热点问题，《个人信息保护法》还专门规定国家网信部门统筹协调有关部门依据本法推进人脸识别、人工智能等新技术、新应用领域个人信息保护规则、标准制定工作。

个人信息保护绝不能停留于纸面的权利宣誓与义务要求，更要重视之后法律实施过程中可能面临的新问题和新挑战，平衡个人信息权益与信息产业良性发展的双重诉求，个人信息保护还需要有效统筹协调立法、执法和司法三个环节，要让老百姓看得到、摸得着、感受得到真正的个人信息权益保护，推进个人信息保护工作的纵深化发展。（来源：中国网信网）

➢ 个人信息与隐私为何需要区别保护？

隐私作为一项重要的人格权，主要是通过《民法典》人格权编的规则予以保护，并辅之以相应的单行法和司法解释，形成周延的保护。对于个人信息而言，由于对此种权益的保护具有公法与私法的双重属性，完全通过私法的保护是不全面的，其中涉及公法的管理性规范，需要公法上的协同。因此，有必要制定一部集公法规范与私法规范于一体、全面保护个人信息的法律。

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《个人信息保护法》，并将于 2021 年 11 月 1 日起施行。《个人信息保护法》是我国第一部系统、全面保护个人信息的专门性法律，其在性质上属于公法、私法的组合。但就《个人信息保护法》的内容而言，大多是关于民事权利和义务的规定，就民事规范而言，《个人信息保护法》和民法典之间的关系就是特别法与基础法的关系，或者说是特别法与普通法的关系。

个人信息与隐私确实存在交叉重合关系。《民法典》在第 1032 条关于隐私概念的规定中，已经明确提出了私密信息的概念，并将其作为隐私权保护的重要内容之一。而《个人信息保护法》第二章专门规定了敏感信息处理的特殊规则，其实，敏感信息大多属于私密信息。

虽然如此，个人信息不同于隐私，需要通过特别立法予以规范和保护。

二者的范围并非完全等同。依据《民法典》第 1032 条第 2 款，“隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。”除私密信息涉及敏感个人信息以外，其他类型的隐私不涉及个人信息。即使就部分敏感个人信息而言，权利人可能出于特定的目的而愿意公开，或已经进行了公开。这些信息可能已经不再构成隐私，但仍然属于敏感个人信息。

个人信息具有集合性。隐私通常很难具有集合性，其本身是单个主体享有的权益。基于人权保护的原因，许多国家将隐私作为基本人权对待，故一般不允许将隐私作集合化处理。而个人信息通常可以集合在一起形成数据，无论是匿名化还是非匿名化处理，个人信息都可成为数据。这就决定了个人信息与大数据的关联非常密切。从全球范围来看，许多法律文件均采用的是个人数据权的表述，且这一术语的使用已基本在欧盟层面的立法中达成了一致。故对于个人信息也要强调数据的流通与共享，因此，也会出现对个人信息的匿名化处理，此时会形成纯粹的数据。

个人信息具有可利用性。与数据具有流通价值不同，隐私原则上不能利用，即使实践中已经产生了利用隐私的情况，但利用范围极其狭窄，并且一般也不得违背公序良俗。隐私权更强调私密性，故隐私权规则对隐私的保护程度要更强。而对于个人信息而言，法律对于其保护与应用是并重的，既强调保护，也要注重利用和流通，故在个人信息保护的场合利益权衡的空间要大得多。所以，对个人信息的规范，法律要注重规范的收集、利用、储存等处理行为。《民法典》第 993 条的规定中，有关人格权的商业化利用刻意未将隐私权纳入，因此，原则上隐私权不得进行商业化利用。

个人信息具有自动处理性。隐私通常不涉及大规模处理的问题，侵犯隐私通常具有个别性。现代社会中，为了社会组织、运行与管理现代化，个人信息的大规模收集和自动处理是必须的，而社会的良序运行不以隐私的收集与自动化处理为必要。这种个人信息的自动化处理又可能会出现算法歧视、算法黑箱、网络画像的滥用等问题。有的企业采集、获取消费者的浏览偏好、消费习惯等信息，利用大数据分析、用户画像等方式，向消费者推送相关信息，支配甚至误导消费者。

此类行为违反了诚实信用原则，损害了公平交易，因此，《个人信息保护法》第 24 条规定，利用个人信息进行自动化决策，不得对个人在交易价格等交易条件上实行不合理的差别待遇。通过自动化决策方式向个人进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式。这就明确规定了禁止“大数据杀熟”。但隐私在一般情形下不具有上述特点，对其处理一般具有个别性和非自动处理性。故对隐私的保护需要行政介入的程度相较个人信息更小。

个人信息泄露的程序法应对具有特殊性。由于个人信息往往以集合的方式出现，一旦其泄露可能会涉及大规模侵权问题，因而需要进行特殊的诉讼制度与行政的介入来处理。正是由于个人信息具有规模性，所以个人信息的诉讼可能会采取集体诉讼的方式来处理，也可以通过公益诉讼方式解决个人诉讼动因不足的问题，我国《个人信息保护法》第 71 条专门规定了公益诉讼。

总之，由于个人信息具有上述特殊性，难以在单一部门法中完全实现，故需要民法与行政法的结合来进行保护，这就产生了《个人信息保护法》，它在本质上属于领域立法。虽然隐私与个人信息天然具有重合性，但是，这两者具有明显的区别，《民法典》和《个人信息保护法》对它们进行了明确的规则界分，设置了不同的保护规则，并在适用中将产生不同的法律效果。正确理解并适用隐私权和个人信息的规则界分，对保护人民群众的切身利益，维护个人人格尊严具有重要意义。（来源：北京日报）

四、政府之声

➢ 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》

2021 年 9 月 14 日，中共中央办公厅、国务院办公厅印发了《关于加强网络文明建设的意见》（以下简称《意见》），并发出通知，要求各地区各部门结合实际认真贯彻落实。《意见》指出，加强网络文明建设，是推进社会主义精神文明建设、提高社会文明程度的必然要求，是适应社会主要矛盾变化、满足人民对美好生活向往的迫切需要，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。**《意见》包括总体要求、加强网络空间思想引领、加强网络空间文化培育、加强网络空间道德建设、加强网络空间行为规范、加强网络空间生态治理、加强网络空间文明创建、组织实施八个部分。**


中华人民共和国中央人民政府
www.gov.cn

简 | 繁 | EN | 注册 | 登录

国务院 总理 新闻 政策 互动 服务 数据 国情 国家政务服务平台

首页 > 新闻 > 滚动

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》

2021-09-14 17:53 来源： 新华社 【字体：大 中 小】 打印

新华社北京9月14日电 近日，中共中央办公厅、国务院办公厅印发了《关于加强网络文明建设的意见》（以下简称《意见》），并发出通知，要求各地区各部门结合实际认真贯彻落实。

《意见》指出，加强网络文明建设，是推进社会主义精神文明建设、提高社会文明程度的必然要求，是适应社会主要矛盾变化、满足人民对美好生活向往的迫切需要，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。《意见》包括总体要求、加强网络空间思想引领、加强网络空间文化培育、加强网络空间道德建设、加强网络空间行为规范、加强网络空间生态治理、加强网络空间文明创建、组织实施八个部分。

《意见》强调，加强网络文明建设要坚持以习近平新时代中国特色社会主义思想为指导，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，大力弘扬社会主义核心价值观，全面推进文明办网、文明用网、文明上网、文明兴网，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，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。

《意见》明确，加强网络文明建设的工作目标是：理论武装占领新阵地，马克思主义在

网络意识形态领域的指导地位进一步巩固，全党全国人民团结奋斗的共同思想基础进一步巩固；文化培育取得新成效，社会主义核心价值观深入人心，人民群众网上精神文化生活日益健康丰富；道德建设迈出新步伐，网民思想道德素质明显提高，向上向善、诚信互助的网络风尚更加浓厚；文明素养得到新提高，青少年网民网络素养不断提升，网络平台主体责任和行业自律有效落实；治理效能实现新提升，网络生态日益向好，网络空间法治化深入推进，网络违法犯罪打击防范治理能力持续提升；创建活动开创新局面，群众性精神文明创建活动向网上有效延伸，网络文明品牌活动巩固提升，网络空间更加清朗。

《意见》指出，要加强网络空间思想引领。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，推动党的创新理论走深走心走实。加强重点理论网站、公众账号、客户端建设，紧密结合中国特色社会主义伟大实践特别是新时代党和国家事业发展新变化新成就，有针对性地开展网上理论宣传活动。精心做好网上重大主题宣传，加强网络传播手段建设和创新，打造“现象级”传播产品。深入推进媒体融合发展，实施移动优先战略，加大中央和地方主要新闻单位、重点新闻网站等主流媒体移动端建设推广力度。

《意见》指出，要加强网络空间文化培育。以社会主义核心价值观引领网络文化建设，广泛凝聚新闻网站、商业平台等传播合力，把社会主义核心价值观传播到广大网民中、传导到社会各方面。深入开展网上党史学习教育，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，弘扬党和人民在奋斗中形成的伟大精神，旗帜鲜明反对历史虚无主义。激发中华优秀传统文化活力，打造广大网民喜闻乐见的特色品牌活动和原创精品，推动中华优秀传统文化创造性转化、创新性发展。丰富优质网络文化产品供给，引导网站、公众账号、客户端等平台和广大网民创作生产积极健康、向上向善的网络文化产品，举办丰富多彩的网络文化活动。提升网络公共文化服务水平，推动国家重大文化设施和国有文化资源数字化网络化，提高网络公共文化服务供给的普惠性和便捷性。

《意见》指出，要加强网络空间道德建设。强化网上道德示范引领，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，推动形成崇德向善、见贤思齐的网络文明环境。深化网络诚信建设，举办形式多样的线上线下品牌活动，大力传播诚信文化，倡导诚实守信的价值理念，鼓励支持互联网企业和平台完善内部诚信规范与机制，营造依法办网、诚信用网的良好氛围。发展网络公益事业，深入实施网络公益工程，广泛开展形式多样的网络文明志愿服务和网络公益活动，打造网络公益品牌。

《意见》指出，要加强网络空间行为规范。培育符合社会主义核心价值观的网络伦理和

行为规则，鼓励各地区各部门结合文明创建工作制定出台符合自身特点的网络文明准则，规范网上用语，把网络文明建设要求融入行业管理规范。着力提升青少年网络素养，进一步完善政府、学校、家庭、社会相结合的网络素养教育机制，提高青少年正确用网和安全防范意识能力，精心打造青少年愿听愿看的优秀网络文化产品。健全防范青少年沉迷网络工作机制，依法坚决打击和制止青少年网络欺凌，保护青少年在网络空间的合法权益。强化网络平台责任，加强网站平台社区规则、用户协议建设，引导网络平台增强国家安全意识。加强互联网行业自律，坚持经济效益和社会效益并重的价值导向，督促互联网企业积极履行社会责任。发挥行业组织引导督促作用，促进行业健康规范发展，鼓励支持各类网络社会组织参与网络文明建设。

《意见》指出，要加强网络空间生态治理。深入开展网络文明引导，大力强化网络文明意识，充分利用重要传统节日、重大节庆和纪念日组织开展网络文明主题实践活动，教育广大网民自觉抵制歪风邪气，弘扬文明风尚。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，构建以中国互联网联合辟谣平台为依托的全国网络辟谣联动机制。深入推进“清朗”、“净网”系列专项行动，深化打击网络违法犯罪，深化公众账号、直播带货、知识问答等领域不文明问题治理，开展互联网领域虚假信息治理。健全网络不文明现象投诉举报机制，动员广大网民积极参与监督，推动网络空间共治共享。坚持依法治理网络空间，把弘扬社会主义核心价值观贯穿网络立法执法司法普法各环节，发挥法律法规对维护良好网络秩序、树立文明网络风尚的保障作用。加强个人信息保护法、数据安全法贯彻实施，加快制定修订并实施文化产业促进法、广播电视法、网络犯罪防治法、未成年人网络保护条例、互联网信息服务管理办法等法律法规。创新开展网络普法系列活动，增强公民法律意识和法治素养。

《意见》指出，要加强网络空间文明创建。推动群众性精神文明创建活动向网上延伸，充分发挥新时代文明实践中心和县级融媒体中心作用，加强网民网络文明素养实践教育基地建设，推动基层开展网络文明建设活动。开展军民共建网络文明活动，促进军政军民团结。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。深入实施争做中国好网民工程，引导广大网民尊德守法、文明互动、理性表达，引导全社会提升网络文明素养，净化网络环境。

《意见》要求，各地区各部门要充分认识加强网络文明建设的重要意义，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。各级网信办、文明办要牵头抓总，加强对网络文明建设的组织指导和协调服务。注重发挥网民主体

作用，广泛搭建平台，开展特色活动，吸引广大网民特别是青少年网民主动参与网络文明建设。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。加强对工作规律的认识把握，不断推动内容形式、方法手段、渠道载体等创新，增强网络文明建设的针对性有效性和吸引力感染力。（来源：新华社）

➢ 证监会发布《证券期货业网络安全等级保护基本要求》等 2 项金融行业标准

2021 年 8 月 30 日，证监会发布《证券期货业网络安全等级保护基本要求》、《证券期货业网络安全等级保护测评要求》2 项金融行业标准，自公布之日起施行。


中国证券监督管理委员会
CHINA SECURITIES REGULATORY COMMISSION

证券期货监督管理信息公开目录

索 引 号:40000895X/　　分类: 其他；证监会公告
发布机构: 证监会　　发文日期: 2021年08月30日
名　　称:【第19号公告】《证券期货业网络安全等级保护基本要求》等2项金融行业标准
文　　号: :证监会公告[2021]19号　　主 题 词:

【第19号公告】《证券期货业网络安全等级保护基本要求》等2项金融行业标准

中国证券监督管理委员会公告
〔2021〕19号

现公布金融行业推荐性标准《证券期货业网络安全等级保护基本要求》（JR/T 0060—2021）、《证券期货业网络安全等级保护测评要求》（JR/T 0067—2021），自公布之日起施行。《证券期货业信息系统安全等级保护基本要求（试行）》（JR/T 0060—2010）、《证券期货业信息系统安全等级保护测评要求（试行）》（JR/T 0067—2011）同时废止。

中国证监会
2021年8月30日

证监会发布《证券期货业网络安全等级保护基本要求》等2项金融行业标准

国家标准《网络安全等级保护基本要求》(GB/T 22239—2019)、《网络安全等级保护测评要求》(GB/T 28448—2019)于 2019 年 5 月正式发布，是国家开展网络安全等级保护工作的指导性文件。

《证券期货业网络安全等级保护基本要求》(JR/T 0060—2021)规定了证券期货业网络安全等级保护的总体要求，以及第一级到第四级等级保护对象的安全通用要求和安全扩展要求，适用于证券期货业分等级的非涉密对象的安全建设和监督管理。《证券期货业网络安全等级保护测评要求》(JR/T 0067—2021)规定了证券期货业网络安全等级保护的等级测评方法、第一级到第四级的网络安全等级保护对象的测评要求、整体测评以及测评结论，适用于证券

期货业安全测评服务机构、等级保护对象的运营使用单位及行业主管部门对证券期货业等级保护对象的安全状况进行安全测评，也可供网络安全职能部门进行证券期货业网络安全等级保护监督检查时参考使用。

下一步，证监会将继续推进资本市场信息化建设，着力加强基础标准建设，持续完善技术安全监管制度，确保在技术进步的同时，实现安全管控水平稳步提升。（来源：中国证监会）

- **《证券期货业网络安全等级保护基本要求》等 2 项金融行业标准**
- **全文：**http://www.csrc.gov.cn/pub/zjhpublic/zjh/202109/t20210903_404765.htm

➢ 工业和信息化部发布关于加强车联网网络安全和数据安全工作的通知

2021 年 9 月 15 日，工业和信息化部发布《关于加强车联网网络安全和数据安全工作的通知》（下称《通知》）。《通知》要求，智能网联汽车生产企业、车联网服务平台运营企业要采取合法、正当方式收集数据，还要防范数据泄露、毁损、丢失、篡改、误用、滥用等风险。


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 > 政务公开 > 政策文件 > 文件发布 > 通知
发文机关：工业和信息化部
标　　题：工业和信息化部关于加强车联网网络安全和数据安全工作的通知
发文字号：工信部网安〔2021〕134号
成文日期：2021-09-15　　发布日期：2021-09-16
发布机构：网络安全管理局　　分　　类：网络安全管理
工业和信息化部关于加强车联网网络安全和数据安全工作的通知
工信部网安〔2021〕134号
各省、自治区、直辖市及新疆生产建设兵团工业和信息化主管部门，各省、自治区、直辖市通信管理局，中国电信集团有限公司、中国移动通信集团有限公司、中国联合网络通信集团有限公司，有关智能网联汽车生产企业、车联网服务平台运营企业，有

《通知》要求，按照“谁主管、谁负责，谁运营、谁负责”的原则，智能网联汽车生产企业、车联网服务平台运营企业要建立数据管理台账，实施数据分类分级管理，加强个人信息与重要数据保护。

《通知》还要求智能网联汽车生产企业、车联网服务平台运营企业合理开发利用数据资源，防范在使用自动化决策技术处理数据时，侵犯用户隐私权和知情权。明确数据共享和开发利用的安全管理和责任要求，对数据合作方数据安全保护能力进行审核评估，对数据共享

使用情况进行监督管理。

《通知》还提到了汽车数据的境外提供和存储问题。工业和信息化部要求，智能网联汽车生产企业、车联网服务平台运营企业向境外提供在中华人民共和国境内收集和产生的重要数据时，应当依法依规进行数据出境安全评估并向所在省（区、市）通信管理局、工业和信息化主管部门报备。各省（区、市）通信管理局会同工业和信息化主管部门做好数据出境备案、安全评估等工作。（来源：工信部）

- **《工业和信息化部关于加强车联网网络安全和数据安全工作的通知》全文：**
- https://www.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2021/art_ba43080de41242e4ab6d6d5fa3218ff9.html

➢ CNNIC 发布第 48 次《中国互联网络发展状况统计报告》

2021 年 9 月 15 日，中国互联网络信息中心（CNNIC）发布第 48 次《中国互联网络发展状况统计报告》（以下简称《报告》）显示，互联网行业的基础支撑、创新驱动、融合引领作用更加凸显，在国民经济和社会中的地位显著提升。

《报告》显示，截至 2021 年 6 月，我国网民规模达 10.11 亿，较 2020 年 12 月增长 2175 万，互联网普及率达 71.6%。《报告》显示，截至 2021 年 4 月，我国光纤宽带用户占比提升至 94%，固定宽带端到端用户体验速率达到 51.2Mbps，移动网络速率在全球 139 个国家和地区中排第 4 位。截至 2021 年 6 月，我国 IPv6 地址数量达 62023 块/32，较 2020 年底增长 7.6%；移动电话基站总数达 948 万个，较 2020 年 12 月净增 17 万个。截至 2021 年 5 月，我国 5G 标准必要专利声明数量占比超过 38%，列全球首位；5G 应用创新案例已超过 9000 个；具有一定行业和区域影响力的工业互联网平台超过 100 家，连接设备数超过了 7000 万台（套）；“5G + 工业互联网”在建项目已超过 1500 个，覆盖 20 余个国民经济重要行业。互联网应用蓬勃发展，《报告》显示，截至 2021 年 6 月，我国网上外卖用户规模达 4.69 亿，较 2020 年 12 月增长 4976 万；在线办公用户规模达 3.81 亿，较 2020 年 12 月增长 3506 万，网民使用率为 37.7%；在线医疗用户规模达 2.39 亿，较 2020 年 12 月增长 2453 万，占网民整体的 23.7%。（来源：人民邮电报）

- **第 48 次《中国互联网络发展状况统计报告》全文：**
- http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/202109/P020210915523670981527.pdf

五、本期重要漏洞实例

➢ Microsoft 发布 2021 年 9 月安全更新

发布日期：2021-09-14

更新日期：2021-09-14

描述：9 月 14 日，微软发布了 2021 年 9 月份的月度例行安全公告，修复了其多款产品存在的 85 个安全漏洞。受影响的产品包括：Windows 10 21H1 & Windows Server v21H1（33 个）、Windows 10 20H2 & Windows Server v20H2（33 个）、Windows 10 2004 & Windows Server v2004（33 个）、Windows 8.1 & Server 2012 R2（25 个）、Windows Server 2012（23 个）、Windows RT 8.1（25 个）和 Microsoft Office-related software（9 个）。利用上述漏洞，攻击者可进行欺骗，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-2021-40444	Microsoft MSHTML 远程代码执行漏洞	重要 远程代码执行	Server, version 20H2 Server, version 2004 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1 Server 2022
CVE-2021-36965	Windows WLAN AutoConfig Service 远程代码执行漏洞	严重 远程代码执行	Server, version 20H2 Server, version 2004 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1 Server 2022
CVE-2021-36958	Windows Print Spooler 远程代码执行漏洞	重要 远程代码执行	Server, version 20H2 Server, version 2004 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1 Server 2022

CVE-2021-38658	Microsoft Office Graphics 远程代码执行漏洞	重要 远程代码执行	Office 2016 Office 2013 Office 2019 Office 2019 for Mac
CVE-2021-38655	Microsoft Excel 远程代码执行漏洞	重要 远程代码执行	Excel 2016 Excel 2013 Office Web Apps Server 2013 365 Apps Enterprise Office 2019 Office 2019 for Mac Office Online Server
CVE-2021-38646	Microsoft Office Access Connectivity Engine 远程代码执行漏洞	重要 远程代码执行	Office 2016 Office 2013 Office 2019 365 Apps Enterprise
CVE-2021-38651	Microsoft SharePoint Server 欺骗漏洞	重要 欺骗	SharePoint Foundation 2013 SharePoint Server 2019 SharePoint Enterprise Server 2016

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

➢ Google Chrome libjpeg-turbo 信息泄露漏洞

发布日期：2021-09-26
受影响系统：Google Chrome <94.0.4606.54
描述：

CVE(CAN) ID: CVE-2021-37972
Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。Google Chrome 94.0.4606.54 之前版本中的 libjpeg-turbo 存在信息泄露漏洞。攻击者可利用漏洞获取敏感信息。
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/2021/09/stable-channel-update-for-desktop_21.html

➢ Adobe Framemaker 越界写入漏洞

发布日期：2021-09-26
受影响系统：
Adobe Adobe Framemaker <=2019 Update 8
Adobe Adobe Framemaker <=2020 Release Update 2
描述：

CVE(CAN) ID: CVE-2021-39831
Adobe FrameMaker 是一款文档处理程序，用于编写和编辑包括结构化文档在内的大型或复杂文档。Adobe Framemaker 2019 Update 8、2020 Release Update 2 及更早版本存在越界写入漏洞。攻击者可利用该漏洞执行任意代码。
建议：

厂商补丁：
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：
链接：https://helpx.adobe.com/security/products/framemaker/apsb21-74.html

➢ 多款 Cisco SD-WAN 产品缓冲区溢出漏洞

发布日期：2021-09-26
受影响系统：
Cisco IOS XE SD-WAN Software
Cisco SD-WAN vEdge Cloud Routers
Cisco SD-WAN vManage Software
Cisco SD-WAN vEdge Routers
Cisco SD-WAN vBond Orchestrator Software
Cisco SD-WAN vSmart Controller Software
描述：

CVE(CAN) ID: CVE-2021-1279
Cisco SD-WAN vEdge 是美国思科（Cisco）公司的是一款路由器。该设备可为思科 SD-WAN 解决方案提供基本 WAN，安全性和多云功能。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。多款 Cisco SD-WAN 产品存在缓冲区溢出漏洞。该漏洞源于程序未对 SNMPv3 管理功能的输入进行正确验证检查。未经身份认证的远程攻击者可通过将特制的 SNMPv3 流量发送到特定设备利用该漏洞导致设备拒绝服务。
建议：

厂商补丁：
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP

六、本期网络安全事件

➢ 南非司法部网络系统遭到黑客攻击陷入瘫痪

2021 年 9 月 6 日据外媒报道，南非司法和宪法发展部正在努力恢复其运作，因为最近的勒索软件攻击加密了其所有系统，导致内部和公众无法使用所有电子服务。作为攻击的后果，司法和宪法发展部表示，儿童抚养费的支付现在被搁置，直到系统重新上线。该事件发生在 9 月 6 日，该部门启动了此类事件的应急计划，以确保该国的一些活动继续进行。

南非司法和宪法发展部发言人 Steve Mahlangu 表示：“（攻击）导致所有信息系统被加密，内部员工以及公众都无法使用。因此，该部门提供的所有电子服务都受到影响，包括签发授权书、保释服务、电子邮件和部门网站。”

上周，Mahlangu 表示，在转为手动模式记录听证会后，法庭开庭继续进行。此外，还采取了手动程序来发布各种法律文件。然而，勒索软件攻击影响了每月的儿童抚养费支付，这些支付被推迟到系统恢复之前。Steve Mahlangu 称：“虽然该部门无法确定所需系统恢复的确切日期，但它将确保所有儿童抚养费的安全，以便在系统重新上线后支付给合法的受益人。”

该部门仍在恢复正常运作的过程中，但不能确定何时活动将再次变得正常。这项工作的一部分是建立一个新的电子邮件系统，一些工作人员已经迁移到该系统。再加上网络恢复需

要很长的时间，这表明黑客没有得到报酬。

目前还不清楚谁是这次攻击的幕后黑手。许多勒索软件团伙在加密数据之前也会窃取数据，以迫使受害者在公开泄密的压力下支付赎金。Mahlangu 上周说，该部的 IT 专家已经发现“没有数据泄露的迹象”。到目前为止，还没有任何一个拥有数据泄露网站的团伙声称对这次攻击负责。（来源：cnBeta）

➢ 联合国证实其网络曾于今年 4 月受到黑客攻击

2021 年 9 月 10 日，据国外媒体报道 9 日联合国证实，今年早些时候联合国的网络受到了黑客攻击，劫取大量数据，这些数据可以用来攻击跨政府机构内部机构。

据悉，**黑客进入联合国网络的方法似乎并不复杂：**就是利用从黑网购买的一名联合国雇员的登录账号窃取数据。其属于联合国专有项目管理软件 Umoja 上的一个账户。网络安全公司 Resecurity 的调查结果报道了这一事件。据该公司称，黑客可以从那里更深入地进入联合国的网络。已知的黑客最早进入联合国系统的日期是 4 月 5 日，截至 8 月 7 日，他们仍在网络上活动。而与此前美国的几次黑客攻击事件不同的是，黑客侵入联合国系统没有进行损坏，而是收集了联合国计算机网络的信息。

据悉，联合国在 Resecurity 公司向其通报之前已经发现了黑客的攻击并做出了反应，以

减轻影响。这些黑客可能在为未来进一步的攻击做铺垫，或者将信息出售给其他可能试图侵入联合国的组织。

Recorded Future 的高级威胁分析师艾伦·利斯卡(Allan Liska)说，“传统上，像联合国这样的组织一直是攻击目标，我们预计，网络犯罪分子将越来越多地针对这些组织，并对其进行渗透。而且我们发现联合国雇员的用户名和密码在暗网上出售。”（来源：央视网）

➢ 建行一客户经理泄露客户信息 3 万多条 获刑八个月

2021 年 9 月 1 日，近日，广东省人民检察院在官网公布了一批个人信息保护检察公益诉讼典型案例。其中，某银行客户经理王某非法出售客户信息引发关注。具体而言，**2017 年至 2018 年期间，王某非法出售其在业务活动中获取的银行客户账户信息共 31465 条，信息内容包括公民姓名、身份证号码、电话号码、银行卡账号**等，上述信息被相关贷款公司用于拨打电话并推销贷款业务信息，从事不正当竞争。

在裁判文书网上也查阅到了该案件，通过检察院官网公布的案件、裁判文书网及湛江银保监局公布的处罚信息来看，上述涉案银行为建设银行。

2017 年 4 月开始，黄杰程（另案处理）在湛江市某公司从事信用贷款、抵押贷款业务。其通过朋友介绍认识原在中国建设湛江分行工作的王涛与原在某公司湛江分公司工作的周声凯，黄杰程知道周声凯从事过贷款业务，手中有客户资料，其趁周声凯离职之际，将周声凯手中的客户资料交给自己，再让员工以拨打手机的方式推销公司贷款产品。

随后，周声凯于 2018 年 11 月 6 日将收集的公民信息资料通过邮箱的形式，发送给了黄杰程，共计包括湛江市某楼盘业主的个人信息、含公民姓名及电话号码等有效信息共 15585 条。2017 年下半年，黄杰程又让王涛为其提供中国建设银行客户资料，并答应付给王涛获利的 15%作为回扣。随后，王涛擅自登录银行内部电脑系统，截图客户资料后多次通过电子邮箱发送到黄杰程的电子邮箱，黄杰程让员工利用上述信息打电话联系客户办理贷款业务。

经查，王涛共计提供给黄杰程含公民姓名及电话号码等有效信息累计 31465 条，黄杰程因此按获利总额的 15%支付出售公民信息的回扣 6500 元给王涛，另支付给王涛 30224 元作为介绍客户的“辛苦费”。王某共计牟利 36724 元。 经过审理，法院认为，王涛、周声凯构成侵犯公民个人信息罪。

最终，法院一审判决：王涛犯侵犯公民个人信息罪，判处有期徒刑八个月，缓刑一年，并处罚金人民币一万元。周声凯犯侵犯公民个人信息罪，判处有期徒刑六个月，缓刑一年，并处罚金人民币三千元。 另外，在广东省检察院公布的案件中显示，2020 年 12 月 31 日，湛江银保监分局以涉案银行对客户信息安全管理不到位的案由作出罚款 20 万元的行政处罚决定。随后，湛江银保监分局对上述客户经理作出禁止从事银行业工作 1 年的行政处罚决定。（来源：红星新闻）

➢ 物流仓库管理员出售公民个人信息 5000 余条获刑 10 个月

2021 年 9 月 22 日，近日，上海市青浦区人民检察院以涉嫌侵犯公民个人信息罪对被告人石某提起公诉，并对其侵害社会公共利益的行为提起刑事附带民事公益诉讼。

案情介绍

石某自 2015 年起来到上海打工，在租房时认识了比他大 5 岁的室友朱某。朱某传授给石某许多找工作的经验，两人成为好友。2017 年 3 月，石某因盗窃罪被判处拘役 4 个月，期满后，他搬离了合租的公寓，但是双方互留了联系方式，也经常碰面聚会。不久后，石某找到一份在快递物流公司做仓库管理员的工作，而朱某也成为了一名保险公司业务员。到 2020 年初，朱某觉得做自己这行要掌握更多的客户信息，如果能掌握其他保险公司的客户信息，就能“针对性”地推销保险了，于是便找到石某。

“你每天要接触那么多信息，只要找出其他保险公司寄出的保单，把这些客户的姓

名、地址和手机号码传给我，我就以每条有效信息 10 元的价格付给你钱，多划算啊！”朱某向石某提议。石某原本就觉得自己工资不够开销，听到 10 元一条的价格不由心动，立即答应了。

自 2020 年 6 月起，石某开始向朱某出售客户信息，一开始他小心翼翼在自己所在的网点内查看有有没有符合朱某要求的信息，但这样做效率较低。不久后，朱某建议石某可以使用内部工作账号来查询保险公司寄出的快递。石某于是照办，根据朱某提供的扫描 APP 账号，将信息上传。朱某筛选后，挑出符合要求的信息计算数量，将“报酬”转账给石某。

两人自认为神不知鬼不觉，石某使用自己工作账号前前后后查询了 5000 多条面单信息，朱某认可了其中 2000 多条，并支付了 2 万余元人民币。直至 2021 年 2 月，快递公司发现员工账号异常，报案后警方于当日将石某抓获。朱某知晓后立即将石某联系方式删除，试图逃跑，但最终难逃法网，被警方抓获。

检察机关审查认为

石某在 2020 年 6 月至 2021 年 1 月担任物流公司仓库管理员期间，利用工作便利，查询包含收件人姓名、电话和地址的公民个人信息 5000 余条并出售给他人使用，从中非法获利人民币 2.7 万余元，其行为已触犯我国刑法，构成侵犯公民个人信息罪；同时，也违反了民法典及网络安全法相关规定，侵犯了不特定多数人个人隐私及个人信息安全,进而损害了公共信息安全这一社会公共利益。

判决情况

2021 年 9 月，法院以侵犯公民个人信息罪判处被告人石某有期徒刑十个月，并处罚金；在附带民事公益诉讼中，法院判决被告人石某在庭审直播中公开向社会公众赔礼道歉、永久删除非法获取的公民个人信息，并支付相应赔偿款。（来源：腾讯网 ）

➢ 加州医院因数据泄露被起诉 近 50 万患者信息受影响

2021 年 9 月 28 日，据外媒报道：加州大学圣地亚哥分校健康中心在 7 月通过公告披露了一起安全事件。该通知表明，在 2020 年 12 月 2 日至 2021 年 4 月 8 日期间，有人未经授权访问了“某些员工电子邮件帐户”。

入侵发生在一名拥有健康系统电子邮件帐户的员工接受网络钓鱼攻击中提供的诱饵之后。3 月 12 日在系统网络中检测到可疑活动，并于 4 月 8 日关闭了受感染的电子邮件帐户。“当加州大学圣地亚哥分校健康中心发现这个问题时，我们终止了对这些帐户的未经授权的访问，并加强了我们的安全控制，”医疗保健提供者说。

卫生系统表示：攻击中可能被访问和泄露的数据可能包括全名、地址、出生日期、电子邮件地址、传真号码、索赔信息（包括接受护理的日期和费用）、实验室结果、医疗诊断和条件、医疗记录号、处方信息、治疗信息、社会安全号、政府识别号、财务帐号、学生识别号、用户名和“我们的患者、学生和员工社区的子集”的密码。

9 月 7 日，加州大学圣地亚哥分校健康中心开始通知 495,949 名个人（可提供联系信息），

他们可能受到了违规行为的影响。

《圣地亚哥联合论坛报》报道称，代表 El Cajon 一名癌症患者的律师上周就数据泄露向加州大学圣地亚哥分校健康中心提起诉讼。原告指控医疗保健系统违反合同、疏忽和违反加州消费者隐私和医疗保密法。

“如果加州大学圣地亚哥分校健康中心制定了正确的数据保护协议，这种违规行为是可以预防的，”圣地亚哥律师贾森哈特利说。

原告声称，医疗保健系统未能就如何避免网络钓鱼攻击对员工进行充分培训，并且忽视了实施合理的安全措施。该诉讼正在为所有医疗数据和个人信息可能已被暴露的个人寻求集体诉讼地位和未指明的损害赔偿。（来源：GoUpSec）

➢ 破解 AT&T 逾 190 万部手机一男子被美国判处 12 年监禁

2021 年 9 月 18 日据报道，美国地方法院判处一名累计破解超过 190 万部 AT&T 手机的男子穆罕默德·法赫德(Muhammad Fahd)12 年监禁。根据美国司法部公布的情况说明，穆罕默德甚至在知道自己被调查的情况下，仍在继续犯罪活动。他的这些活动总共持续 7 年。在法赫德的宣判听证会上，法官罗伯特·拉斯尼克(Robert Lasnik)表示，法赫德犯下了“可怕的长期网络犯罪”，导致 AT&T 总共损失 2.015 亿美元。

美国司法部表示，2012 年，法赫德通过 Facebook 联系了 AT&T 的一名员工，“用一大笔钱”贿赂他们，让他们协助破解客户的手机。法赫德是巴基斯坦和格林纳达公民。他还劝说这名 AT&T 员工，在该公司的华盛顿州博赛尔呼叫中心唆使他人一同参与欺诈活动。

最终，这些员工为“没有资格的客户”破解手机，而这些客户向法赫德支付费用。2013 年春季，AT&T 推出了一个系统，导致员工在破解 IMEI 时更困难。法赫德随后招募了一名工程师来开发恶意软件，并将其安装至 AT&T 的系统，从而更高效地远程破解手机。美国司法部说，这些 AT&T 员工向法赫德详细介绍了公司的系统和破解方法，帮助他的违法活动。据称，法赫德使用的恶意软件获得了系统信息和其他 AT&T 员工的账号密码。开发者利用这些信息对恶意软件进行改进。

AT&T 指控称，法赫德和他的同伙通过这种方式破解了超过 190 万部手机。借助破解，客户就可以不必在设备上支付费用，给 AT&T 造成了九位数的损失。

在 2017 年遭到起诉之后，法赫德于 2018 年在香港被捕。他随后被引渡至美国，并于 2020 年 9 月承认合谋实施电信诈骗。（来源：新浪科技）