# 国盟信息安全通报

2021 年 11 月 30 日第 245 期

全国售后服务中心

# 国盟信息安全通报

（第 245 期）

国际信息安全学习联盟

**2021 年 11 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 585 个，其中高危漏洞 137 个、中危漏洞 409 个、低危漏洞 39 个。漏洞平均分值为 5.77。本周收录的漏洞中，涉及 0day 漏洞 393 个（占 67%），其中互联网上出现“AyaCMS 跨站请求伪造漏洞、Sourcecodester Complaint Management System 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原创漏洞总数 10498 个，与上周（20493 个）环比减少 49%。

# 主要内容

一、概述 ..... 4
二、安全漏洞增长数量及种类分布情况 ..... 4
➢漏洞产生原因（2021 年 11 月 1 日—2021 年 11 月 30）.....4
➢漏洞引发的威胁（2021 年 11 月 1 日—2021 年 11 月 30）.....5
➢漏洞影响对象类型（2021 年 11 月 1 日—2021 年 11 月 30）.....5
三、安全产业动态 ..... 6
➢互联网下一站不能再以方便牺牲安全.....6
➢营造良好数字生态 .....7
➢法网密织 数据安全国家治理现新局.....12
➢统筹数字经济发展和数据安全 依法切实保护个人信息权益.....16
四、政府之声 ..... 18
➢工业和信息化部发布关于开展信息通信服务感知提升行动的通知.....18
➢中央网络安全和信息化委员会印发《提升全民数字素养与技能行动纲要》 .....19
➢国家网信办对《网络数据安全管理条例（征求意见稿）》公开征求意见.....20
➢新《中华人民共和国审计法》2022 年 1 月 1 日起施行.....22
五、本期重要漏洞实例 ..... 24
➢Microsoft 发布 2021 年 10 月安全更新.....24
➢IBM Tivoli Key Lifecycle Manager 信息泄露漏洞.....25
➢Adobe Acrobat Reader DC 堆栈缓冲区溢出漏洞.....26
➢Desdev DedeCMS 跨站脚本漏洞.....26
六、本期网络安全事件 ..... 27
➢安踏集团通报一员工秘密窃取公司 95GB 保密信息被开除.....27
➢多伦多交通委员会承认数万员工个人信息被泄漏.....28
➢非法获取明星航班信息 两粉丝侵犯公民个人信息获刑.....29
➢特斯拉“断网”让数百车主“被锁车外” 马斯克发推道歉 .....30
➢快递员伙同他人非法获取公民个人信息，出售 10000 条被追责.....31
➢连续两天大规模宕机 星展银行遭遇 11 年来最大故障.....32

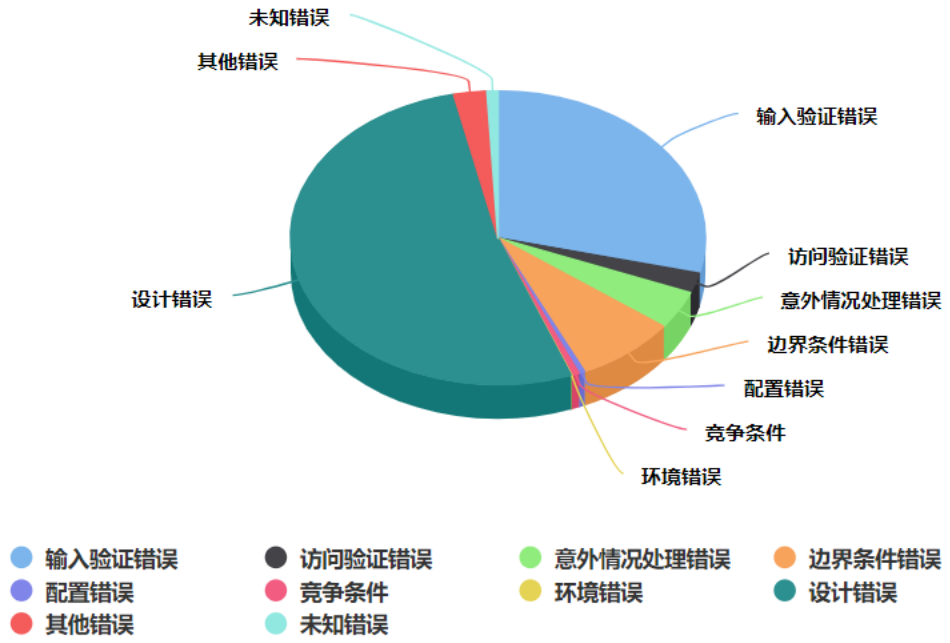
**注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。**

# 一、概述

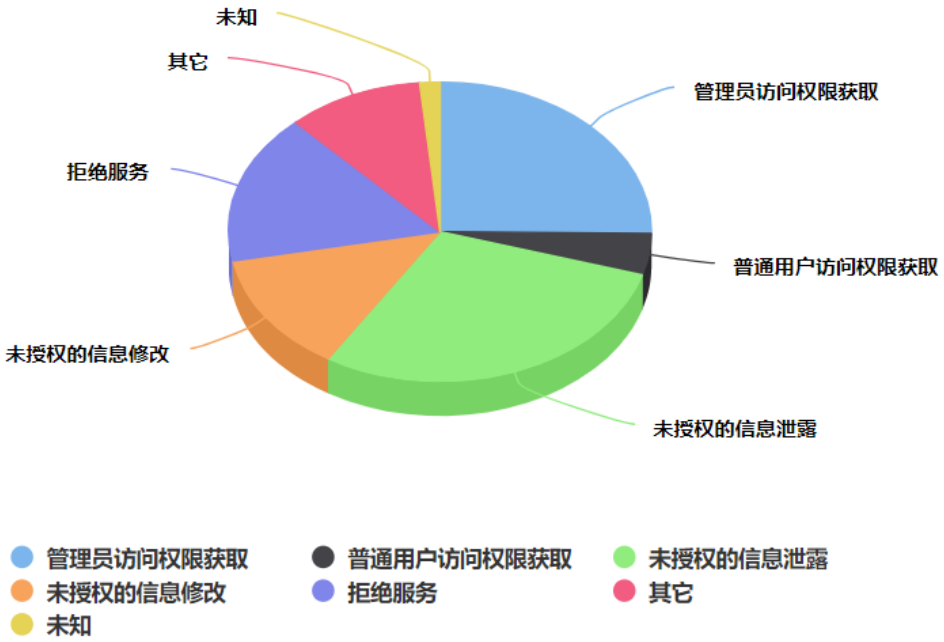
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 402 个，其中高危漏洞 117 个、中危漏洞 231 个、低危漏洞 54 个。漏洞平均分值为 5.63。本周收录的漏洞中，涉及 0day 漏洞 334 个（占 83%），其中互联网上出现“libde265 堆缓冲区溢出漏洞（CNVD-2021-78426）、libde265 堆缓冲区溢出漏洞（CNVD-2021-78427）”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的原创漏洞总数 7662 个，与上周（5750 个）环比增加 33%。

# 二、安全漏洞增长数量及种类分布情况

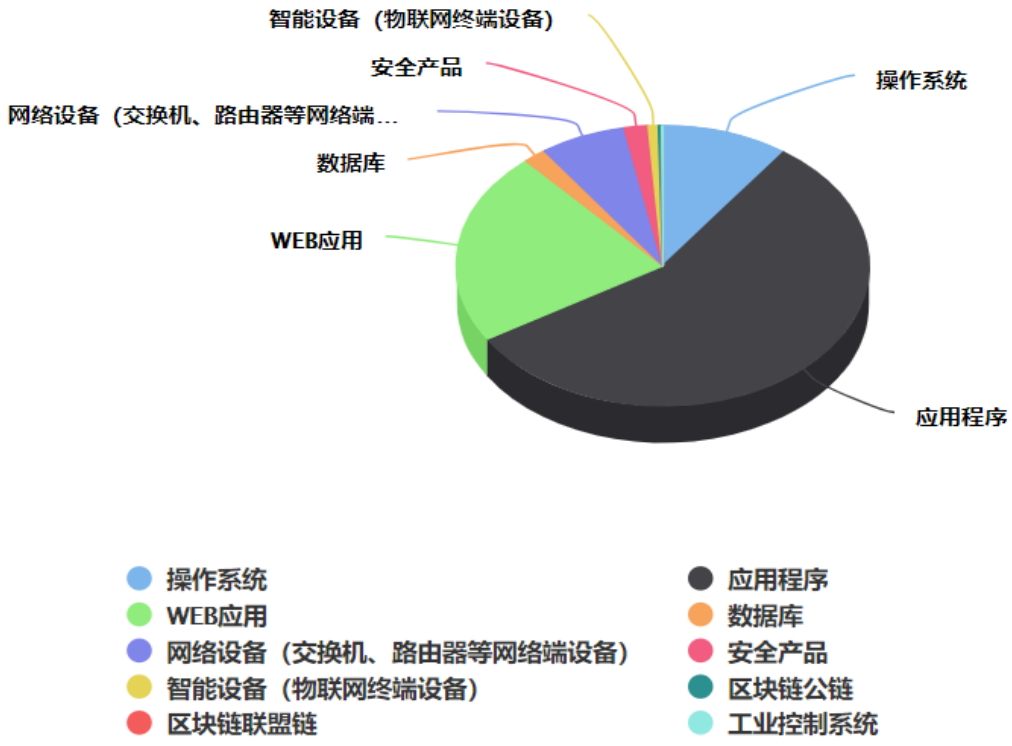
## ➢ 漏洞产生原因（2021 年 11 月 1 日—2021 年 11 月 30）



## ➢ 漏洞引发的威胁（2021 年 11 月 1 日—2021 年 11 月 30）




## ➢ 漏洞影响对象类型（2021 年 11 月 1 日—2021 年 11 月 30）



# 三、安全产业动态

## ➢ 互联网下一站不能再以方便牺牲安全

2021 年 11 月 14 日，国家网信办发布了关于《网络数据安全管理条例》公开征求意见的通知。其中特别提到，数据处理者利用生物特征进行个人身份认证的，应对必要性、安全性进行风险评估，不得将人脸、步态、指纹、虹膜、声纹等生物特征作为唯一的个人身份认证方式。

随着技术迭代升级，具有生物特征的网络认证方式成为新潮流，其中蕴藏的风险却令人担忧。从指纹到人脸、从步态到声纹，生物特征对每个人来说具有唯一性、基础性，一旦滥用或泄露，负面效应难以估量。以人脸为例，轻则被商家用来精准营销，重则可能落入诈骗犯罪者手中。此前，“谁偷了我的脸”已引发不少纠纷，还曾冒出消费者戴着头盔看房、业主戴帽子口罩全身武装回家的尴尬。从这个意义上说，明确登录认证不能“唯”生物特征，是对个人隐私的切实保护，也是对当下焦点问题的及时回应。

互联网诞生已 52 年，接入中国也已 27 年。一直以来，其最大的标签就是“方便”。方便交流，从 Email 到微博微信，万里之遥亦可轻松对话；方便购物，各大平台全球扫货，足不出户即可轻松下单；方便生活，在线问诊、共享课程，一根网线对接现实需求。然而，透过网络世界的“繁华”，我们也看到了技术几乎不受限制地开发应用，以及对个人信息的无度索取。如果说在人们刚触网时，或不明就里或为了“方便”让渡掉了一些权利，那么现在，

当“你刚夹一筷子，就被送了一桌子”，当个体的姓名电话、指纹人脸都被明码标价，“方便”的外溢负面效应就到了必须警惕的时候。

今天的中国互联网拥有世界上体量庞大的网民群体，走过跑马圈地的上半程，互联网靠什么走向提质增效的下一站？其中很重要的一点就是守住个人隐私保护红线，不再以方便牺牲安全。这些年，随着《民法典》《个人信息保护法》《网络安全法》《数据安全法》等不同层级、不同门类的法律法规陆续出台，我国数据治理规则的体系逐步建立并完善，但相比技术应用的飞奔，制度更新总有某种滞后性。共享单车无序投放带来的治理“后遗症”，算法推荐大行其道造成的“信息茧房”等都提醒我们，既然治理上的“时差”难以避免，就更需要见事早，把问题想在前面，把规矩定在前面。

用户数据，如何存储、怎么传输，谁有权限接触、接触到什么层次，应获得怎样的授权，违反会受到何种惩处……这些问题，不光要写在纸面上，更要落到实践中。整体来看，目前我国这方面的法治震慑力还不足，还需要以普遍问题作为突破点，以具体案例作为抓手，真正让法律长出“牙齿”。对“数据小偷”的严肃惩处，对更多新技术、新应用的开发也是一种必要提醒，确保信息安全意识融入到代码的第一行间。

互联网生活早已成为公共生活的重要子集，谁都不希望关门闭户，也不希望自身信息处于“裸奔”状态。我们能做的，是让技术运行在规范轨道，以造福社会而不是侵扰生活。（来源：北京日报）

## ➢ 营造良好数字生态

2021 年 11 月 5 日，《人民日报》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：**

当今时代，以信息技术为代表的新一轮科技革命和产业变革加速推进，形成了以数字理念、数字发展、数字治理、数字安全、数字合作等为主要内容的数字生态，对经济社会发展、人民生产生活和国际格局产生了广泛影响，给社会生产方式、生活方式和治理方式带来深刻变革。党的十八大以来，以习近平同志为核心的党中央高度重视数字生态建设，“十四五”规划和 2035 年远景目标纲要作出“营造良好数字生态”的重要部署，明确了数字生态建设的目标要求、主攻方向、重点任务。着力营造开放、健康、安全的数字生态，是“十四五”

时期加快建设网络强国和数字中国、推动经济社会高质量发展的重要战略任务。

**坚持思想引领，把握数字文明新机遇**

习近平总书记指出：“数字技术正以新理念、新业态、新模式全面融入人类经济、政治、文化、社会、生态文明建设各领域和全过程，给人类生产生活带来广泛而深刻的影响。当前，世界百年变局和世纪疫情交织叠加，国际社会迫切需要携起手来，顺应信息化、数字化、网络化、智能化发展趋势，抓住机遇，应对挑战。”我们要深入学习贯彻习近平新时代中国特色社会主义思想，立足新发展阶段，完整、准确、全面贯彻新发展理念，构建新发展格局，推动高质量发展，深刻把握人类社会进入信息时代、迈向数字文明的发展大势，充分认识营造良好数字生态的重要意义和深远影响。

**抢占信息时代发展先机的战略任务。**近年来，数字技术创新和迭代速度明显加快，在提高社会生产力、优化资源配置等方面的作用日益凸显。营造良好数字生态，有利于充分激发数字技术的创新活力、要素潜能、发展空间，引领和驱动经济结构调整、产业发展升级、消费需求增长、治理格局优化，为加快建设数字经济、数字社会、数字政府提供良好环境和有力支撑。特别要看到，世界主要国家均把信息化作为国家战略重点和优先发展方向，通过优化数字生态加快推动数字化转型发展。我们必须主动适应数字化变革的时代潮流，掌握网信事业发展的历史主动，着力营造良好数字生态，打造数字优势、赢得发展先机。

**构筑人民美好数字生活的迫切要求。**网信事业必须贯彻以人民为中心的发展思想，把实现好、维护好、发展好最广大人民根本利益作为一切工作的出发点和落脚点。我国网民规模已超过 10 亿，形成了全球最为庞大、生机勃勃的数字社会，数字生活成为人民群众的重要生活方式。同时也要清醒看到，算法滥用、平台垄断、大数据“杀熟”、个人信息和数据泄露等问题突出，直接损害人民群众的合法权益。我们要把营造良好数字生态作为满足人民对

美好生活新期待的重要举措，优化数字环境，推动数字惠民，让亿万人民在共享发展成果上有更多获得感、幸福感、安全感。

**加快建设网络强国和数字中国的重要支撑。**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指引下，我国核心技术突破和产业布局优化不断提速，数字经济作为经济发展新引擎的作用日益凸显，数据安全保护能力持续提升，数字生态建设取得积极成效。实践证明，加强数字生态建设有力促进了各类要素在生产、分配、流通、消费各环节有机衔接，实现了对产业链、供应链、价值链的优化升级和融合融通，为建设网络强国和数字中国奠定了重要基础。新征程上，我们要紧紧围绕贯彻落实“十四五”规划和 2035 年远景目标纲要，进一步释放数字创新活力，以良好数字生态为构建新发展格局、推动经济社会高质量发展提供强劲动能。

**坚持创新赋能，激发数字经济新活力**

数字经济具有高创新性、强渗透性、广覆盖性，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，是推动经济社会高质量发展的重要引擎。深化数字技术创新应用、激发数字经济发展活力，是营造良好数字生态的重要内容和关键领域。要把创新作为第一动力，大力推动技术创新、产业创新、应用创新、服务创新，努力为数字经济赋能、提质、增效，营造繁荣发展的数字生态。

**加强关键核心技术攻关。**立足高水平自立自强，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，更加注重基础研究和原始创新，推动网信领域关键核心技术、基础前沿技术加快突破。突出自主安全可控，优化核心技术产业布局，培育互利共生、融合发展的良好产业生态，不断增强产业链供应链韧性，切实掌握技术自主权和发展主动权。

**加快新型基础设施建设。**把握信息基础设施快速演进升级的重要契机，加强顶层设计和前瞻布局，统筹推进通信网络基础设施、算力基础设施、融合与创新基础设施等建设，聚焦 5G、IPv6、卫星互联网、物联网、人工智能平台等重点领域，大力推进体系化建设、规模化部署、产业化应用，推动我国新一代信息基础设施朝着高速泛在、天地一体、云网融合、智能敏捷、绿色低碳、安全可控的方向加速演进。

**推动数字经济和实体经济融合发展。**充分发挥数字技术对经济发展的放大、叠加、倍增作用，大力推进数字产业化、产业数字化，促进互联网、大数据、人工智能和实体经济深度融合，推动制造业、服务业、农业的数字化、网络化、智能化升级。发挥海量数据和丰富应用场景优势，加快推进“上云用数赋智”行动，培育数字新产业、新业态、新模式，打造具

有国际竞争力的数字产业集群。积极推进数字化和绿色化协同转型，实现数字化进程中的绿色发展。

**坚持综合施策，营造数字生态治理新环境**

加强数字生态建设，既要厚植创新创造的土壤，也要构建规范有序的环境。要始终把法治作为基础性手段，坚持促进发展和监管规范两手抓、两手都要硬，着力构建数字生态规则体系，全面提升数字生态治理能力，推动数字生态健康、有序、可持续发展。

**构建清朗网络空间。**加强互联网内容建设，充分发挥数字化、网络化、智能化传播优势，推动党的创新理论深入人心，不断壮大网上主流思想舆论，构建网上网下同心圆。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，聚焦群众反映强烈的网络生态乱象，压实网站平台信息内容主体责任，建设行业自律机制，深入推进“清朗”“净网”系列专项行动，持续净化网络空间。大力加强网络文明建设，用积极健康、向上向善的网络文化滋养人心、滋养社会，营造文明办网、文明用网、文明上网、文明兴网的良好氛围。

**推进数字惠民便民。**坚持以人民为中心的发展思想，依托数字政府和数字社会建设，不断提升公共服务数字化、均等化、便捷化水平，推动社会治理精准化、高效化发展。加快推进数字乡村、新型智慧城市建设，持续提升教育、医疗、卫生、环境保护等重点民生领域数字化水平，丰富数字化生活场景和体验，打造智慧共享、和睦共治的新型数字生活。

**提升数据治理效能。**统筹数据开发利用、隐私保护和公共安全，加快完善数据治理体制机制，建立健全数据资源产权制度、交易规则和管理规范，确保数据要素安全有序流通。完善数据资源开放共享制度，推动政务数据、公共数据、企业数据、个人数据等全社会各类数

据良性互动、融合应用，打破数据孤岛，释放数据红利。有序推动培育数据交易市场，着力培育规范的交易平台和市场主体，深度挖掘数据要素价值，充分释放数据促进经济社会发展的强劲动能。

**规范互联网平台运营。**构建与数字平台特征相适应的政策法规体系，完善促进企业有序发展和规范运营的监管机制，依法保障新产业、新业态、新模式健康发展。坚持鼓励技术创新与推动技术向善并重，完善适应人工智能、大数据、云计算等新技术新应用的制度规则，依法规制算法滥用等不正当竞争行为。防止平台垄断和资本无序扩张，加大执法力度，提升监管能力，确保平台经济公平竞争、有序发展。

**坚持防范风险，筑牢数字安全新屏障**

安全是发展的前提，发展是安全的保障。营造良好数字生态，要坚持安全和发展并重，深入实施网络安全法、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等法律法规，有效防范和化解网络安全和数据安全领域的风险挑战，全面加强重要领域数据资源、重要网络和信息系统以及个人信息的安全保障。

**着力构建数据安全保障体系。**建立健全数据安全管理、风险评估、检测认证等机制，构建贯穿基础网络、数据中心、云平台、数据、应用等一体协同安全保障体系。完善适用于大数据环境下的数据分类分级保护制度，加强对海量数据汇聚融合的风险防护，强化数据资源全生命周期安全防护。加强重点领域数据安全管理，完善重要数据目录，强化政务数据安全。

**提升网络安全防护能力。**防范应对数字新技术新应用安全风险，密切跟踪发展动态，提升人工智能、5G、区块链、工业互联网、车联网等安全防护能力。加强网络安全基础设施建设，强化跨领域网络安全信息共享和工作协同。压实网络安全工作责任制，完善关键信息基础设施安全保护体系，加大关键系统、设备、平台等网络安全检查力度，做到关口前移、防患未然。加强网络安全宣传教育和人才培养，大力发展网络安全产业，加快形成多方参与、优势互补、融合发展的网络安全良性生态。

**加大个人信息保护力度。**推动重点行业建立完善长效保护机制，强化企业主体责任，规范企业采集使用个人信息行为。加强对生物特征等敏感个人信息的保护，深化违法违规收集使用个人信息治理，坚决打击非法买卖个人信息、侵犯公民隐私等各类违法犯罪活动。完善个人信息安全事件举报受理渠道，切实维护广大网民合法权益。深入开展个人信息安全防护知识技能宣传普及，提升全社会网络安全和数据安全意识。

**坚持开放共享，构建数字生态合作新格局**

数字生态具有高度全球化的特征，开放合作、互利共赢是营造良好数字生态的重要内涵。

习近平总书记指出：“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。”“中国愿同世界各国一道，共同担起为人类谋进步的历史责任，激发数字经济活力，增强数字政府效能，优化数字社会环境，构建数字合作格局，筑牢数字安全屏障，让数字文明造福各国人民，推动构建人类命运共同体。”我们要深入学习贯彻习近平总书记重要讲话、重要指示精神，深化网络空间数字生态合作，加快构建网络空间命运共同体，促进发展共同推进、安全共同维护、治理共同参与、成果共同分享。

**推动完善网络空间国际规则。**坚持以联合国为主渠道、以联合国宪章为基本原则，推动研究制定更加平衡地反映各方利益关切特别是广大发展中国家利益的网络空间国际规则。加强国家间数字生态领域政策协调，积极参与数据安全、数字货币、数字税等国际规则和数字技术标准制定，推动建立更加公正合理的互联网基础资源分配机制，实现网络空间资源共享、责任共担、合作共治。

**打造数字生态合作平台。**积极搭建双边、区域和国际合作平台，充分发挥世界互联网大会等主场平台作用，创建良好的营商环境，深化数字贸易、数字技术、数字服务等各领域合作。加强优质文化产品的数字化生产和网络化传播，推动各国、各地区、各民族网上文化交流互鉴。推进“数字丝绸之路”建设，深入拓展“丝路电商”合作，持续推进跨境电子商务综合试验区建设，着力打造开放、互利、共赢的数字生态。

**共享数字化发展成果。**加强同新兴市场国家、共建“一带一路”国家和广大发展中国家在网络基础设施建设、数字经济、网络安全、网络治理等方面的务实合作，打破信息壁垒，消除数字鸿沟，让更多发展中国家和人民共享互联网带来的发展机遇。积极探索数字技术在疫情防控、全球减贫、医疗教育等领域创新应用，推动数字科技协同创新，努力让数字化发展成果更好造福各国人民。（来源：《人民日报》（2021 年 11 月 05 日第 09 版））

## ➢ 法网密织 数据安全国家治理现新局

近年来，随着《网络安全法》和配套制度的相继实施，以及打击危害公民个人信息和数据安全违法犯罪各项措施相继推进，个人、组织数据安全意识明显提升，数据安全整体保障能力在一定程度上有所加强。

与此同时也应看到，当下国家整体数据安全形势依然严峻。中国对外开放不断打开新局

面，作为当前全球第一数据资源大国和全球第二大数字经济体，海量数据聚集，涉及政治、经济、文化、军事、生物、医疗、基因、人口、地理等各个领域，以及人民群众日常衣、食、住、行、销、乐等各个方面，区块链、人工智能、5G 等新技术新应用场景越来越丰富。同时要看到，各类数据拥有主体多样，处理活动愈加复杂，给数据安全、社会安全、国家安全、海外利益等带来的风险也不断发展与演变。

2021 年，《数据安全法》《个人信息保护法》和《关键信息基础设施安全保护条例》等法律法规相继施行，承继、衔接已实施多年的《国家安全法》《网络安全法》《密码法》《刑法》等，新时代数据安全法治保障整体合力形成，数据安全国家治理开启新篇章。

**一、各有侧重又密切关联的法律关系**

《国家安全法》《网络安全法》《个人信息保护法》与《数据安全法》等是国家数据安全法律体系的重要组成部分，共同构筑了中国数据安全整体框架和制度，形成保障数据安全保障的整体合力。

基于定位的不同，以上法律在规范内容方面各有侧重。

2015 年立足总体国家安全观重新制定的新《国家安全法》颁布实施，第 25 条明确，国家建设网络与信息安全保障体系，提升网络与信息安全保护能力。2017 年实施的《网络安全法》是中国网络安全领域的基础性、综合性法律，在数据安全之外还关注运行安全、信息安全，确立了包括网络安全等级保护制度、关键信息基础设施保护制度在内的一系列运行安全制度，强调网络空间总体安全。2021 年 9 月 1 日刚开始实施的《数据安全法》，则是中国数据安全领域的基础性、专门性法律。其基础性体现在将数据安全最高监管机构提升至中央国家安全领导机构，并明确建立国家数据安全工作协调机制，加强对数据安全工作的统筹，

推进《国家安全法》在数据安全领域的落地。其专门性体现在区别于《网络安全法》等综合性立法，聚焦数据安全领域突出问题，在《网络安全法》外明确诸多创设性、细化性一系列基本制度及数据处理规则原则，包括数据安全审查、数据交易安全、数据出口管制、数据对等措施、重要数据出境管理、执法数据调取配合、境外数据调取阻断、政务数据安全、数据安全应急处置等。《网络安全法》从网络运行安全、网络信息安全角度提出了数据管理要求，管理对象侧重个人信息和关键信息基础设施收集产生的重要数据，管理范围侧重数据采集、使用等特定环节。《数据安全法》将任何以电子或其他方式记录的信息全口径纳入数据范畴予以保护，并对数据的收集、存储、使用、加工、传输、提供、公开等全流程予以监管，确保数据的“有效保护”和“合法利用”两种状态。

与《数据安全法》《网络安全法》在关注个体权益保障的同时，更加关注国计民生、国家安全等宏观安全和公共利益不同，《个人信息保护法》则是一部权益保护法，旨在维护人民群众在网络空间的合法权益，以《民法典》所确立的个人信息民事权益为基础，确立了以个人“知情同意”为核心的数据处理规则，以及包括决定权、查阅复制权、可携带权、更正权、删除权等在内的一系列权利。

同时，法律之间又密切关联。网络安全与数据安全是“一体两面”的关系，维护网络安全的目的是保护数据和个人信息安全，保护数据和个人信息安全有赖于维护网络安全。

《数据安全法》将《网络安全法》确立的网络安全等级保护制度、关键信息基础设施安全保护制度延伸至数据领域，强化数据安全与网络安全的衔接。网络安全等级保护制度作为《网络安全法》确定的基础制度，在保护数据和个人信息安全方面发挥了重要作用。《数据安全法》将网络安全等级保护制度作为数据安全保护的基础制度，规定“利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务”。

同时，将重要数据出境安全管理制度与《网络安全法》中规定的关键信息基础设施数据出境安全评估制度相衔接，将数据安全与网络安全保护制度统筹设计、有效衔接。作为《网络安全法》重要配套行政法规的《关键信息基础设施安全保护条例》将维护数据的完整性、保密性和可用性作为关键信息基础设施安全保护的核心目标之一，并在第 15 条运营者职责中明确纳入“履行个人信息和数据安全保护责任，建立健全个人信息和数据安全保护制度”。

个人信息作为数据类型的一种，《个人信息保护法》第 9 条明确规定，个人信息处理者应当对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息安全，并在第五章“个人信息处理者的义务”中对义务作出了具体规定，包括制定内部管理制度和操作规程、

对个人信息实行分类管理、采取相应的加密、去标识化等安全技术措施、合规审计、个人信息保护影响评估等等。个人信息除受《个人信息保护法》规范外，其安全管理也同样需要遵守《数据安全法》的规定。同样的，《数据安全法》第 32 条规定了数据合法正当收集的原则，不得窃取或者其他非法方法获取数据，同时也规定，法律、行政法规对收集、使用数据目的、范围有规定的，应该在此范围内收集、使用。

值得一提的是，以上基本法律都无一例外有类似“违反本法规定，构成犯罪的，依法追究刑事责任”的专门规定。区别于《网络安全法》《数据安全法》《个人信息保护法》三部法律主要通过行政监管的方式强化安全保护，《刑法》和两高的司法解释是通过刑事手段保障数据安全和公民个人信息合法权益。

《网络安全法》《数据安全法》《个人信息保护法》中诸多规定与《刑法》已实现对接，违反其中规定，构成犯罪的将追究刑事责任。与数据安全相关的刑法罪名主要体现在第二百五十三条之一“侵犯公民个人信息罪”、第二百八十五条“非法获取计算机信息系统数据”、第二百八十六条“破坏计算机信息系统罪”、第二百八十六条之一“拒不履行信息网络安全管理义务罪”等。

司法解释方面则涉及 2011 年 6 月最高人民法院、最高人民检察院《关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》、2017 年 3 月最高人民法院、最高人民检察院《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》、2019 年 6 月最高人民法院、最高人民检察院《关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》等，为数据安全和公民个人信息犯罪明确了定罪量刑标准。

**二、法律的生命力在于实施**

目前，中国正式迎来《国家安全法》《数据安全法》《网络安全法》《个人信息保护法》《刑法》等法律并行的数据安全国家治理新阶段，规则细化等各方面的工作已在加速开启中。

2021 年 5 月 27 日，《数据安全管理条例》纳入国务院 2021 年度立法工作计划；2021 年 7 月 10 日，以落实《数据安全法》第 24 条数据安全审查制度为目的的《网络安全审查办法（修订草案征求意见）》向社会公开征求意见；2021 年 10 月 29 日，同时以《网络安全法》《数据安全法》《个人信息保护法》三法为上位制定依据，多年来备受各界关注的《数据出境安全评估办法（征求意见稿）》向社会公开征求意见。

值得注意的是，在穿透《网络安全法》《数据安全法》的网络安全等级保护制度和关键信息基础设施安全保护制度上，《数据安全法》将实施近 20 年的网络安全等级保护制度中的数据安全保障基因特征进一步凸显，明确了其在数据安全领域的基础支撑定位。在此背景下，

网络安全等级保护制度和关键信息基础设施安全保护制度必然也会顺应数据安全领域新形势需求，与时俱进，切实落实《数据安全法》赋予的使命和要求。包括但不限于推进规则指引，强化数据安全技术支撑；在网络安全等级保护、关键信息基础设施安全保护框架下推进数据安全保护技术标准制定出台，明确技术措施和必要的其他措施要求。

法律的生命力在于实施，法律的权威也在于实施。可以预见，不仅是规则细化完善，协同监管执法、法律竞合适用、执法规范建设、安全责任落实、主动合规遵循、违法犯罪打击、立法影响评估等都将成为考量数据安全法治实施效能的重要内容。（来源：财经 E 法 作者黄道丽）

## ➢ 统筹数字经济发展和数据安全 依法切实保护个人信息权益

**个人信息是重要的数字资产。**加强个人信息保护，规范个人信息的获取及使用，不仅事关个人权益维护，也关系数字经济健康发展。“十四五”规划和 2035 年远景目标纲要对加快推进数据安全、个人信息保护等领域基础性立法提出明确要求。民法典对个人信息保护作出了规定。今年 8 月，个人信息保护法通过，于 11 月正式施行。这是一部专门规定个人信息保护基本原则和制度的法律，有力增强了个人信息保护的系统性、权威性和针对性，对于统筹个人信息保护和数据合理利用，统筹数字经济发展和数据安全，加快推进数字中国建设具有重要意义。

**更好保护个人信息权益。**习近平总书记强调：“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，让人民群众在信息化发展中有更多获得感、幸福感、安全感。”随着新技术、新业态、新应用不断涌现，以电子等方式记录的个人信息大量产生。人民群众普遍关心个人信息安全，关注个人隐私能否得到保护。个人信息保护法坚持以人民为中心，全面调整、规范各类主体的个人信息处理活动，明确了包括知情权、决定权、删除权等在内的个人信息权益，更加严格地规定了敏感个人信息的范围和处理规则。对于社会反映强烈的胁迫用户同意处理个人信息、“大数据杀熟”和非法买卖、提供或者公开他人个人信息等违法行为明确了法律责任。这些规定有利于进一步健全和完善保护个人信息权益的体制机制。

**促进数字经济健康发展。**做大做强数字经济，需要不断发掘和释放各类信息资源的价值潜力、激活海量数据要素的生产潜能，这些离不开对个人信息的有效合理利用。个人信息保护法明确了个人信息的定义，不仅注重保护个人信息权益，预防和惩治侵害个人信息权益的行为，而且对个人信息的收集、存储、使用、加工、传输、提供、公开、删除等处理活动进行了全流程规范，明确要求处理个人信息应当在事先充分告知的前提下取得个人同意。考虑到个人信息处理场景的不同特点，还规定除取得个人同意之外其他可以合法处理个人信息的情形，如为订立、履行个人作为一方当事人的合同所必需等。这些制度的建立，为个人信息处理活动提供了明确指引，增强了市场对法律政策的明确预期，能够促进数据要素合理利用，有利于更好激发数字经济发展的活力。

**引导数据安全有序流动。**习近平总书记指出：“网络信息是跨国界流动的，信息流引领技术流、资金流、人才流，信息资源日益成为重要生产要素和社会财富，信息掌握的多寡成为国家软实力和竞争力的重要标志。”随着数字经济跨境发展，一些个人信息在全球范围流动，这给数据安全和数字经济发展带来了新的机遇和挑战。在网络安全法、数据安全法已对数据依法流动作出部分规范的基础上，个人信息保护法对个人信息的跨境流动作出相应制度安排，明确了向境外提供个人信息应当具备的条件，规定个人信息处理者向境外提供个人信息时必须履行的告知、安全评估等义务，还要求个人信息处理者未经主管机关批准不得向外国司法或者执法机构提供存储于中国境内的个人信息。这为向境外提供个人信息的情况提供了明确的行为规则。

个人信息保护法立足中国实际，借鉴国外有益经验，适应了人民群众对美好生活的需要。实施好个人信息保护法，必将进一步强化个人信息权益保障，增强我国数字经济竞争新优势，夯实建设数字中国和网络强国的法治基石。（来源：人民日报）

# 四、政府之声

## ➢ 工业和信息化部发布关于开展信息通信服务感知提升行动的通知

2021 年 11 月 1 日，工业和信息化部印发《关于开展信息通信服务感知提升行动的通知》（以下简称《通知》），决定 2021 年 11 月至 2022 年 3 月，开展信息通信服务感知提升行动（简称“524”行动）。

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开展信息通信服务感知提升行动的通知

发文字号：工信部信管函〔2021〕292号

成文日期：2021-11-01　　发布日期：2021-11-01

发布机构：信息通信管理局　　分　　类：信息通信管理

**工业和信息化部关于开展信息通信服务感知提升行动的通知**

工信部信管函〔2021〕292号

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、中国广播电视网络集团有限公司，相关互联网企业，中国信息通信研究院：

《通知》将聚焦影响用户感知的信息通信服务环节，推动实现服务举措“五优化”（即优化资费套餐设置展示方式、双千兆服务宣传方式、隐私政策和权限调用展示方式、APP 开屏弹窗信息展示方式、网盘类服务提供方式），建立个人信息保护“双清单”（即建立已收集个人信息清单、与第三方共享个人信息清单），实现服务能力“四提升”（即提升跨区域通办能力、携号转网服务能力、响应能力、APP 关键责任链个人信息保护能力）。明确到 2022 年 3 月底，信息通信行业综合服务明显改善，用户获得感、幸福感和安全感进一步提升。

《通知》明确要求在 2021 年 12 月底前，基础电信企业应及时提醒用户套餐内流量使用情况，电信企业应合理设置套餐外流量单价；在同一网络条件下，网盘类服务企业向免费用户提供的上传和下载的最低速率应确保满足基本的下载需求。（来源：工业和信息化部）

- **《工业和信息化部关于开展信息通信服务感知提升行动的通知》全文：**
- https://www.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2021/art_046fc75a9c12418b927c3cbe5963

aaf1.html

## ➢ 中央网络安全和信息化委员会印发《提升全民数字素养与技能行动纲要》

2021 年 11 月 5 日，中央网络安全和信息化委员会印发《提升全民数字素养与技能行动纲要》（以下简称《行动纲要》），对提升全民数字素养与技能作出安排部署。

《行动纲要》指出，提升全民数字素养与技能，是顺应数字时代要求，提升国民素质、促进人的全面发展的战略任务，是实现从网络大国迈向网络强国的必由之路，也是弥合数字鸿沟、促进共同富裕的关键举措。要把提升全民数字素养与技能作为建设网络强国、数字中国的一项基础性、战略性、先导性工作，切实加强顶层设计、统筹协调和系统推进，促进全民共建共享数字化发展成果，推动经济高质量发展、社会高效能治理、人民高品质生活、对外高水平开放。

《行动纲要》强调，要以习近平新时代中国特色社会主义思想为指导，全面贯彻党的十九大和十九届二中、三中、四中、五中全会精神，深入学习贯彻习近平总书记在庆祝中国共产党成立 100 周年大会上的重要讲话精神，立足新发展阶段，贯彻新发展理念，构建新发展格局，坚持以人民为中心，落实高质量发展要求，以满足人民日益增长的美好生活需要、促进人的全面发展和全体人民共同富裕为根本目的，坚持深化供给侧结构性改革，以创新驱动、高质量供给引领新需求，着力发展数字基础设施、优化数字资源供给、完善数字环境保障，着力构建覆盖全民、城乡融合、公平一致、可持续、有韧性的数字素养与技能发展培育体系，

着力拓展全民数字生活、数字学习、数字工作、数字创新四大场景，激发全民建设网络强国和数字中国的积极性、主动性、创造性，提升全民数字化适应力、胜任力、创造力，增强人力资本积累，拓展人口质量红利，厚植创新发展优势，为全面建设社会主义现代化国家提供强大的数字动力支撑和坚实的人力资源基础。

《行动纲要》提出，坚持以人为本、普惠共享，统筹谋划、系统推进，深化改革、协调发展，正确导向、保障安全。到 2025 年，全民数字化适应力、胜任力、创造力显著提升，数字素养与技能提升发展环境显著优化，基本形成渠道丰富、开放共享、优质普惠的数字资源供给能力。初步建成全民终身数字学习体系，老年人、残疾人等特殊群体数字技能稳步提升，数字鸿沟加快弥合。劳动者运用数字技能的能力显著提高，高端数字人才队伍明显扩大。全民运用数字技能实现智慧共享、和睦共治的数字生活，数字安全保障更加有力，数字道德伦理水平大幅提升。展望 2035 年，基本建成数字人才强国，全民数字素养与技能等能力达到更高水平，高端数字人才引领作用凸显，数字创新创业繁荣活跃，为建成网络强国、数字中国、智慧社会提供有力支撑。

《行动纲要》围绕七个方面部署了主要任务，一是丰富优质数字资源供给，二是提升高品质数字生活水平，三是提升高效率数字工作能力，四是构建终身数字学习体系，五是激发数字创新活力，六是提高数字安全保护能力，七是强化数字社会法治道德规范。围绕主要任务和薄弱环节，《行动纲要》还设立了数字社会无障碍和适老化改造提升工程等六个重点工程。

《行动纲要》从加强组织领导、加大政策支持、开展试点示范、强化考核评估、加强宣传推广、深化国际合作等六个方面保障实施，确保目标任务落到实处。（来源：网信中国）

- **《提升全民数字素养与技能行动纲要》**
- **全文：**http://www.cac.gov.cn/2021-11/05/c_1637708867754305.htm

## ➢ 国家网信办对《网络数据安全管理条例（征求意见稿）》公开征求意见

2021 年 11 月 14 日，国家互联网信息办公室发布《网络数据安全管理条例（征求意见稿）》（以下简称《条例》），面向社会公开征求意见。《条例》旨在落实三大上位法关于数据安全管理的规定，规范网络数据处理活动，保护个人、组织在网络空间的合法权益，维护国家安全和公共利益。

《条例》明确了国家建立数据分类分级保护制度。按照数据对国家安全、公共利益或者个人、组织合法权益的影响和重要程度，将数据分为一般数据、重要数据、核心数据，不同级别的数据采取不同的保护措施。对个人信息和重要数据进行重点保护，对核心数据实行严格保护。一百万以上的个人信息按重要数据级别保护，并定义了重要数据范畴。分类分级保护制度的建立和实施，是向数据安全精细化管理迈出的重要一步。

《条例》明确了数据处理者开展哪些活动需要申报网络安全审查。特别是掌握大量关系国家安全、经济发展、公共利益的数据资源或大量个人信息数据的企业，其组织变动或涉及境外的经营活动，可能影响国家安全的，均应主动申报。

《条例》从多个方面强化了个人信息保护：针对个人信息处理知情权环节，详细列出了个人信息处理规则的内容；针对个人信息处理决定权，明确了“单独同意”的含义；针对个人信息的查阅、复制、更正、补充、限制处理、删除其个人信息等权利，要求在十五个工作日予以答复；明确了个人信息转移权的行使条件。

《条例》明确将重要数据锚定在“危害国家安全、公共利益的数据”上，通过强化重要数据保护，确立了国家对重要数据的最终控制权地位。具体要求包括重要数据的行政备案；重要数据的强制性安全评估；数据处理者共享、交易、委托处理重要数据时，应当征得主管部门同意等。《条例》规定处理重要数据的系统应当满足三级以上网络安全等级保护和关键信息基础设施安全保护要求，核心数据则从严保护，进一步凸显密码对数据保护的基石地位。

《条例》明确了跨境提供数据的条件，数据出境安全评估的情形，数据处理者向境外提供数据应当履行的义务，数据出境安全报告的要求，建立数据跨境安全网关等。

《条例》对互联网平台运营者提出了具体规范，将其可能影响国家安全的数据处理行为纳入网络安全审查范畴，对平台规则、隐私政策修订等提出增强要求。特别是规范互联网平台运营者不得利用数据以及平台规则等从事的活动，是对“大数据杀熟”、“爬虫”自动化工具、算法透明度解释等热点问题的回应。《条例》还要求通过委托第三方审计方式，每年对平台数据安全情况、平台规则和自身承诺的执行情况、个人信息保护情况、数据开发利用情况等进行年度审计，并披露审计结果。可见，《条例》全面强化了对大型互联网平台的数据安全治理。

《条例》明确了国家建立数据安全审计制度。数据处理者应当委托数据安全审计专业机构定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。主管、监管部门组织开展对重要数据处理活动的审计，重点审计数据处理者履行法律、行政法规规定的义务等情况。

数据安全关系到经济发展、公共利益和国家安全。《条例》的发布，是对网络数据安全管理具体方式方法的进一步明确，是对政企机构、互联网平台等数据处理者或运营方围绕数据相关活动或行为的进一步规范，也是对国家数据主权的进一步巩固。广大政企机构、互联网平台需要顺应行业发展大势，主动拥抱监管，以正确的方式、科学的手段加强数据处理、应用和运营过程中的安全管理，包括数据分类分级、数据安全治理、数据安全共享、数据脱敏、数据防泄漏、数据活动全流程监管溯源等，建立完备、合规的数据安全防护和管理体系。

（来源：中国网信网）

- **《网络数据安全管理条例（征求意见稿）》**
- **全文：**http://www.cac.gov.cn/2021-11/14/c_1638501991577898.htm

## ➢ 新《中华人民共和国审计法》2022 年 1 月 1 日起施行

2021 年 10 月 23 日，十三届全国人大常委会第三十一次会议通过《全国人民代表大会常务委员会关于修改〈中华人民共和国审计法〉的决定》，国家主席习近平签署第 100 号主席令予以公布，自 2022 年 1 月 1 日起施行。

《中华人民共和国审计法》（以下简称《审计法》）的修订和颁布施行，是我国审计事业发展进程中的一件大事，有利于审计机关依法全面履行审计监督职责，规范审计行为，提高审计质量，防范审计风险，推动新时代审计工作高质量发展，更好发挥审计在党和国家监督

体系中的重要作用，推进国家治理体系和治理能力现代化。

原《审计法》共 54 条，此次修订中，修改 34 条，增加 7 条，合并 1 条，修订后共 60 条。新修订《审计法》在保持原《审计法》框架结构和基本内容不变的基础上，主要在健全审计监督机制、完善审计监督职责、优化审计监督手段、规范审计监督行为、强化审计查出问题整改、加强审计机关自身建设等方面作了修订。（来源：中国人大）

- **《中华人民共和国审计法》全文：**
- http://www.npc.gov.cn/npc/c30834/202110/940943e73fff48b2adffd851b35a2f70.shtml

# 五、本期重要漏洞实例

## ➢ Microsoft 发布 2021 年 10 月安全更新

发布日期：2021-11-11

更新日期：2021-11-11

描述：11 月 11 日，微软发布了 2021 年 11 月份的月度例行安全公告，修复了其多款产品存在的 55 个安全漏洞。受影响的产品包括：3D Viewer、Azure、Azure RTOS、Azure Sphere、Microsoft Dynamics、Microsoft Edge (Chromium-based)、Microsoft Edge (Chromium-based) in IE Mode、Microsoft Exchange Server、Microsoft Office、Microsoft Office Access、Microsoft Office Excel、Microsoft Office SharePoint、Microsoft Office Word、Microsoft Windows、Microsoft Windows Codecs Library、Power BI、Role: Windows Hyper-V、Visual Studio、Visual Studio Code、Windows Active Directory、Windows COM、Windows Core Shell、Windows Cred SSProvider Protocol、Windows Defender、Windows Desktop Bridge、Windows Diagnostic Hub、Windows Fastfat Driver、Windows Feedback Hub、Windows Hello、Windows Installer、Windows Kernel、Windows NTFS、Windows RDP、Windows Scripting 和 Windows Virtual Machine Bus。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。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-2021-26443 | **Microsoft Virtual Machine Bus (VMBus) 远程代码执行漏洞** | 严重<br>远程代码执行 | Server, version 20H2<br>Server, version 2004<br>Windows 10<br>Windows 11<br>Server 2022<br>Server 2019 |
| CVE-2021-3711 | **SM2 解密缓冲区溢出漏洞** | 严重<br>缓冲区溢出 | Visual Studio 2019<br>Visual Studio 2017 |
| CVE-2021-38666 | **Remote Desktop Client 远程代码执行漏洞** | 严重<br>远程代码执行 | Windows RT 8.1<br>Server 2012<br>Server 2008 |
| CVE-2021-42292 | **Microsoft Excel 安全功能绕过漏洞** | 重要<br>安全功能绕过 | Office LTSC for Mac 2021<br>365 Apps for Enterprise<br>Office 2019 for Mac<br>Office LTSC 2021<br>Office 2019<br>Office 2016<br>Office 2013<br>Excel 2013<br>Excel 2016 |
| CVE-2021-42321 | **Microsoft Exchange Server 远程代码执行漏洞** | 重要<br>远程代码执行 | Exchange Server 2019<br>Exchange Server 2016 |

| | | | |
|---|---|---|---|
| CVE-2021-42298 | **Microsoft Defender 远程代码执行漏洞** | 中等<br>远程代码执行 | Malware Protection Engine |
| CVE-2021-42279 | **Chakra Scripting Engine 内存破坏漏洞** | 中等<br>远程代码执行 | Server, version 2004<br>Server 2016<br>Windows 10<br>Server 2019 |
| CVE-2021-42316 | **Microsoft Dynamics 365 (on-premises)远程代码执行漏洞** | 重要<br>远程代码执行 | Dynamics 365 |

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

## ➢ IBM Tivoli Key Lifecycle Manager 信息泄露漏洞

**发布日期**：2021-11-23
**更新日期**：2021-11-25
**受影响系统**：
IBM Tivoli Key Lifecycle Manager 4.1
IBM Tivoli Key Lifecycle Manager 4.0
IBM Tivoli Key Lifecycle Manager 3.0.1
IBM Tivoli Key Lifecycle Manager 3.0
**描述**：

---

CVE(CAN) ID: CVE-2021-38980
IBM Tivoli Key Lifecycle Manager（TKLM）是美国 IBM 公司的一套密钥生命周期管理软件。该软件为存储设备提供密钥存储、密钥维护和密钥生命周期管理等功能。
IBM Tivoli Key Lifecycle Manager 3.0, 3.0.1, 4.0 和 4.1 版本存在信息泄露洞。远程攻击者可利用该漏洞获取敏感信息以进一步攻击系统。
链接：https://www.ibm.com/support/pages/node/6518326
**建议**：

---

厂商补丁：
IBM
---
IBM 已经为此发布了一个安全公告（6518326）以及相应补丁：
6518326：Security Bulletin: Application error in IBM Security Guardium Key Lifecycle Manager (CVE-2021-38980)
链接：https://www.ibm.com/support/pages/node/6518326

## ➢ Adobe Acrobat Reader DC 堆栈缓冲区溢出漏洞

**发布日期：**2021-05-11
**更新日期：**2021-11-23
**受影响系统：**
Adobe Acrobat Reader DC <= 2021.001.20150
Adobe Acrobat Reader DC <= 2020.001.30020
Adobe Acrobat Reader DC <= 2017.011.30194
**描述：**

---

CVE(CAN) ID: CVE-2021-28560
Adobe Acrobat 是一套 PDF 文件编辑和转换工具。Adobe Acrobat Reader 是一款 PDF 查看器。该软件用于打印，签名和注释 PDF。
Adobe Acrobat Reader DC 存在堆栈缓冲区溢出漏洞。攻击者可利用该漏洞执行任意代码。
链接：https://helpx.adobe.com/security/products/acrobat/apsb21-29.html
**建议：**

---

厂商补丁：
Adobe
Adobe 已经为此发布了一个安全公告（APSB21-29）以及相应补丁：
APSB21-29：Security update available for Adobe Acrobat and Reader | APSB21-29
链接：https://helpx.adobe.com/security/products/acrobat/apsb21-29.html

## ➢ Desdev DedeCMS 跨站脚本漏洞

**发布日期：**2021-10-22
**更新日期：**2021-11-19
**受影响系统：**Desdev DedeCMS 7.5 SP2
**描述：**

---

CVE(CAN) ID: CVE-2020-36496
Desdev DedeCMS（织梦内容管理系统）是中国卓卓网络（Desdev）公司的一套基于 PHP 的开源内容管理系统（CMS）。该系统具有内容发布、内容管理、内容编辑和内容检索等功能。
DedeCMS 7.5 SP2 版本中的组件 sys_admin_user_edit.php 存在跨站脚本漏洞。攻击者可利用该漏洞通过 filename、mid、userid 和 templet 参数导致跨站脚本执行。
**建议：**

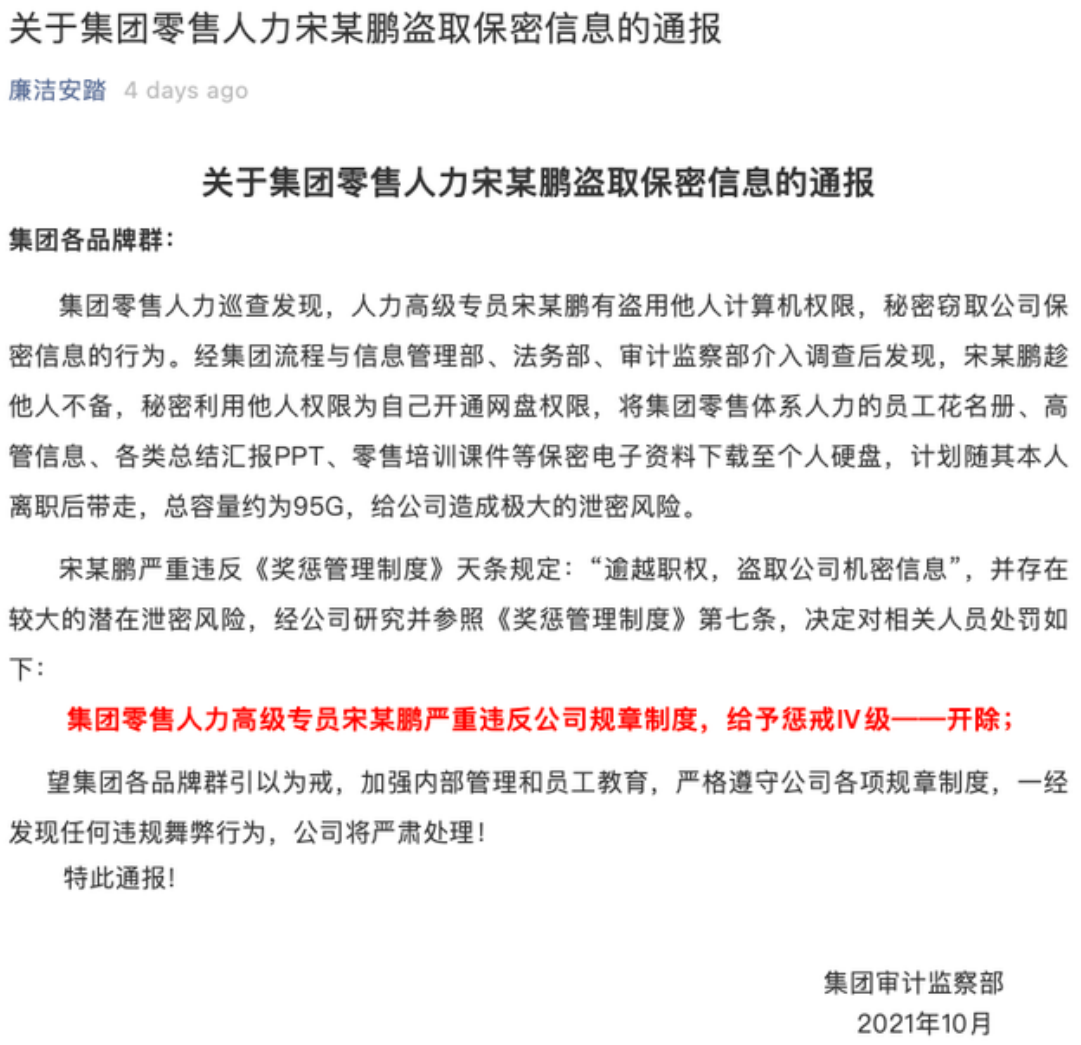
---

厂商补丁：
Desdev
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：
http://www.dedecms.com/products/dedecms/downloads/

# 六、本期网络安全事件

## ➢ 安踏集团通报一员工秘密窃取公司 95GB 保密信息被开除

2021 年 10 月 25 日，“廉洁安踏”微信公众号消息，安踏集团审计监察部日前发布通报称，集团零售人力巡查发现，人力高级专员宋某鹏有盗用他人计算机权限，秘密窃取公司保密信息的行为，严重违反公司规章制度，给予惩戒Ⅳ级——开除。



关于集团零售人力宋某鹏盗取保密信息的通报

廉洁安踏 4 days ago

**关于集团零售人力宋某鹏盗取保密信息的通报**

**集团各品牌群：**

集团零售人力巡查发现，人力高级专员宋某鹏有盗用他人计算机权限，秘密窃取公司保密信息的行为。经集团流程与信息管理部、法务部、审计监察部介入调查后发现，宋某鹏趁他人不备，秘密利用他人权限为自己开通网盘权限，将集团零售体系人力的员工花名册、高管信息、各类总结汇报PPT、零售培训课件等保密电子资料下载至个人硬盘，计划随其本人离职后带走，总容量约为95G，给公司造成极大的泄密风险。

宋某鹏严重违反《奖惩管理制度》天条规定：“逾越职权，盗取公司机密信息”，并存在较大的潜在泄密风险，经公司研究并参照《奖惩管理制度》第七条，决定对相关人员处罚如下：

**集团零售人力高级专员宋某鹏严重违反公司规章制度，给予惩戒Ⅳ级——开除；**

望集团各品牌群引以为戒，加强内部管理和员工教育，严格遵守公司各项规章制度，一经发现任何违规舞弊行为，公司将严肃处理！

特此通报！

集团审计监察部

2021年10月

“宋某鹏趁他人不备，秘密利用他人权限为自己开通网盘权限，将集团零售体系人力的员工花名册、高管信息、各类总结汇报 PPT、零售培训课件等保密电子资料下载至个人硬盘，计划随其本人离职后带走，总容量约为 95G，给公司造成极大的泄密风险。”安踏集团在通报中称。（来源：互联网综合整理）

## ➢ 多伦多交通委员会承认数万员工个人信息被泄漏

2021 年 11 月 11 日，多伦多交通委员会（TTC）近日承认，由于上个月其系统受到勒索软件的攻击，数万名员工的个人信息可能已经被泄露。TTC 负责运营多伦多公交车、地铁、有轨电车和辅助交通系统等等，在近日发布的声明中表示，泄漏的数据包括 25000 名离职和现职员工的姓名、地址和身份证号码等。该机构说，它正在继续调查是否有“少数”客户和供应商也受到了影响。

该机构补充说，虽然“没有证据”表明任何信息被滥用，但它正在通知那些受影响的个人，并将向他们提供信用监测和身份盗窃保护。TCC 还建议员工给他们的银行打电话，提醒他们注意安全漏洞。

**TTC 首席执行官 Rick Leary 说：**10 月 29 日的勒索软件攻击导致了车辆跟踪和“next bus”系统的瘫痪，以及 Wheel-Trans 在线预订系统的宕机。他补充说，这次事件导致 TTC 的一些服务器被加密和锁定。虽然大多数面向客户的系统已经恢复，但 TTC 的内部电子邮件系统仍然处于离线状态。

**Leary 表示：**我想代表整个组织，向可能受到影响的所有人表达我对发生这种情况的深深遗憾。我不会忘记，像我们这样的组织被赋予了大量的个人信息，我们必须尽最大努力保

护这些信息。在未来几周，我们将继续重建其余受影响的服务器和内部服务，如重新建立外部电子邮件功能。但事实上，根据其他组织的经验，这可能需要一些时间。（来源：cnBeta）

## ➢ 非法获取明星航班信息 两粉丝侵犯公民个人信息获刑

2021 年 11 月 16 日，非法获取明星航班信息用以追星的“粉丝”刘某某、王某某，近日被北京市朝阳区人民法院以侵犯公民个人信息罪依法判处拘役 5 个月、缓刑 5 个月，拘役 4 个月、缓刑 4 个月。

今年 6 月，首都机场公安局民警发现有“粉丝”在首都机场三号航站楼聚集尾随跟拍某明星乘机，对机场正常秩序造成严重影响。经查，“粉丝”刘某某、王某某不仅有扰乱公共场所秩序、侵犯隐私的行为，同时还非法获取 100 余条明星身份及乘坐航班信息，并将部分信息在“粉丝”微信群中转发。

首都机场公安局对二人违法行为依法作出行政拘留处罚，并对其涉嫌侵犯公民个人信息犯罪行为进行调查取证后，采取刑事强制措施，移送检察机关审查起诉。近日，朝阳法院作出判决，刘某某、王某某分别被以侵犯公民个人信息罪依法判处拘役 5 个月、缓刑 5 个月，拘役 4 个月、缓刑 4 个月。

**首都机场警方提示：**今年 1 月 1 日实施的《民法典》、11 月 1 日实施的《个人信息保护法》，都明确规定了公民个人信息受法律保护。《刑法》、《治安管理处罚法》对侵犯公民个人

信息应受的刑事、行政处罚作出明文规定。“粉丝”追星本无可厚非，但切记不得逾越法律底线，否则必将受到法律的制裁。（来源：北京日报）

## ➢ 特斯拉“断网”让数百车主“被锁车外” 马斯克发推道歉

2021 年 11 月 20 日,据英国广播公司(BBC)报道：特斯拉汽车应用程序服务中断，导致全球多地车主无法通过其手机上的应用程序打开车门或启动汽车。数十名特斯拉车主在社交媒体上抱怨，他们在手机应用程序上收到错误提示“故障代码 500”，无法连接到自己的汽车。

英国《卫报》称，来自美国、加拿大的车主率先报告这一问题，欧洲和亚洲的车主也发现了类似状况。据网络状况监控网站 DownDetector 的数据显示，在美东时间 19 日 16 时 40 分左右，约 500 名用户报告该问题，而到当日 21 时 20 分左右，仍有 60 份问题报告。

据美国有线电视新闻网(CNN)20 日报道，很多车主习惯用手机上的特斯拉应用程序打开车门、启动发动机。不过，特斯拉也为每位车主配备实体钥匙卡，而且在提前进行相关设置后，在脱离网络服务器的情况下也能使用手机应用启动车辆。美国印第安纳州的特斯拉车主扎卡里·基弗称，此次在特斯拉应用程序服务中断时，他在离家约 1 个小时车程的地方。他大约一个月前丢了车钥匙，还换了新手机，因此这次服务中断让他被困在车外好

几个小时，最后只能打电话叫拖车。所幸在拖车到达前，特斯拉应用程序又开始工作了。基弗告诉 CNN，特斯拉的客户服务似乎并没有特别有帮助，“我很失望，他们似乎根本不在乎。”

在发现该问题后，**特斯拉首席执行官马斯克 19 日在推特上回复一名报告该问题的韩国车主称：**“现在应该在恢复正常。看来我们无意中增加了网络流量冗余。很抱歉，我们将采取措施确保此类事件不再发生。”英国伯明翰大学商学院教授戴维·贝利也是此次遭遇故障的特斯拉车主。他对 BBC 称，“某种程度上，特斯拉是自己成功的受害者。其鼓励客户使用它创造的尖端技术，而有时这也会出错。”（来源：环球时报 ）

## ➢ 快递员伙同他人非法获取公民个人信息，出售 10000 条被追责

2021 年 11 月 23 日，现实生活中，相信不少人都遇到过垃圾短信、各种推销电话、电信诈骗等。那到底是谁出卖了你的个人信息?

《中华人民共和国个人信息保护法》规定，任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。公民个人信息受法律保护。然而，就有些人铤而走险。合肥一快递人员，伙同他人非法获取公民个人信息 2 万多条，并将其中的 10000 条出售给他人，涉嫌侵犯公民个人信息罪，目前两人均被追究刑事责任。

2020 年 3、4 月间，26 岁的刘某某、27 岁的陈某某准备共同实施非法获取公民个人信

息并出售。2020 年 7 月初，刘某某应聘到蜀山区一快递网点工作，期间使用快递网点的移动终端(巴枪)登录快递员工号，扫描快递单号获取公民个人信息，共计查询 22972 条公民个人信息。

之后，刘某某将获取的公民个人信息发送给陈某某，陈某某将其中的 10000 条公民个人信息出售给赵某某。2020 年 9 月和 11 月，刘某某、陈某某两人分别被合肥市蜀山警方抓获归案，归案后均如实供述了案件事实。

**蜀山区人民检察院认为：**刘某某、陈某某违反国家有关规定，非法获取公民个人信息 22972 条，并将其中的 10000 条出售给他人，两人的行为均已触犯了《中华人民共和国刑法》第 253 条之一，犯罪事实清楚，证据确实、充分，应当以侵犯公民个人信息罪分别追究其刑事责任。被告人刘某某、陈某某均认罪认罚，依据《中华人民共和国刑事诉讼法》第十五条的规定，可以从宽处理;经抓获归案后均如实供述了案件事实，属坦白，依法可以从轻处理。因此，建议分别判处有期徒刑 1 年，并处罚金。（来源：先点融媒）

## ➢ 连续两天大规模宕机 星展银行遭遇 11 年来最大故障

2021 年 11 月 25 日，东南亚地区最大银行——新加坡星展银行出现了服务大规模中断的情况。据外媒报道，自当地时间 11 月 23 日上午起，星展银行的网上银行服务开始出现大规模中断，遭到数千名客户投诉，而在 11 月 24 日紧急恢复服务几小时后再次遭遇中断。外媒称，星展银行方面表示，该行将这两天服务中断归咎于“访问控制服务器”的故障。该行表示，这导致许多客户无法登录其账户。新加坡监管机构已指示该银行调查持续两天的问题的原因。“由于访问控制服务器出现问题，导致客户在两天内无法登录其账户和访问其数字服务。”星展银行补充表示，该银行已与其“第三方工程提供商”合作解决问题。

据了解，11 月 23 日早上，一些客户在登录或访问星展银行的在线和移动服务时遇到困难，彼时，该行出现的服务中断首次被报道。最初，星展银行并未公布这一问题的细节，不过在其 Twitter 和 Facebook 官方社交平台上，该行称已经意识到客户“在访问银行服务时时断时续”。

**星展银行在当地时间周三凌晨发布的最新消息中表示：**问题已得到解决，服务已恢复。然而，客户再次投诉该行线上服务仍出现了难以访问的问题，银行在当天晚些时候也

再度承认问题的第二次发生。 星展银行有关负责人表示，该行一直在与第三方工程提供商一道解决问题，该行意识到其许多客户仍然无法访问其服务，并正在制定解决方案。 不过该行表示，客户的存款和资金是安全的，可以通过分行或电话银行继续满足金融服务需求。并表示，已将所有分行的银行服务延长了两个小时。

**监管表态**

在星期三的一份声明中，新加坡货币管理局(MAS)表示，在 DBS 完成评估后，将考虑采取适当行动。“这是一个严重的故障事件，MAS 希望 DBS 进行彻底调查，以确定根本原因并实施必要的补救措施，”MAS 银行和保险部助理董事总经理 Marcus Lim 表示。该行业监管机构表示，已收到星展银行关于其访问控制服务器的通知，并正在就此问题与该银行进行跟进。

Lim 表示，预计所有金融机构都将建立“系统和流程”，以确保向客户提供“一致的可用性”。本月初，星展银行宣布计划明年投资 3 亿新加坡元(合 2.222 亿美元)，以增强其支持银行财富和零售产品及服务的数字和智能银行能力。该公司表示，在这方面的努力将提高其数字和物理接触点的个性化用户体验。

**值得一提的是，近期，多国金融监管机构加强对于金融机构出现系统故障的纠正措施。**

据日经新闻报道，日本财务省将对瑞穗银行采取纠正措施。报道称，今年 9 月，瑞穗银行在外汇交易处理滞后时的应对违反《外汇法》规定的反洗钱程序。在瑞穗银行此次的

故障中，外汇交易系统出现问题，可能是存有关于犯罪和恐怖活动洗钱汇款前的检查工作缺陷。 报道称，尽管检查后，监管并没有发现非法汇款的证据，但由于瑞穗银行是日本最大的银行之一，对支付系统负有责任，日本财务省因此决定对其采取纠正措施。（来源：央视财经）


信息安全意识产品服务

021-33663299