国盟信息安全通报

2021 年 06 月 30 日第 240 期

全国售后服务中心

国盟信息安全通报

（第 240 期）

国际信息安全学习联盟

2021 年 6 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 605 个，其中高危漏洞 168 个、中危漏洞 363 个、低危漏洞 74 个。漏洞平均分值为 5.59。本周收录的漏洞中，涉及 0day 漏洞 327 个（占 54%），其中互联网上出现“Liftoff GateOne 任意命令执行漏洞、White Shark System（WSS）跨站请求伪造漏洞”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 3577 个，与上周（2579 个）环比增加 39%。

主要内容

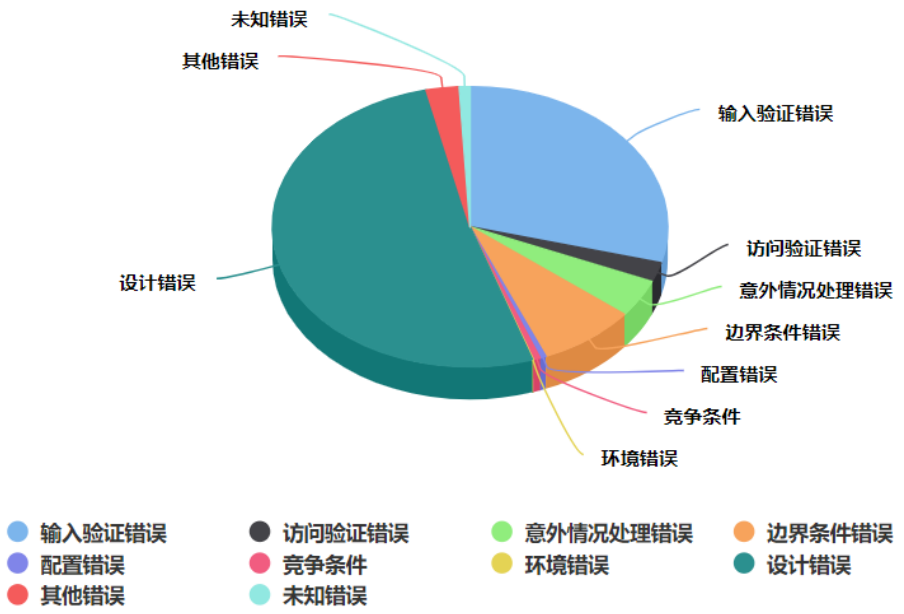
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

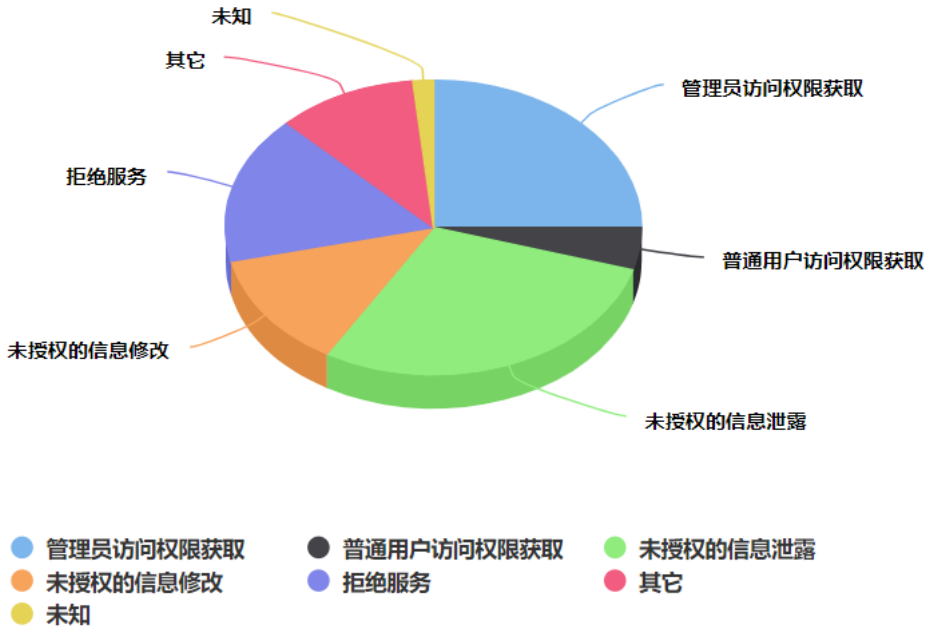
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 605 个，其中高危漏洞 168 个、中危漏洞 363 个、低危漏洞 74 个。漏洞平均分值为 5.59。本周收录的漏洞中，涉及 0day 漏洞 327 个（占 54%），其中互联网上出现“Liftoff GateOne 任意命令执行漏洞、White Shark System（WSS）跨站请求伪造漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 3577 个，与上周（2579 个）环比增加 39%。

二、安全漏洞增长数量及种类分布情况

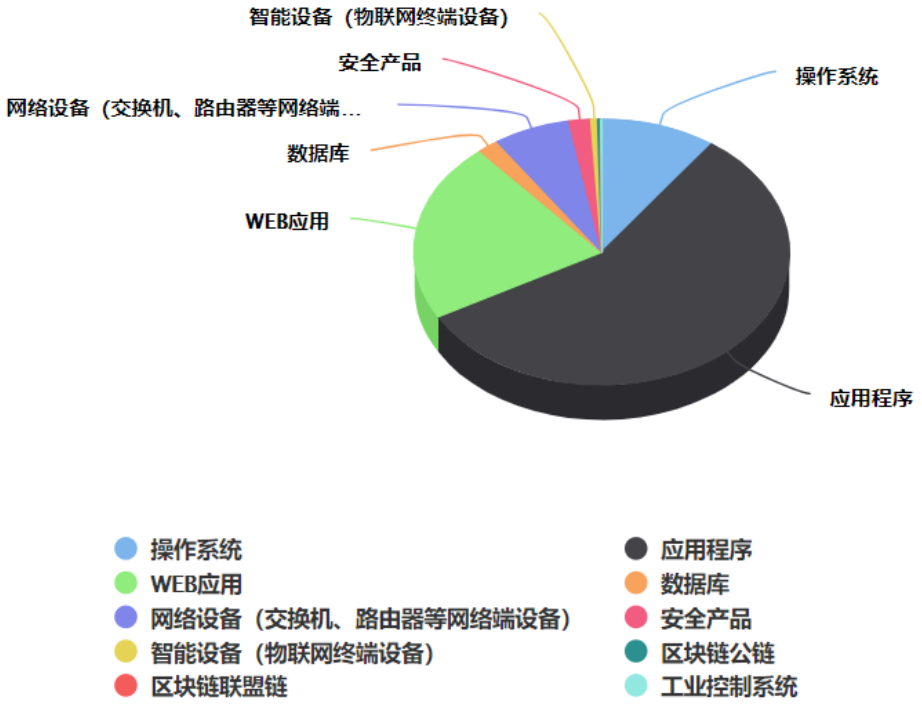
➢ 漏洞产生原因（2021 年 6 月 1 日—2021 年 6 月 30）



➢ 漏洞引发的威胁（2021 年 6 月 1 日—2021 年 6 月 30）



➢ 漏洞影响对象类型（2021 年 6 月 1 日—2021 年 6 月 30）



三、安全产业动态

➢ 《数据安全法》为全球数据安全治理贡献中国智慧和中国方案

随着信息技术和人类生产生活交汇融合，各类数据迅猛增长、海量聚集，对经济发展、人民生活产生了重大而深刻的影响。数据安全已成为事关国家安全与经济社会发展的重大问题。党中央高度重视，就加强数据安全工作和促进数字化发展作出一系列重要部署。按照党中央决策部署，贯彻总体国家安全观的要求，全国人大常委会积极推动数据安全立法工作。经过三次审议，2021 年 6 月 10 日，《数据安全法》经十三届全国人大常委会第二十九次会议通过并正式发布，将于 2021 年 9 月 1 日起施行。

作为我国数据安全领域的基础性法律，《数据安全法》主要有以下三个特点：一是坚持安全与发展并重。设专章对支持促进数据安全与发展的措施作了规定，保护个人、组织与数据有关的权益，提升数据安全治理和数据开发利用水平，促进以数据为关键生产要素的数字经济发展；二是加强具体制度与整体治理框架的衔接。从基础定义、数据安全管理、数据分类分级、重要数据出境等方面，进一步加强与《网络安全法》等法律的衔接，完善我国数据治理法律制度建设；三是回应社会关切。加大数据处理违法行为处罚力度，建设重要数据管理、行业自律管理、数据交易管理等制度，回应实践问题及社会关切。

《数据安全法》完善了国家数据安全工作体制机制，规定中央国家安全领导机构负责国家数据安全工作的决策和议事协调等职责，并提出建立国家数据安全工作协调机制。在网络

数据安全工作方面，专门明确国家网信部门依照本法和有关法律、行政法规的规定，负责统筹协调网络数据安全和相关监管工作。

《数据安全法》重点确立了数据安全保护的各项基本制度，完善了数据分类分级、重要数据保护、跨境数据流动和数据交易管理等多项重要制度，形成了我国数据安全的顶层设计。

《数据安全法》对数据分类分级制度进行了探索。《数据安全法》第二十一条规定，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，并明确加强对重要数据的保护，对关系国家安全、国民经济命脉、重要民生、重大公共利益等内容的国家核心数据，实行更加严格的管理制度。《数据安全法》针对重要数据在管理形式和保护要求上提出了严格和明确的保护制度。在管理形式上，《数据安全法》采用目录管理的方式，明确将“确定重要数据目录”纳入国家层面管理事项，国家数据安全工作协调机制统筹协调有关部门制定重要数据目录。而各地区、各部门制定本地区、本部门及相关行业、领域的重要数据具体目录，有利于形成国家与各地方、各部门管理权限之间的合理协调机制，推动重要数据统一认定标准的建立。在保护要求上，《数据安全法》在一般保护之外，强化了重要数据、核心数据的保护要求。一是规定数据处理者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；二是规定了重要数据处理者“明确数据安全负责人和管理机构”的义务，要求重要数据处理者在内部作出明确的责任划分，落实数据安全保护责任；三是规定了重要数据处理者进行风险评估的要求，重要数据处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等。

《数据安全法》建立数据安全风险评估、报告、信息共享、监测预警和应急处置机制，通过对数据安全风险信息的获取、分析、研判、预警以及数据安全事件发生后的应急处置，实现数据安全事前、事中和事后的全流程保障。《数据安全法》第二十二条规定：“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。国家数据安全工作协调机制统筹协调有关部门加强数据安全风险信息的获取、分析、研判、预警工作。”第二十九条规定：“开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施……”从制度衔接上看，数据安全风险评估、报告、信息共享、监测预警机制是国家安全制度的组成部分。《国家安全法》第四章第三节建立了风险预防、

评估和预警的相关制度，规定国家制定完善应对各领域国家安全风险预案。数据安全风险评估、报告、信息共享、监测预警机制是《国家安全法》规定的风险预防、评估和预警相关制度在数据安全领域的具体落实。从保护阶段上看，数据安全风险评估、报告和信息共享构成了数据安全保护的事前保护义务，监测预警机制构成了数据安全保护的事中保护义务，数据安全事件的应急处置机制形成了对数据安全的事后保护。

《数据安全法》对数据的出境管理进行了补充和完善。一是针对重要数据完善了跨境数据流动制度，《数据安全法》在《网络安全法》第三十七条的基础之上，规定“其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。”既与《网络安全法》相衔接，也实现了对所有重要数据出境的安全保障。二是通过出口管制的形式限制了管制物项数据的出口，《数据安全法》第二十五条规定“国家对与维护国家安全和利益、履行国际义务相关的属于管制物项的数据依法实施出口管制”，明确将数据出口管制纳入数据安全管理工作中，实现了与《出口管制法》的衔接，有利于从维护国家安全的角度限制相关数据的出境，对整体跨境数据流动制度进行补充。三是对外国司法、执法机构调取我国数据的情况进行了规定。《数据安全法》第三十六条首先明确“中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供数据的请求。”同时规定“非经中华人民共和国主管机关批准”不得向境外执法或司法机构提供境内数据，并对违法违规提供数据的行为，明确了包括警告、罚款等在内的行政处罚措施。这一制度的设置体现了对于合法合规向外国司法或者执法机构提供数据的重视，明确了我国处理外国司法或者执法机构关于提供数据请求的一般原则，同时也是依法应对少数国家肆意滥用长臂管辖，防范我国境内数据被外国司法或执法机构不当获取。

数据交易制度的确立使得数据依法有序流动成为现实。数据是数字经济时代的重要生产要素，而数据交易则是满足数据供给和需要的最主要方式，明确数据交易的法律地位，是满足现实需求、助力数字经济发展的重要表现，是当前数据交易制度发展的制度基础。《数据安全法》第十九条规定国家建立健全数据交易管理制度，规范数据交易行为，培育数据交易市场。此外，《数据安全法》还在第三十三条规定了数据交易中介服务机构的主要义务，规定从事数据交易中介服务的机构在提供交易中介服务时，应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录。《数据安全法》为数据交易制度提供了兼顾安全和发展的原则性规定，有利于在保障安全基础上，促进数据有序流动，激励相关主体参与到数据交易活动中来，充分释放数据红利。

随着《数据安全法》的正式出台，我国网络法律法规体系实现进一步完善，为后续立法、执法、司法相关实践提供了重要法律依据，为数字经济的安全健康发展提供了有力支撑。（来源：网信中国）

➢ 共同保障网络安全 携手维护国际和平

2021 年 6 月 29 日，联合国安理会举行网络安全问题公开会，中国常驻联合国代表张军出席会议并阐述中方立场。

张军表示，各国在网络世界既享有共同机遇、拥有共同利益，也面临共同挑战、承担共同责任，正日益成为休戚与共的命运共同体。国际社会应携手合作，共同保障网络安全，维护国际和平。

首页 > 会议与发言

张军：共同保障网络安全，携手维护国际和平

2021/06/29

张军表示，应以维护和平促安全，防止网络空间成为新的战场。国际社会应遵守《联合国宪章》宗旨和原则，特别是主权平等、禁止使用武力、不干涉内政、和平解决争端等原则。应尊重各国自主选择网络发展道路、网络管理模式、平等参与网络空间治理的权利。应审慎对待武装冲突法等适用于网络空间问题，防范网络空间军备竞赛。

张军表示，应以交流合作促安全，营造网络空间良好环境。网络空间霸权主义、单边主义、保护主义只会加剧紧张对抗，毒化合作氛围，应当受到国际社会共同抵制和反对。应为企业提供开放、公平、非歧视的营商环境，保障全球信息通信产业链供应链开放、稳定、安全，推动全球经济健康发展，反对以各种理由人为干扰企业正常经营行为。

张军表示，应以加强治理促安全，推进网络空间公平正义。各国应践行真正的多边主义，在联合国框架下建立各方平等参与、开放包容、可持续的网络安全治理进程，制定各国普遍接受的网络空间国际规则，反对搞小圈子和集团政治。中方期待新一届联合国网络安全问题

开放式工作组为维护网络安全作出新贡献，愿与各方一道推动在联合国框架下制订打击网络犯罪国际公约。

张军表示，应以普惠发展促安全，实现网络空间共同繁荣。各国应采取更加积极、包容、协调、普惠的政策，促进信息通讯技术在全球范围内均衡发展，大力发展数字经济等新模式新业态，反对搞科技霸权。应加强数字基础设施建设和互联互通，打破信息壁垒，弥合数字鸿沟，帮助发展中国家提高数字化、网络化、智能化水平，落实 2030 年可持续发展议程。

张军指出，中方去年提出《全球数据安全倡议》，聚焦关键基础设施和个人信息保护、企业境外数据存储和调取、供应链安全等重大问题，为维护全球数据和网络安全提出建设性解决方案。中方还积极推进“数字丝绸之路”建设，同各国共同构建面向未来的智能化互联互通新格局。

张军强调，网络空间承载人类梦想，关乎民众福祉与和平安全。中方愿同世界各国一道，把握信息革命机遇，培育创新发展新动能，开创数字合作新局面，打造网络安全新格局，构建网络空间命运共同体，携手创造人类更加美好的未来。（来源：人民网）

➢ 全球互联背景下数据本地化发展趋势与展望

尽管网络信息技术不断促进全球各地互通互联，但各国或地区不但没有放弃地域维度的管控思路，数据治理的地域化反而借由数据本地化等立法有所强化。

一、各国或地区关于数据本地化立法现状

关于何为数据本地化，目前存在多种定义。从广义上理解，数据本地化可以视为任何对数据跨境流动加以限制的制度。全球互联网治理委员会（Global Commission on Internet Governance）在其 2015 年的报告《数据本地化规则对金融服务的影响》（Addressing the Impact of Data Location Regulation inFinancial Services）中，将数据本地化概括为四种类型：一是数据出境的地域限制，即要求数据必须于某一国家或区域境内存储和处理；二是数据位置的地域限制，即允许数据副本出境处理，但在本国或本区域内必须存有副本；三是基于许可制的数据出境限制，即要求数据出境需经有权机关许可；四是基于标准体系的数据出境限制，即要求数据出境必须采取标准化的步骤以确保数据安全和隐私保护。其中，前两种类型会直接限制数据跨境流动，是当前世界数据本地化立法的主要类型。

无论是以上何种类型，均包含对数据出境的限制。经济合作与发展组织（OECD）在其 2019 年的调查报告《贸易与跨境数据流动》（Trade and Cross-Border Data Flows）中，将数据跨境流动的管制强度由弱到强分为四个层级：第一层级是对数据跨境流动不设任何法律限制，该层级多出现于最不发达国家；第二层级是不对数据跨境做事前限制，但设置事后审查和追责机制；第三层级是规定数据出境条件和情形，并对数据接收国设置资质限制，例如欧盟《通用数据保护条例》（GDPR）采用的就是这种思路；第四层级是最高限制层级，即数据能否跨境流动需要经过个案审查。

各国或地区要求本地化的数据类型，大致可以分为两类：一类针对公民个人信息，例如澳大利亚《由个人控制的电子健康记录法》（PCEHR Act）针对公民健康类数据，而俄罗斯和马来西亚则要求存储本国公民的各类个人数据；另一类则涉及非个人数据，例如德国《电子通信法》（TKG）对原始数据的本地存储进行规定，印度《国家数据分享和准入政策》（NDSAP）则要求所有通过使用公共基金收集的数据均存储于本国境内，而我国《网络安全法》基于保障网络数据安全的考量，明确要求在境内存储“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据”。

除本地化存储要求外，各国的一些配套措施也在不同程度上推进数据本地化，例如越南的《互联网服务和在线信息管理、提供和使用条例》（Decreeon the Management，Provision and Use of InternetServices and Online Information）要求信息收集网站、社交网站、移动通信网络服务提供者、在线游戏服务提供者等，至少将一个服务器设置在越南境内；法国也曾建议对收集、管理和商业应用本国境内人员个人数据的行为征税，其中，数据的异地存储有可能因为不完全合规而被征收更高的税额。

数据跨境流动的限制必然伴随复杂的安全评估和审查程序。例如，根据欧盟 GDPR 规定，在向欧盟境外第三国传输数据时需要经过两个步骤的审查：其一是数据传输行为本身是否有合法授权和依据；其二是数据接收国是否符合欧盟委员会的相关安全性要求。我国于 2019 年颁布的《个人信息出境安全评估办法（征求意见稿）》也有类似机制，要求将需要进行出境前安全评估的个人信息扩展至各类网络运营者在境内运营过程中收集的信息，而不仅限于关键信息基础设施运营者。该征求意见稿一方面明确禁止特定情形下的个人信息出境，另一方面则搭建起个人信息安全评估出境的一般性流程。

类似的安全评估和风险评估要求同样体现在我国的《数据安全法（草案）》和《个人信息保护法（草案）》中。2021 年 4 月的《数据安全法（草案）》二次审议稿要求建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查；同时，重要数据处理者应当定期开展风险评估，并向有关主管部门报送风险评估报告；此外，境外司法或执法机构要求调取中国境内数据时，非经中国主管机关批准，不得提供。2021 年 4 月的《个人信息保护法（草案二次审议稿）》第三章，从跨境数据流动角度规定了个人信息保护相关规则，重申了《网络安全法》关于关键信息基础设施运营者处理个人信息的境内存储规则，亦对其本地化要求进行了扩充，即将境内存储要求扩展至处理个人信息达到国家规定数量的其他个人信息处理者；同时，第三章也就其他情形下的个人信息出境设置了限制性条件；此外，国家机关处理的个人信息原则上也应当在中国境内存储。这些规定总体上呈现出以强化数据本地化来提升数据控制和保护的立法思路。

二、数据本地化的立法动因与挑战

数据本地化这种强调数据地域属性的做法，源于国家主权、数据安全、个人信息保护等多种因素。根据经合组织于 2020 年发布的报告《数据本地化趋势和挑战：基于隐私指南的考量》（DataLocalization Trends and Challenges：Considerationsfor the Review of the Privacy Guidelines），数据本地化的立法动因主要集中在九个方面：一是保障网络安全；二是防范外国网络间谍；三是协助执法机关和国家安全机关获取数据；四是减少网络犯罪并服务于其侦查；五是保护个人数据；六是提升网络事件响应能力；七是形成地缘政治优势；八是确保政府获取特定类型数据；九是形成经济竞争优势。

尽管存在上述动因，但需要注意到的是，数据本地化与全球信息网络化大潮之间仍然存在兼容问题。

首先，数据本地化与互联网基本架构和新兴信息技术之间存在技术冲突。在信息网络技术的支撑下，数据本身呈现出去地域化的特征，数据的全球高速流动和分散存储是现代互联

网的内在属性，云计算正是这一属性的典型例证。数据存储于何地，以何种方式存储，是以数据高效流动和使用为决定因素，这与当前各国数据本地化立法的出发点存在分歧。从这个角度看，数据本地化也不可避免地与数字经济发展产生冲突。

其次，数据本地化可能造成不同地域之间新的法律冲突。不同国家和地区对本地化的数据类型和范围要求不尽相同，对数据的分类也存在较大差异，这种差异将直接反映在网络信息业者的合规义务以及可能由此产生的合规冲突之上。应对合规要求以及化解合规冲突需要网络信息企业建立起相应的内部合规机制，而该机制的有效运行又依赖于相应的专业人员和技术支撑，此时，合规义务不可避免地会转化为企业的合规成本，从而加重企业的运营负担。考虑到网络信息业者自身经营能力差异，这种合规负担对于中小微互联网企业发展的影响尤为严重。

再次，在数据全球分布和流动成为网络信息产业的基本要求和核心生命力的背景下，数据本地化制度不可避免地会提高网络信息业者的经营成本，一方面体，现在网络信息业者需要通过建立当地数据存储中心以符合本地化要求，另一方面，也体现在可能形成新的数据和网络安全风险。这些成本不可避免地会转嫁至消费者端，一定程度上可能迫使网络信息业者避免在某些国家或地区开展业务，并可能进一步阻碍新技术和新产品在全球范围内的扩展。

最后，即便以强化数据治理为由，数据本地化亦有可能损及网络空间治理的实际效能。以网络犯罪为例，数据本地化的重要正当性事由之一，在于强化本国侦查机关的数据取证能力，但该事由并非必然成立。一方面，数据本地化制度大多并非针对所有数据，因此，无法确保与具体刑事案件证据材料需求相匹配。另一方面，犯罪分子通常会采取多种方式，利用刑事诉讼的地域管辖权限制，将相关数据转移至境外，从而人为造成取证困难。更重要的是，

在跨境数据取证需求普遍化的当下，数据本地化制度对他国取证形成的限制会借由对等和互惠原则传递至本国，反噬本国侦查机关的跨境取证能力。

数据本地化所呈现出的多重弊端也反映在一些国家或地区对该制度的犹疑摇摆态度之上。以欧盟为例，欧盟曾于 2013 年提出强化对云计算的管理，对欧盟境内的数据出境设置更高的门槛，并重新审视欧盟与美国之间关于数据跨境流动的“安全港”规则。欧洲法院在 2020 年的施雷姆斯二号案（Schrems II）中，进一步宣布隐私盾协议无效。

然而，促进形成单一数据市场又是欧盟的一贯目标。在其 2018 年 6 月形成的欧美内部政治协议中，欧盟单一数字市场副主席安德鲁斯·安西普（AndrusAnsip）明确表示，“数据本地化是典型的保护主义，它与单一市场不相兼容。在实现人员、货物、服务和资金自由流动后，通过此项协议支持非个人数据的自由流动，以促进技术和商业模式创新。”在此背景下，2018 年《欧盟非个人数据自由流动框架条例 》（Regulation on A Framework for the Free Flowof Non-Personal Data in the European Union），明确要求除非基于公共安全考量，否则禁止针对非个人数据的本地化要求。

三、数据本地化立法的发展趋势

从当前世界主要国家和地区的数据政策和立法发展状况看，以数据本地化为代表的网络和数据的地域性分割趋势非但不会削弱，反而可能在复杂的国际形势下被进一步强化。同时，不同国家或地区对数据本地化的态度往往与所涉视角紧密相关：一方面，针对商业贸易和网络信息产业发展而言，去本地化要求是较为普遍的观点，例如，于 2020 年 7 月生效的《美墨加三国协议》（USMCA）也从促进区域贸易的角度，对数据本地化持否定态度；另一方面，从数据主权、国家和公共安全以及个人信息保护角度看，加强本地化要求又成为重要手段之一，例如，欧盟 GDPR 即反映出此类思路。但是，这些方面的考量因素并非彼此独立，而是在网络信息时代相互交织，共同作用于各个领域的网络和数据治理规则。

在互联互通的网络全球化时代，建构开放、包容的命运共同体更为关键，如何在尊重国家主权和保障公民基本权利的前提下，推动网络空间国际治理整体能力的提升，促进数据资源发挥最大效能，是网络信息时代提出的重大命题。

围绕数据本地化的立法争议正是这一重大命题的集中体现。化解该争议、最大限度推动国际共识和规范的形成，需要建立在数据跨境流动的场景化的基础之上，针对不同类型的数据在不同场景下的流动特征，设置不同层级的跨境传输限制规则。

首先，在网络空间治理层面，需要正视数据本地化制度对数据跨境流动在客观上造成的阻碍。从网络信息技术发展的内在属性出发，立法者应当以推动数据合理、高效流动为基本

原则，数据本地化规则作为例外情形适用。这一原则需要国际层面的共同推动，促进本地化基本原则和规则体系国际共识的形成。

其次，在需要适用本地化数据治理的情形下，应当进一步区分不同场景，其核心在于，一方面，就不同场景背后所保护的具体权益进行分类、分层，另一方面，对该场景下数据跨境的具体特征加以明晰。特别是需要区分商业场景与社会公共治理场景，以及区分数据跨境传输的常态化场景和个案化场景。

再次，在区分数据本地化适用场景的前提下，应当就本地化措施本身进行细化和阶层化，避免一刀切式地采用最为严格的出境限制。具体而言，这种阶层化包含以下两个层面的含义：一是就本地化规则区分严格境内存储、副本境内存储等不同层级；二是就数据出境规则设置审批制、备案制、标准制等不同层级。这意味着，一方面，需要针对特定场景下特定本地化层级的立法设置依据比例原则进行评估，另一方面，需要针对具体的数据跨境活动建立起数据出境的个案影响评估机制。

最后，数据本地化规则不能脱离数据治理体系单独建设，需要将本地化要求放置在网络空间治理的整体框架下，将数据本地化要求与网络安全、个人信息保护、网络空间管辖权等相关领域立法相配合，突破部门法的分割视野，形成数据治理领域法的协同建设。（来源：本文刊登于《中国信息安全》杂志 2021 年第 5 期）

➢ 个人信息保护困局亟需打破

数字经济时代，随着个人信息价值的凸显，个人信息收集乱象突出，个人信息泄露事件频发，个人信息滥用程度严重，我国个人信息安全面临着严峻的挑战。监管执法部门已通过开展一系列联合专项行动，严厉打击侵害公民个人信息的违法违规行为。然而，当前个人信息安全逐步呈现出“问题频出-监管打击-安全平稳期-问题再次复现”的往复循环的态势，黑客攻击、内鬼窃取、APP 过度索权等均成为了个人信息保护的难题。

App 强制授权、过度索权等问题严重。当前，在用户安装 App 时，“请求获取位置权限”“请求获取通信录内容”“请求获取设备信息”等获取权限的要求接连弹出，依次等待用户予以放权。若用户不同意勾选，就无法享受相应服务。此外，有网络安全机构对某 App 进行检测时发现，用户在初次安装使用该 App 时仅有存储、电话、通信录和位置信息 4 项权限提示，但随后 App 还要获取其他数十项子权限。若用户点击不同意，则应用自动退出。App

公开隐私政策，明示需获取的各种权限和信息，本是基于尊重用户知情权的考虑，然而，用户的现实体验却与设计初衷大相径庭，甚至南辕北辙。过度索权和强制授权等问题已成为用户安装使用 App 的常态，用户个人信息自主权丧失。

平台企业利用数据垄断优势贩卖个人信息。个人信息是平台企业发展的重要战略资产，平台企业以牺牲消费者权益为代价，通过数据贩卖最大化进行商业谋利。以巧达科技为例，其通过爬虫技术垄断了所有公开简历信息，而且在未经用户明确同意情况下，共享给第三方，通过简历数据进行价值变现。在未经用户的同意下，利用垄断优势进行个人信息的贩卖交易活动，严重侵害了用户的个人隐私权益，为用户的人身、财产安全造成了巨大威胁。

人脸识别技术滥用侵犯个人隐私。当前，随着人工智能应用的成熟，人脸识别技术被广泛应用于生活各个领域，在为生活提供便利的同时，也引发了用户个人隐私信息被过度采集和滥用的风险，进一步引了大众对“十步一刷脸”等个人生物信息采集现状的隐忧。2021 年 315 晚会上，人脸识别成为首个被关注的话题。据报道，一些商家会在线下门店安装人脸识别设备，并在未提前告知用户、没有取得用户同意的前提下，大量抓取用户的脸部信息。商家据此得到用户的年龄、性别、面部特征甚至是心情状态，并可在人脸信息上进行标记，用来实施营销推广。不同于传统的信息数据，人脸识别生物信息具有唯一性、永久性与不可替换性，一旦被泄露就会造成永久性的泄露和损失，为个人隐私安全埋下极大隐患。

加强个人信息保护刻不容缓。面对个人信息安全乱象丛生且屡禁不止的问题，在借鉴欧盟、美国等国家和地区个人信息保护先进经验的基础上，结合我国实际，提出强化个人信息保护的几点建议。

国家层面，加快个人信息保护立法和监管。一是建立健全我国个人信息保护的法律法规

体系。目前我国针对数据及个人信息保护的两部法案《数据安全法》和《个人信息保护法》仍处在草案阶段，配套下位法缺失，部分问题处于模糊地带，需进一步出台配套法律法规，针对具体问题制定相应解决措施。例如，规范数据权属关系及用户知情同意的具体方式，完善个人信息收集使用规则，明确数据产业链条上各方权益和责任。二是加快研究制定个人信息安全保护的相关标准。完善个人信息收集、传输、存储等数据全生命周期管理规范，研究制定个人信息分级分类标准，区分可使用、可交易的商业数据信息和不可使用、不可交易的数据信息，明确相应级别的保护措施。三是加强个人信息保护监管。持续推进 App 违法违规收集使用个人信息专项治理，创新监管手段，引入第三方检测评估和认证监测机制。

企业层面，规范个人信息安全管理。一是重视隐私条款政策的制定和规范性。使用浅显易懂的表达方式，明确告知用户企业收集个人信息的类型、目的及使用范围；为用户删除数据、注销账户提供渠道；建立用户反馈投诉入口，以及争议解决机制。二是夯实企业个人信息保护责任。企业应将个人信息保护理念融入企业运营管理全流程，在产品及服务设计阶段进行风险检测，将必要的隐私设计纳入产品及服务的最初设计之中，并通过定期开展个人信息安全影响评估，根据评估结果采取适当措施，降低侵害个人隐私安全风险。三是管理和技术手段结合保护用户个人信息。积极探索个人信息安全防护的新技术、新手段，进一步加强防攻击、防泄漏、防窃取的监测、预警、控制和应急处置能力，以更好的应对云计算、人工智能等新技术新业务带来的个人信息保护挑战。

个人层面，提升个人信息保护意识。一方面，要不断加强自我保护意识和提升保护技能。通过了解隐私政策、关闭非必要权限、加强对个性化标签和定向推送的管理等方式，降低个人信息泄露风险。另一方面，学习了解民典法、个人信息保护法、网络安全法等相关法律，做到知法懂法守法用法；应在发现个人信息泄露或违法使用的行为之后，通过监管渠道投诉举报个人信息违法违规行为，依法维护自身权益。（来源：赛迪智库）

四、政府之声

➢ 《中华人民共和国数据安全法》正式发布

2021 年 6 月 10 日，随着信息技术和人类生产生活交汇融合，各类数据迅猛增长、海量聚集，对经济发展、人民生活都产生了重大而深刻的影响。数据安全已成为事关国家安全与经济社会发展的重大问题。党中央对此高度重视，就加强数据安全工作和促进数字化发展作出一系列部署。按照党中央决策部署和贯彻总体国家安全观的要求，全国人大常委会积极推动数据安全立法工作。经过三次审议，2021 年 6 月 10 日，十三届全国人大常委会第二十九次会议通过了数据安全法。这部法律是数据领域的基础性法律，也是国家安全领域的一部重要法律，将于 2021 年 9 月 1 日起施行。

制定数据安全法是维护国家安全的必然要求。数据是国家基础性战略资源，没有数据安全就没有国家安全。数据安全法贯彻落实总体国家安全观，聚焦数据安全领域的风险隐患，加强国家数据安全工作的统筹协调，确立了数据分类分级管理，数据安全审查，数据安全风险评估、监测预警和应急处置等基本制度。通过建立健全各项制度措施，提升国家数据安全保障能力，有效应对数据这一非传统领域的国家安全风险与挑战，切实维护国家主权、安全和发展利益。

制定数据安全法是维护人民群众合法权益的客观需要。数字经济为人民群众生产生活提供了很多便利，同时各类数据的拥有主体更加多样，处理活动更加复杂，一些企业、机构忽视数据安全保护、利用数据侵害人民群众合法权益的问题也十分突出，社会反映强烈。数据安全法明确了相关主体依法依规开展数据活动，建立健全数据安全管理制度，加强风险监

测和及时处置数据安全事件等义务和责任，通过严格规范数据处理活动，切实加强数据安全保护，让广大人民群众在数字化发展中获得更多幸福感、安全感。

制定数据安全法是促进数字经济健康发展的重要举措。近年来，我国不断推进网络强国、数字中国、智慧社会建设，以数据为新生产要素的数字经济蓬勃发展，数据的竞争已成为国际竞争的重要领域。数据安全法坚持安全与发展并重，在规范数据活动的同时，对支持促进数据安全与发展的措施、推进政务数据开放利用等作出相应规定，通过促进数据依法合理有效利用，充分发挥数据的基础资源作用和创新引擎作用，加快形成以创新为主要引领和支撑的数字经济，更好服务我国经济社会发展。。（来源：中国人大网）

- **中华人民共和国数据安全法全文**
- http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml

➢ 四部门开展摄像头偷窥等黑产集中治理

2021 年 6 月 11 日，中央网络安全和信息化委员会办公室、工业和信息化部、公安部、市场监管总局发布关于开展摄像头偷窥等黑产集中治理的公告。**全文如下：**

近年来，不法分子利用黑客技术破解并控制家用及公共场所摄像头，将智能手机、运动手环等改装成偷拍设备，出售破解软件，传授偷拍技术，供客户“偷窥”隐私画面并借此牟利，已形成黑产链条，严重侵害公民个人隐私，人民群众对此反应强烈。为切实保护公民个人隐私安全，中央网信办、工业和信息化部、公安部、市场监管总局决定，自 2021 年 5 月

至 8 月，在全国范围组织开展摄像头偷窥黑产集中治理。现将有关事项公告如下：

一、社交软件、网站、论坛等互联网平台要严格履行信息发布审核的主体责任，全面清理平台上发布的涉摄像头破解教学、漏洞风险利用、破解工具售卖，偷拍设备改装，偷窥偷拍视频交易等摄像头偷窥黑产相关违法有害信息。

二、摄像头生产企业要按照数据安全、信息安全有关规定和标准提升产品安全能力，提供公共服务的视频监控云平台及有关企业要严格履行网络安全主体责任，强化云平台网络安全防护，落实对远程视频监控 App 的数据安全防护责任。

三、电商平台要严格履行主体责任，全面开展排查，对平台上的假冒伪劣摄像头做清理、下架处理。

四、公安机关依法打击提供摄像头破解软件工具、对摄像头设备实施攻击控制、获取买卖公民隐私视频等违法犯罪活动，严惩违法犯罪分子。

五、网信、工信、公安、市场监管等部门加强监管和执法，对于不落实主体责任的社交软件、网站、论坛、视频监控云平台、电商平台等互联网平台和企业，依法依规严厉进行处罚。（来源：中国网信网）

➢ 《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见（二）》发布

2021 年 6 月 22 日上午，最高人民法院、最高人民检察院、公安部联合召开新闻发布会，发布《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见（二）》（下称《意见二》），进一步明确法律标准，依法严厉惩治、有效打击电信网络诈骗及其关联犯罪。


中华人民共和国最高人民检察院

首页 | 最高检新闻 | 地方动态 | 通知公告 | 直播访谈 | 图片 | 专题 | 法律规章 | 权威发布

最高人民检察院网上发布厅

“两高一部”发布《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见（二）》

发布时间：2021年6月22日

6月22日上午，最高人民法院、最高人民检察院、公安部联合召开新闻发布会，发布《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见（二）》（下称《意见二》），进一步明确法律标准，依法严厉惩治、有效打击电信网络诈骗及其关联犯罪。

据悉，最高法、最高检、公安部曾在2016年12月联合发布《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》（下称《意见一》）。此次，《意见二》在《意见一》的基础上，对于电信网络诈骗犯罪以及涉手机卡、信用卡犯罪等关联犯罪，提出更加明确具体的适用法律依据。

《意见二》共十七条，针对司法实践中存在的新的突出问题，如电信网络诈骗犯罪案件及关联犯罪案件的管辖，跨境电信网络诈骗犯罪案件的取证，涉手机卡、信用卡即所谓“两卡”犯罪案件的处理，办理电信网络诈骗犯罪案件的政策适用等问题进行了规定。

《意见二》专门规定，在有证据证实行为人参加境外诈骗犯罪集团或犯罪团伙，在境外针对境内居民实施电信网络诈骗犯罪，诈骗数额虽难以查证，但一年内出境赴诈骗窝点累计时间30日以上或多次出境赴诈骗窝点的，应当认定为刑法第二百六十六条规定的“其他严重情节”，以诈骗罪依法追究刑事责任。

《意见二》规定，行为人明知他人利用信息网络实施犯罪，为其犯罪而提供收购、出售、出租信用卡、银行账户、非银行支付账户等支付结算帮助，数量

据悉，最高法、最高检、公安部曾在 2016 年 12 月联合发布《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》（下称《意见一》）。此次，《意见二》在《意见一》的基础上，对于电信网络诈骗犯罪以及涉手机卡、信用卡犯罪等关联犯罪，提出更加明确具体的适用法律依据。

《意见二》共十七条，针对司法实践中存在的新的突出问题，如电信网络诈骗犯罪案件及关联犯罪案件的管辖，跨境电信网络诈骗犯罪案件的取证，涉手机卡、信用卡即所谓“两卡”犯罪案件的处理，办理电信网络诈骗犯罪案件的政策适用等问题进行了规定。

《意见二》专门规定，在有证据证实行为人参加境外诈骗犯罪集团或犯罪团伙，在境外针对境内居民实施电信网络诈骗犯罪，诈骗数额虽难以查证，但一年内出境赴诈骗窝点累计时间 30 日以上或多次出境赴诈骗窝点的，应当认定为刑法第二百六十六条规定的“其他严重情节”，以诈骗罪依法追究刑事责任。

《意见二》规定，行为人明知他人利用信息网络实施犯罪，为其犯罪而提供收购、出售、出租信用卡、银行账户、非银行支付账户等支付结算帮助，数量达到 5 张（个）以上，或者提供收购、出售、出租他人手机卡、流量卡等通讯工具帮助，数量达到 20 张以上，以帮助信息网络犯罪活动罪追究刑事责任。这项规定解决了非法交易“两卡”行为构成帮助信息网络犯罪活动罪“情节严重”的认定问题。

《意见二》还在《意见一》规定加大对电信网络诈骗犯罪财产刑处罚力度的基础上，进一步规定，办理电信网络诈骗犯罪案件时，查扣在案的涉案账户内资金，应当优先返还被害人，如不足以全额返还的，应当按照比例返还。确保尽最大力量挽回被害群众的经济损失，切实维护人民群众合法权益。（来源：最高人民检察院）

- **“两高一部”发布《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见（二）》**
- **全文：**https://www.spp.gov.cn/xwfbh/wsfbt/202106/t20210622_522041.shtml#1

➢ 最高人民法院发布《人民法院在线诉讼规则》及其理解适用

2021 年 6 月 6 月 17 日，最高人民法院召开新闻发布会，发布《人民法院在线诉讼规则》（以下简称《规则》）。《规则》是最高人民法院颁布的首部指导全国法院开展在线诉讼工作的司法解释，将于 2021 年 8 月 1 日起施行。

《规则》的制定印发，是人民法院深入贯彻习近平法治思想，践行网络强国战略的重要成果，是构建完善“中国特色、世界领先”的互联网司法模式的关键举措。《规则》首次构建了涵盖各审判领域、覆盖诉讼全流程的在线诉讼规则体系，全面总结体现了近年来人民法院在线诉讼领域探索成果，积极回应了人民群众互联网时代司法新需求，对保障当事人合法诉讼权益，增强人民群众诉讼便利，提升审判质量效率，推动司法审判模式划时代变革具有重大意义。

《规则》共三十九条，内容涵盖了在线诉讼法律效力、基本原则、适用范围、适用条件，以及从起诉立案到宣判执行等主要诉讼环节在线程序规则，为各方诉讼主体参与在线诉讼提供明确的程序指引。（来源：最高人民法院）

- **《人民法院在线诉讼规则》全文：**
- http://www.court.gov.cn/fabu-xiangqing-309551.html

五、本期重要漏洞实例

➢ Microsoft 发布 2021 年 6 月安全更新

发布日期：2021-06-9

更新日期：2021-06-9

描述：

6 月 8 日，微软发布了 2021 年 6 月份的月度例行安全公告，修复了其多款产品存在的 49 个安全漏洞。受影响的产品包括：Windows 10 21H1（26 个）、Windows 10 20H2 & Windows Server v20H2（26 个）、Windows 10 2004 & Windows Server v2004（26 个）、Windows 8.1 & Server 2012 R2（19 个）、Windows Server 2012（18 个）、Windows RT 8.1（19 个）和 Microsoft Office-related software（8 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。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-2021-31962	**Kerberos AppContainer 安全功能绕过漏洞**	重要 安全功能绕过	Server, version 20H2 Server, version 2004 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2021-33739	**Microsoft DWM Core Library 权限提升漏洞**	重要 特权提升	Server, version 20H2 Server, version 2004 Windows 10
CVE-2021-31955	**Windows Kernel 信息泄露漏洞**	重要 信息泄露	Server, version 20H2 Windows 10 Server, version 2004 Server 2019
CVE-2021-33742	**Windows MSHTML Platform 远程代码执行漏洞**	严重 远程代码执行	Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2021-31956	**Windows NTFS 权限提升漏洞**	重要 特权提升	Server, version 20H2 Server, version 2004 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012

			Windows 8.1
CVE-2021-31199/31201	**Microsoft Enhanced Cryptographic Provider 权限提升漏洞**	重要 特权提升	Server, version 20H2 Server, version 2004 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2021-26414	**Windows DCOM Server 安全功能绕过漏洞**	重要 安全功能绕过	Server, version 20H2 Server, version 2004 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2021-31959	**Scripting Engine 内存破坏漏洞**	严重 远程代码执行	Server 2019 Server 2016 Server 2012 R2 Server 2012 Windows 8.1 Windows 10
CVE-2021-31963	**Microsoft SharePoint Server 远程代码执行漏洞**	严重 远程代码执行	SharePoint Server 2019 SharePoint Foundation 2013 SharePoint Enterprise Server 2016 SharePoint Enterprise Server 2013
CVE-2021-31939	**Microsoft Excel 远程代码执行漏洞**	重要 远程代码执行	Excel 2013 Office 2016 Office Web Apps Server 2013 Office 2013 Office 2019 Office Online Server Excel 2016 365 Apps Enterprise
CVE-2021-31941	**Microsoft Office Graphics 远程代码执行漏洞**	重要 远程代码执行	Office 2016 Office 2013 Outlook 2013 Office 2019 Office 2019 for Mac 365 Apps Enterprise

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

➢ IBM Planning Analytics 跨站脚本漏洞

发布日期：2021-06-29
更新日期：2021-06-30
受影响系统：
IBM Planning Analytics 2.0
描述：

CVE(CAN) ID: CVE-2021-20477
IBM Planning Analytics 是美国 IBM 公司的一套业务规划分析解决方案。该方案支持自动化执行业务规划、预算和分析等流程。
IBM Planning Analytics 2.0 版本存在跨站脚本漏洞。攻击者可利用该漏洞在 Web UI 中嵌入任意 JavaScript 代码，从而改变预期功能，这可能导致可信会话中的凭据泄露。
<*来源：Matt Byrne (Perspective Risk)
链接：https://www.ibm.com/support/pages/node/6462331
*>
建议：

厂商补丁：
IBM

IBM 已经为此发布了一个安全公告（6462331）以及相应补丁:
6462331：Security Bulletin: IBM Planning Analytics Workspace is affected by security vulnerabilities
链接：https://www.ibm.com/support/pages/node/6462331

➢ Linux kernel 越界读写漏洞

发布日期：2021-05-27
更新日期：2021-06-30
受影响系统：
Linux kernel <= 5.2.17
描述：

CVE(CAN) ID: CVE-2021-33200
Linux kernel 是美国 Linux 基金会的开源操作系统 Linux 所使用的内核。
Linux Kernel 5.12.7 及之前版本中存在越界读写漏洞。该漏洞源于 Linux kernel/bpf/ verify .c 未对指针算术操作进行正确限制。攻击者可利用该漏洞越界读写内核内存导致本地特权升级至 root。
建议：

厂商补丁：
Linux

目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：
https://www.openwall.com/lists/oss-security/2021/05/27/1

➢ Adobe Magento 信息泄露漏洞

发布日期：2021-05-11
更新日期：2021-06-29
受影响系统：
Adobe Magento Commerce <= 2.4.2
Adobe Magento Commerce <= 2.4.1-p1
Adobe Magento Commerce <= 2.3.6-p1
Adobe Magento Open Source <= 2.4.2
Adobe Magento Open Source <= 2.4.1-p1
Adobe Magento Open Source <= 2.3.6-p1
描述：

CVE(CAN) ID: CVE-2021-28566
Adobe Magento 是美国奥多比（Adobe）公司的一套开源的 PHP 电子商务系统。该系统提供权限管理、搜索引擎和支付网关等功能。
Adobe Magento 2.4.2 及之前版本、2.4.1-p1 及之前版本和 2.3.6-p1 及之前版本存在信息泄露漏洞。攻击者可利用该漏洞获取文件根路径。

<*来源：Nuswantara Gading Alfa Putranto
链接：https://helpx.adobe.com/security/products/magento/apsb21-30.html
*>
建议：

厂商补丁：
Adobe

Adobe 已经为此发布了一个安全公告（ASPB21-30）以及相应补丁：
ASPB21-30：Security Updates Available for Magento | APSB21-30
链接：https://helpx.adobe.com/security/products/magento/apsb21-30.html

六、本期网络安全事件

➢ 大众遭到黑客攻击 超 300 万奥迪车主个人信息被窃取

2021 年 6 月 11 日据 CNN 报道，大众汽车及其旗下汽车品牌奥迪遭到数据泄露攻击。这些数据泄露了来自美国和加拿大的客户的联系信息，并且部分暴露了个人详细信息，例如驾驶执照号码。

泄露发生的原因是一家供应商：在 2019 年 8 月至 2021 年 5 月期间将客户数据“未经保护”地留在互联网上。大众汽车及其子公司奥迪以及位于美国和加拿大的官方经销商都使用这个供应商的服务。这些基础信息数据包括电话号码、电子邮件地址、邮寄地址，在某些情况下还包括车牌号。

该公司已经联系了位于美国的 90,000 人——主要是奥迪客户——这是因为他们在这次泄露事件中暴露了特别敏感的信息。这包括驾驶执照号码，社保号码、大众或奥迪网站帐号和出生日期，该公司为那些敏感信息遭到泄露的人提供免费信用保护。

这些数据是从大众和奥迪及其一些经销商使用的外部供应商那里窃取的，主要收集于 2014 年至 2019 年之间。据大众称，这些信息主要是用于营销目的，并被留在不安全的文档中，大众没有透露遭窃取的供应商的名字。

大众美国公司在一份声明中表示：“对于这可能给我们现有或潜在客户带来的任何不便，我们深表歉意。与往常一样，我们建议个人对可疑电子邮件或其他可能要求他们提供有关自己或车辆信息的信息保持警惕”。（来源：央视财经）

➢ 非法获取员工及客户敏感信息 法国宜家被罚 100 万欧元

2021 年 6 月 15 日，由于非法监视员工和客户，法国法院周二要求瑞典家具零售业巨头宜家（IKEA）支付 100 万欧元（约合 777 万人民币）的罚款。

分公司宜家法国（IKEA France）被指控非法监视其员工长达数年，并通过查看员工的银行账户记录以及利用假员工撰写员工报告等方式侵犯其隐私信息。最初是工会于 2012 年向法国当局提起诉讼，指控这家瑞典家具巨头的法国子公司以欺诈手段和非法披露个人信息的方式收集个人数据，以及监视数百名员工和大批量客户。工会称，法国宜家通过向警方付费获得了针对个人，特别是工会活动家和一些顾客的个人信息档案资料。

法国凡尔赛宫副检察长帕梅拉·塔巴德尔此前一直要求对宜家法国公司处以 200 万欧元（约合 1,554 万人民币）的罚款。

该公司表示，在采取措施禁止监视手段后，公司正在复核法院的裁决，看是否需要采取进一步的措施。该公司说：“宜家法国已强烈谴责这些做法，对此表示道歉，并实施了一项重大行动计划，以防止此类情况再次发生。”

宜家法国的前首席执行官让·路易斯·巴约在此案中也被认定有罪，并被判处两年的缓刑。法官对他存储个人数据的行为处以 5 万欧元（约合人民币 38.87 万元）罚款。这些指控集中在 2009-2012 年期间，但按照检察官的说法，宜家法国的违法行为可能已持续近十年。

面临指控的人还包括几位前门店经理和人力资源部门的员工以及一名私家侦探和警察。

宜家也被指控在该案中对部分顾客实施了非法监视活动。在 2012 年这些指控曝光后，宜家开除了几名经理，并对其内部政策进行了全面修订。该集团被指控翻阅员工的资料，检查他们的财务和个人生活。它已经承认了其中的部分指控内容，但它否认建立了一个大型的监视系统。（来源：海外即时通）

➢ 全球大规模断网大量网站无法访问 波及数十个国家和地区

2021 年 6 月 8 日早间，美国云计算服务商 Fastly 公司出现技术问题，导致全球大量网站断网。故障持续约一小时后，受影响网站陆续恢复访问。 据美国媒体报道，美国东部时间 8 日 6 时起，美国社交新闻网站红迪网、亚马逊、美国有线电视新闻网、《纽约时报》《金融时报》、英国政府网等大量网站出现用户无法访问的状况，页面提示为服务器端不可用或连接失败。

有故障侦测网站显示，多数网站在同一瞬间报错，疑似为网络服务商出现问题。Fastly 公司当天表示，经过检查后确认一个服务器配置问题引发整个服务器运行中断，在禁用该配置后故障得以修复。据报道，美东时间 7 时起，受影响网站陆续恢复访问。此次大规模断网波及全球数十个国家和地区。

Fastly 工程和基础设施高级副总裁尼克-罗克韦尔（Nick Rockwell）在周二晚些时候的一篇博客文章中说："由于 6 月 8 日出现的一个未被发现的软件漏洞，我们经历了一次全球中断，当时它是由一个客户配置变更所触发的。他说，这次故障是 "广泛而严重的"，但该公司

迅速发现、隔离并禁用了这个问题，49 分钟后，其大部分网络又开始运行。罗克韦尔说，该漏洞已包含在 5 月份推出的软件更新中，该公司正试图弄清楚为什么在测试期间没有发现它。罗克韦尔说："尽管有特定的条件触发了这次中断，但我们应该已经预料到了。"

总部位于旧金山的 Fastly 主要提供内容交付网络服务，这种服务允许客户在分布在 26 个国家的镜像服务器上存储图像和视频等数据，让数据更接近用户意味着它传递得更快。但这一事件凸显了全球互联网是如何依赖于像 Fastly 这样提供重要基础设施的少数幕后公司的，它扩大了人们对这些公司如何容易受到更严重破坏的担忧。（来源：互联网综合整理）

➢ 新加坡星展银行发生系统故障 大批用户余额被扣光

2021 年 6 月 18 日，新加坡星展银行(DBS Bank)发生系统故障，许多用户交易出现双重收费的状况，也有部分用户的余额甚至被扣光，变成负数!一名网友指出，他的 DBS 银行户口显示-$1600，因为他昨天转账了$2000。许多网友分享他们 DBS 银行账户的截图，透露自己的户口也出现重复交易的问题。

DBS 在推特和脸书上发文表示：银行得知一些转账卡和信用卡上出现了重复交易的问题。DBS 指出，银行已经在尝试确定和解决问题，并确保双重收费会被退还。同时，银行对于由此给客户带来的不便表示歉意。

大批网友纷纷涌入 DBS 银行脸书留言谴责。一名网友对于这次的银行系统故障感到非常愤怒，他指出："如果用户遇上紧急事件，需要用钱的话，那如何是好?"有些网友则对 DBS 是在用户自己发现问题后，才发声明，而感到不满。受影响的网友都希望 DBS 能尽快

退钱。DBS 银行系统故障，大批用户余额被扣光目前为止，DBS 并没有给出此次故障发生的原因，也没有提到用户该如何得到退款。（来源：新加坡眼）

➢ 盗取医院“统方”数据牟利，一被告人被判相关工作“从业禁止”

2021 年 6 月 21 日，澎湃新闻报道，在医疗行业内，“统方”一般是指通过统计医生处方用药数据从而掌握药品用量等信息。非法“统方”行为不仅扰乱了正常的药品管理秩序，也极易滋生医药购销领域的腐败行为。

近日，上海黄浦区人民法院审理了一起医院外包软件运维人员非法下载“统方”数据并出售牟利的案件，两名被告人因犯非法获取计算机信息系统数据罪而获刑，同时，区法院还依法对其中的一名被告人作出从业禁止，禁止其在刑罚执行完毕后三年内从事计算机信息系统维护管理相关工作。这也是上海法院首次对此类犯罪的被告人适用从业禁止令。

据了解，张某被长期派驻在上海一家三甲医院，从事“排队叫号系统”的软件维护工作。2019 年 10 月，张某结识了某医药公司医药代表黄某。黄某向张某提出，希望张某能提供医院的统方数据，并表示可以给予一定的报酬。虽然张某平时并无机会接触这些数据，但仍应允了黄某的要求。他找到同在医院负责软件运维工作的陈某帮忙。作为某信息公司的运维工程师，陈某负责该医院门诊预约系统等软件的维护工作，在金钱的诱惑下，陈某答应设法为

张某定期提供“统方”数据。

去年 7 月，医院发现相关信息系统出现异常数据下载后，开展内部排查，并向警方报了案。到案后，陈某如实交代了案件事实，但张某始终拒不供认，直到审查起诉阶段才如实供述案件事实。今年 2 月，黄浦区人民检察院以非法获取计算机信息系统数据罪对张某和陈某提起公诉。案件审理期间，陈某在其家属帮助下退出违法所得人民币 10,200 元。法官审理后认为，两名被告人违反国家关于计算机信息和医药信息的管理规定，非法获取医疗单位计算机信息系统中存储的数据，情节严重，其行为均已构成非法获取计算机信息系统数据罪，应依法追究刑事责任。根据两名被告人的犯罪事实、情节、性质、对社会的危害程度及案发后的上述行为，对两名被告人依法不适用缓刑。同时陈某利用职业便利，非法获取计算机信息系统数据，应该在刑罚执行完毕后给予“从业禁止”。

据此，区法院一审判处张某有期徒刑 1 年 6 个月并处罚金 1.5 万元;陈某有期徒刑 1 年并处罚金 1 万元;禁止陈某在刑罚执行完毕后三年内从事计算机信息系统维护管理相关工作。区法院刑事审判庭庭长闵灏指出，本案被告人利用维护信息的工作便利，违背职业要求的特定义务，数次非法侵入医院计算机信息系统数据库，盗取医院“统方”数据并转卖给他人，侵害了被害单位的权益，扰乱了医疗秩序，滋生腐败等不正之风，社会影响恶劣，为此，法院在作出实刑判决的同时，还首次适用了“从业禁止”令。

通过禁止犯罪分子从事相关工作，使犯罪分子一定时期内无法再次进入相关信息系统管理领域，将有助于预防犯罪分子再次实施此类犯罪，从源头上遏制“统方”数据泄露之风的蔓延。同时，针对目前大数据时代，信息系统数据管理维护过程中个人信息泄露、滥用情况多发、易发的情况，该案也将对相关从业人员产生警示作用，有利于肃正行业的风气，促进行业人员自律。

相关法条：《中华人民共和国刑法》第三十七条之一:

因利用职业便利实施犯罪，或者实施违背职业要求的特定义务的犯罪被判处刑罚的，人民法院可以根据犯罪情况和预防再犯罪的需要，禁止其自刑罚执行完毕之日或者假释之日起从事相关职业，期限为三年至五年。被禁止从事相关职业的人违反人民法院依照前款规定作出的决定的，由公安机关依法给予处罚;情节严重的，依照本法第三百一十三条的规定定罪处罚。其他法律、行政法规对其从事相关职业另有禁止或者限制性规定的，从其规定。（来源：澎湃新闻）

➢ 以色列 20 多万名学生的个人信息遭到泄露

2021 年 6 月 28 日，据外媒报道，上周约 28 万名以色列学生的个人信息在针对 AcadeME 公司的网络攻击中被泄露。据 Jerusalem Post 报道，Think Safe Cyber Facebook 组织的 May Brooks-Kempler 估计，约有 28 万名在校或在校学生的个人信息被盗。

AcadeME 是以色列一个全国性的服务提供商，为在 11000 个不同的行业中寻找工作的学生提供支持。6 月 20 日，它成为了亲巴勒斯坦的马来西亚黑客组织 DragonForce 的受害者。

虽然 AcadeME 否认了这一指控，但所附的代码截图、服务器地址和包含电子邮件地址和姓名的表格却表示并非如此。基本上，证据表明学生的电话号码、地址、全名、电子邮件和密码都遭到了泄露。

这些黑客在 Telegram 上写道：“这是对全世界所有黑客、人权组织和活动人士的紧急呼吁，让他们再次团结起来并发起针对以色列的运动、分享那里的真实情况、向世界揭露他们的恐怖活动……我们永远不会对以色列的战争活动保持沉默。”

去年，针对以色列企业和组织的网络攻击频率有所增加，Amital 软件、Ami Insurance 和 Israel Aerospace Industries 等公司受到了影响。事实上，周五早些时候，该组织对以色列的机构进行了 DDoS 攻击，包括以色列银行(Bank of Israel)、Leumi 银行和 Mizrahi Tefahot。这些网络罪犯还声称在同一天释放了大量以色列护照。

今年年初，以色列国家网络局(INCD)局长 Yigal Unna 表示担心，如果不采取适当措施，

黑客有能力破坏以色列的学术机构。委员会主任表示担心，学术机构和其他机构和组织之间的广泛联系可能会对其他机构和组织构成威胁进而导致它们承担法律责任。（来源：cnBeta）

信息安全意识产品服务

021-33663299