国盟信息安全通报

2020 年 7 月 19 日第 220 期

全国售后服务中心

国盟信息安全通报

（第 220 期）

国际信息安全学习联盟

2020 年 07 月 19 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 252 个，其中高危漏洞 56 个、中危漏洞 163 个、低危漏洞 33 个。漏洞平均分值为 5.40。本周收录的漏洞中，涉及 0day 漏洞 44 个（占 17%），其中互联网上出现“ZyXEL Armor X1 WAP6806 路径遍历漏洞、QuickBox 远程代码执行漏洞”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 4971 个，与上周（2924 个）环比增加 70%。

主要内容

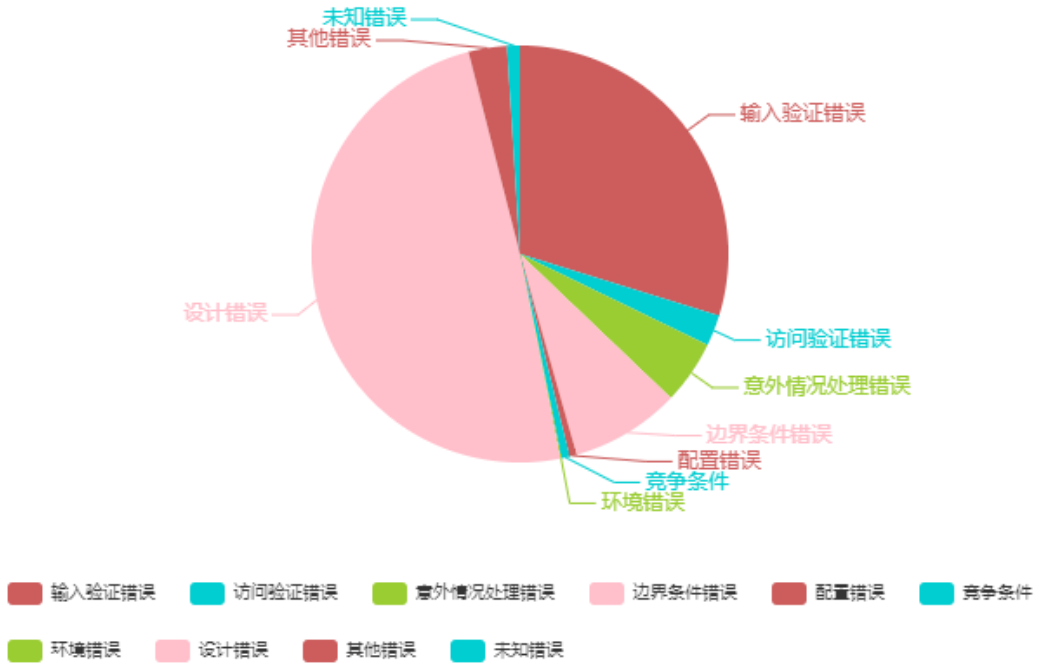
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

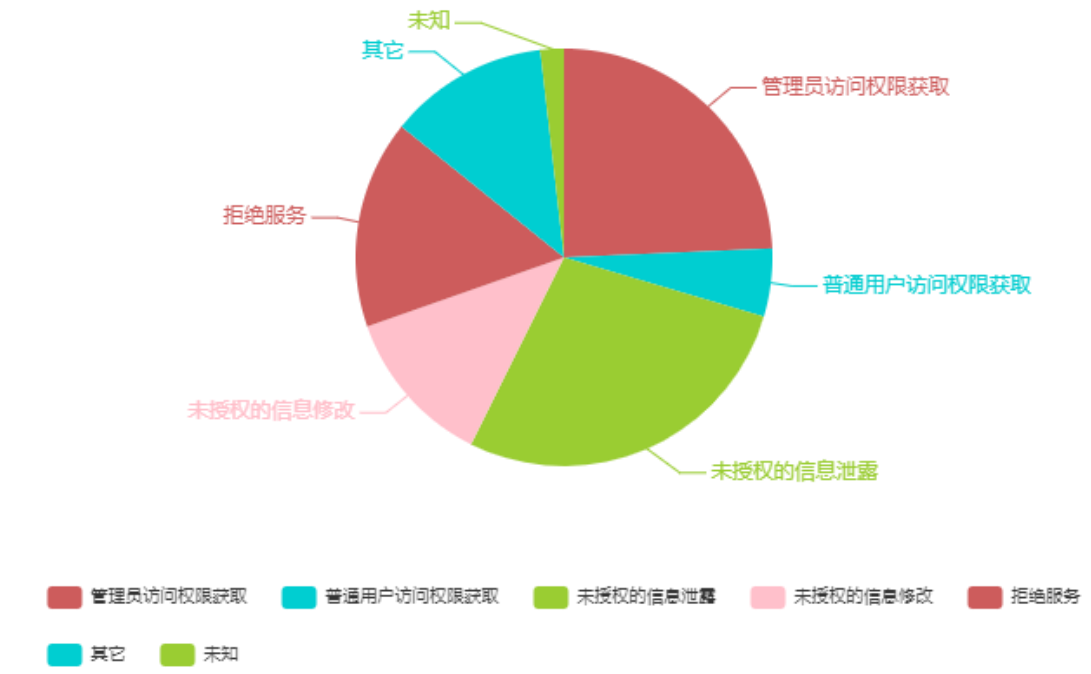
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 252 个，其中高危漏洞 56 个、中危漏洞 163 个、低危漏洞 33 个。漏洞平均分值为 5.40。本周收录的漏洞中，涉及 0day 漏洞 44 个（占 17%），其中互联网上出现“ZyXEL Armor X1 WAP6806 路径遍历漏洞、QuickBox 远程代码执行漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 4971 个，与上周（2924 个）环比增加 70%。

二、安全漏洞增长数量及种类分布情况

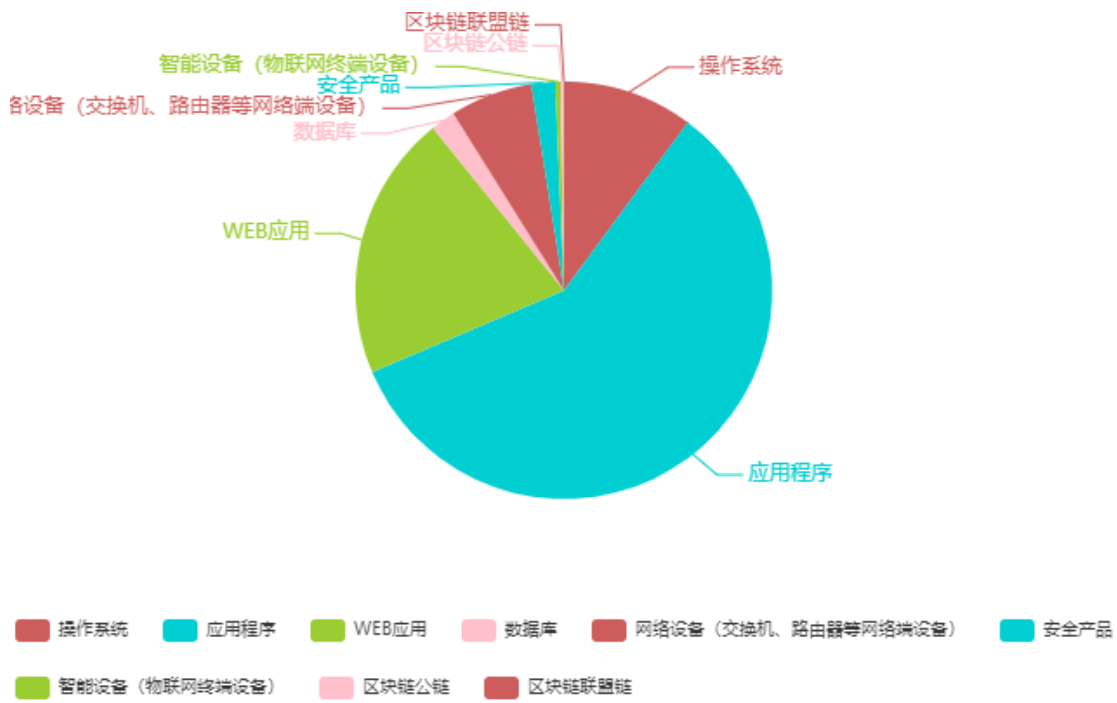
➢ 漏洞产生原因（2020 年 07 月 05 日—2020 年 07 月 19）



➢ 漏洞引发的威胁（2020 年 07 月 05 日—2020 年 07 月 19）



➢ 漏洞影响对象类型（2020 年 07 月 05 日—2020 年 07 月 19）



三、安全产业动态

➢ 加大个人信息保护力度 确保个人信息保护有法可依

人民网研究院组织编写的移动互联网蓝皮书《中国移动互联网发展报告(2020)》7 月 14 日在京正式发布。其中，中国社会科学院上海研究院刘晶晶博士和中国社会科学院法学研究所研究员支振锋撰写的《2019 年移动互联网政策法规与趋势展望》一文认为，2019 年我国加强移动互联网新规则新制度的建设，相关部门采取了一系列措施加大个人信息保护力度，确保个人信息保护有法可依，有章可循。以《网络安全法》为基础框架的一些列新的政策法规的推出，完善了我国移动互联网领域的法制建设。在国家治理、网络安全、信息内容治理、产业发展等方面推出了移动互联网新规则新制度。

国家治理方面，最高人民法院下发了《关于在部分法院推进“移动微法院”试点工作的通知》，对移动互联网如何真正实现司法平等、司法数据安全、真正司法为民提供了法律依据。中宣部和国家广播电视总局联合发布了《县级融媒体中心建设规范》《县级融媒体中心省级技术平台规范要求》《县级融媒体中心网络安全规范》《县级融媒体中心运行维护规范》《县级融媒体中心监测监管规范》等 5 个文件，形成了建设县级融媒体中心的基本标准规范。

网络安全方面，相关部门采取了一些列措施加大个人信息保护力度，确保个人信息保护有法可依、有章可循。《信息安全技术移动互联网应用程序（APP）收集个人信息基本规范（草

案）》，是我国第一个专门针对 APP 收集个人信息时应满足的基本要求而起草的国家标准，明确提出 APP 收集个人信息应满足的 16 项基本要求，并在附录规定了 21 种常用服务类型可收集的最小必要信息以及最小必要权限范围。国家互联网信息办公室发布《儿童个人信息网络保护规定》，这是我国第一部针对儿童个人信息网络保护的专门立法，明确把“儿童”界定为不满十四周岁的未成年人。《信息安全技术网络安全等级保护基本要求》《信息安全技术网络安全等级保护测评要求》《信息安全技术网络安全等级保护安全设计技术要求》等国家标准正式发布实施，体现了等级保护从信息安全向网络安全的转变，更加强调了网络空间安全的概念。工信部发布的《网络安全漏洞管理规定（征求意见稿）》，从漏洞发现、漏洞接收、漏洞验证、漏洞处置、漏洞发布等多个环节实现对网络安全漏洞的全生命周期管理，规定了不同主体在发现或获知网络安全漏洞后以及向社会发布漏洞信息的过程中应当承担的义务。

信息内容治理方面，《网络信息内容生态治理规定》、《网络音视频信息服务管理规定》、《信息安全技术社交网络平台信息标识规范》征求意见稿和互联网信息服务严重失信主体信用信息管理办法（征求意见稿）》等法律法规的推出，对构建良好网络生态、完善网络音视频信息服务管理和强化社交平台信息安全管理责任等方面提供了法律依据。不但彰显网信部门在信息内容治理上全主体参与、全平台覆盖、全流程监管、全环节治理的制度设计，也是对监管部门网络信息内容生态治理工具的全方位展示。

产业发展发面，《网络交易监督管理办法(征求意见稿)》突出了在网络交易环境下消费者知情权和选择权的保障。工业和信息化部印发的《携号转网服务管理规定》赋予用户更多的选择权，一定程度上有利于良好市场环境的形成。教育部等八部门联合出台的《关于引导规范教育移动互联网应用有序健康发展的意见》和《教育移动互联网应用程序备案管理办法》，对教育移动应用行业的发展做了规划并强调监管部门提高以备案为基础的始终时候监管能力。互联网金融风险专项整治工作领导小组、网贷风险专项整治工作领导小组联合发布了《关于加强 P2P 网贷领域征信体系建设的通知》通过支持在营 P2P 网贷机构接入征信系统，实现平台间的借贷信息共享，一定程度上能够缓解多头借贷产生的坏账风险，有利于整个网贷行业的良性发展。

未来移动互联网政策法规发展趋势主要表现在加强数据治理，立法完善数据权属、合理使用与监管；内容治理压实平台责任，延续多部门联合专项治理行动；响应公众个人信息保护需求，创新个人信息保护制度；不断强化新技术新业态的监管，营造健康网络生态等几个方面。（来源：人民网）

➢ 数字经济的压舱石、国家安全的新维度 《数据安全法（草案）》之解读

2020 年 7 月 2 日，全国人大常委会第二十次会议审议了《数据安全法（草案）》（“《数安法》”或“本法”）并公开征求意见。全文 7 章 51 条，包括：总则、数据安全与发展、数据安全制度、数据安全保护义务、政务数据安全与开放、法律责任和附则。《数据安全法》与去年 5 月 28 日国家互联网信息办公室公布的《数据安全管理办法（征求意见稿）》（“《办法》”）互为补充和支撑，搭建了一个更为全面的数据安全保护体系。同时，在《国家安全法》的基础上，本法作为在数据安全领域的专项法律，体现了国家立法层面对数据安全的高度重视。下文拟从《数安法》的保护客体、监管体系、规范行为及对象、数据跨境等主要方面作简要解读。

一、保护的客体

1.《数据安全法》与《办法》的保护客体比较

与去年公布的《办法》比较，《数安法》保护的客体范围更加广泛。首先，《数安法》所保护的客体不仅局限在《办法》所界定的网络数据范围，而且还包括线下物理场所存在的数据。其次，相对于《办法》所专注于“个人信息”和“重要数据”，《数安法》则普遍适用于所有数据。

以上区别的背后原因，笔者认为是因为《办法》作为《网络安全法》下位法，遵循了《网络安全法》主要规范数据自身安全（即网络数据的完整性、保密性、可用性）的思路，而《数

安法》更侧重于数据宏观安全，即从维护国家主权、安全和发展利益方面对数据进行有效保护和合法利用。

2.“数据”与“信息”的关系

另外，《数安法》将“数据”与“信息”的区别予以明确。《数安法》将“数据”定义为任何以电子或者非电子形式对信息的记录。可见，信息是数据所外在表现的内容，数据是底层载体或形式。以“个人信息”为例，《数安法》仅保护记录这些信息载体的合法使用与客观安全状态，而涉及这些载体之上具体内容的部分，即“信息”部分，则由《个人信息保护法》（正处于全国人大常委会审议阶段）等其他相关专门法律所规范。

3.数据安全保护的意义

平衡数据“发展/开放”与数据“安全”之间的关系是贯彻《数安法》全文的主要基调，因为数据的开发利用是数字经济发展的引擎，而数据安全事件又会给国家安全带来威胁和挑战。

a.数据是数字时代的“石油”

根据中国信通院 2019 年 10 月 11 日发布的《全球数字经济新图景（2019 年）》显示，全球数字经济蓬勃发展，在国民经济中占据核心地位，47 个国家数字经济总规模超过 30.2 万亿美元，占 GDP 比重高达 40.3%。

数字经济发展的关键要素是数据。今年 3 月 30 日《中共中央、国务院关于构建更加完善的要素市场优化配置体制机制的意见》中明确提出了数据成为土地、资本、劳动力及技术之外的第五大基本市场要素。今年 5 月 28 日全国人大通过的《民法典》就首次将数据和网络虚拟财产纳入保护范围，赋予数据一定的财产属性。因此，确保数据安全对我国的经济发展至关重要。

b.数据安全是国家安全的新领域

大数据带来了万物互联，但频频引发的各类数据安全事件也随之而来。其导致的后果既有对个人隐私的侵害，更有对国家安全的威胁。例如，2018 年脸书公司（Facebook）5000 万用户信息被泄露，被“剑桥分析”盗取用于大数据分析，影响了美国总统大选。所以，数据安全是国家安全治理的一个重要组成部分。

二、监管体系

在数据安全的监管方面，《数安法》构建了“一个顶点、多维度配合”的体系。

“一个顶点”即中央国家安全领导机构。该机构将针对全国的数据安全情况进行整体指导和战略规划，对具体涉及数据安全的主体进行间接管理。在具体的执行层面，直接监管机

构将接受中央国家安全领导机构的领导或指导。

“多维度配合”则指各地区、各部门、各行业、线上与线下的全方位、交叉监管：

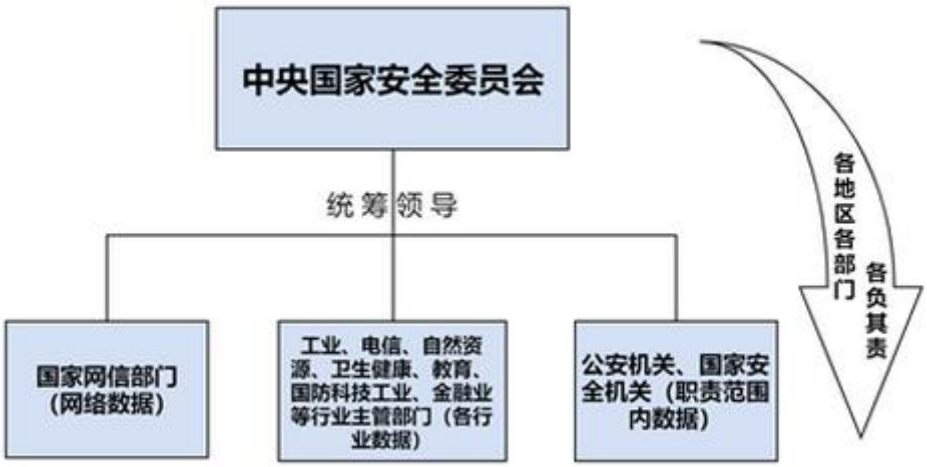
1.工业、电信、自然资源、卫生健康、教育、国防科技工业、金融业等行业主管部门将在本专业领域内针对特定事项进行监管；

2.公安机关、国家安全机关等在职责范围内进行监管；

3.国家网信部门将直接负责网络数据安全方面的监管，包括具体的日常监督、专项整改、管理细则的制定等等。

此外，笔者注意到虽然《网络安全法》与《数安法》同为《国家安全法》的下位法，但只有《数安法》强调其与《国家安全法》一样，均由中央国家安全领导机构间接管理。这可能也印证了《数安法》与《网络安全法》在规范客体和重心上的差异。

为了方便读者理解，笔者整理了如下结构图以说明监管体系之间的关系：



三、规范的行为及对象

1.规范的行为

《数安法》规范的“数据活动”包括：数据的收集、存储、加工、使用、提供、交易、公开等行为。与《办法》作比较，本法增加了加工、提供、交易、公开等四个环节，同时删除了《办法》中“纯粹家庭和个人事务除外”的规定。可见，《数安法》不仅将“数据活动”范围扩大，亦将单纯个人用途使用数据的行为纳入监管。

2.规范的对象

a.规范对象的范围

针对企业而言，目前蓬勃发展的大数据、云计算、人工智能、数据处理软件开发机构等将最直接地适用《数安法》。然而，从事数据活动的主体远不止上述这类企业，还有例如：

电商平台、数据交易中介这类企业会从事数据的收集、储存、提供等环节；社交软件类企业会从事数据的收集、储存、加工等环节；甚至企业 APP 或公众号，在运营中也会收集、储存用户的数据等。

整体上，《数安法》规范对象所涵盖范围很广，不仅企业，也包括涉及数据活动的机构、社会团体、政府部门，甚至个人。需要注意的是，《数安法》第 2 条采用了具有域外适用效力的条款，将违反或损害中国数据安全的境外机构也一并纳入管辖对象的范围。

b.规范对象的义务

为了方便读者理解，笔者汇总整理了各规范对象所对应的合规义务如下：

企业，社会团体，职能部门/机关/单位	个人	境外机构
1） 建立相关内部管理机制义务： a） 全流程数据安全管理制度； b） 数据安全负责人、负责部门机制（针对重要数据处理者）； c） 数据安全风险监测、风险报告、用户通知机制； d） 数据安全风险评估机制（针对重要数据处理者）； e） 有关数据来源,交易双方身份审核,交易数据记录等方面的数据交易合规经营机制（针对数据交易中介服务的机构）； **2） 员工培训义务：**应当定期组织开展数据安全教育培训； **3） 合法义务：**必须采取合法、正当的方式收集数据,不得损害国家安全或他人利益； **4） 配合义务：**在公安、国安等部门调取数据时予以配合； **5） 报告义务：**境外执法机构向其调取存储于中国境内的数据的，应及时报告； **6） 政务公开义务（针对国家机关）：**国家机关应制定政务数据开放目录,构建政务数据开放平台，及时、准确地公开政务数据。	**1） 合法义务：**必须采取合法、正当的方式收集数据,不得损害国家安全或他人利益； **2） 配合义务：**在公安、国安等部门调取数据时予以配合； **3） 报告义务：**境外执法机构向个人要求调取存储于中国境内的数据的，应及时报告。	**1） 合法义务：**必须采取合法、正当的方式收集数据,不得损害国家安全或他人利益。

四、数据跨境的“矛”与“盾”

由于经济全球化和互联网的天然属性，数据在不同国家和地区之间大规模、高频率的流动，数据全球化成为推动全球经济发展的重要力量。在地缘政治方面，美国“棱镜门”事件推动了各国政府将数据跨境流动与国家安全、国家主权等政策逐渐挂钩，加剧了世界各国在网络空间的战略博弈和数据资源争夺。在这方面，《数安法》构建了我国数据跨境流动的“矛”与“盾”。

1.域外追责及反制威慑 -- 跨境数据安全之“矛”

如前文所述，《数安法》在总则第 2 条中依据保护管辖原则，规定数据活动无论在境内还是境外，只要损害我国国家安全、他人合法权益的，就要依法追究法律责任。该规定赋予了《数安法》域外适用效力，与欧盟的《通用数据保护条例》（“GDPR”）有异曲同工之处。

依据国际法的对等原则，《数安法》第 24 条就国外采取与数据投资、贸易相关的歧视性措施时，赋予我国采取反制措施的权利。可以说是在数据安全“守”势的基础上保留了反击的主动权。

2.规范数据跨境流动 -- 跨境数据安全之“盾”

《数安法》第 10 条表明我国对数据跨境流动的基本态度，即在确保数据安全的前提下，促进跨境自由流动，同时积极开展该领域的国际交流与合作、参与国际规则和标准的制定。在数据出境方面，无论是《网络安全法》还是去年 6 月 13 日国家网信办《个人信息出境安全评估办法（征求意见稿）》都采用安全评估制度作为“安全阀”。而在数据入境方面，很多国家为了争夺数据资源也已经开展了积极的多边或双边谈判，谋求建立符合其利益的全球数据流动圈，例如欧盟 GDPR 项下的“充分性”认定名单、美国推动的《美墨加三国协议》(USMCA)、亚太经合作组织(APEC)的“跨境隐私规则”(CBPR)等。下一步如何打造好我国自己的数据跨境流动“朋友圈”是摆在我们面前的一个重要课题。

《数安法》第 23 条首次提出数据出口管制概念，即国家对与履行国际义务和维护国家安全相关的属于管制物项的数据依法实施出口管制。这实际上将去年 12 月 28 日《出口管制法（草案）》中的管制物项从“货物、技术、服务”扩大到“数据”，其目的类似美国的《2018 年出口管制法》和《出口管制条例》（EAR）项下对科技数据的出境限制。

《数安法》第 33 条提出了境外执法机构调取数据的报告批准制度。该制度实际上是回应了近年来很多国家，包括美国《澄清境外数据合法使用法案》（the Cloud Act）在内，不断扩大跨境数据调取权利的立法趋势，为我国数据安全提供了一定保障。需要注意本条款虽然在字面上均可归入数据出境范围，但是与上文中《网络安全法》和《个人信息出境安全评估

办法（征求意见稿）》中的数据出境活动不同。因为本法第 33 条涉及的境外数据接收者是境外执法机构，而其活动涉及中国国家主权，理应适用更为严格的出境限制。

五、结语

当前国际形势复杂多变，特别是新冠疫情给世界主要经济体造成巨大冲击，全球面临经济大衰退。然而，数字经济以其高融合、高技术、高增长等特性，将成为我国经济发展的新引擎。数字经济的要素是数据，数据也是国家基础性战略资源，没有数据安全就没有国家安全。为了应对数据这一非传统领域的国家安全风险与挑战，《数安法》应运而生，旨在通过立法提升国家数据安全保障能力，维护国家主权、安全和发展利益。综上，《数安法》项下的数据安全不仅担当了数字经济压舱石这一重任，还赋予了国家安全一个全新的监管维度。

（来源：关键基础设施安全应急响应中心）

➢ 3·15 曝光：手机插件化身信息“窃贼”，智能生成“虚假”广告……

2020 年 7 月 16 日，今年 3·15 晚会的主题是“凝聚力量、共筑美好”，就是要凝聚政府、企业、社会和每一位消费者的力量，用法治的力量构筑良好的经济生态，保民生，促消费。相比于以往，今年的“3•15”晚会更积极关注新产业、新业态和新消费模式。本场晚会由中央广播电视总台、最高人民法院、最高人民检察院、中央网络安全和信息化委员会办公室、国家发展和改革委员会、工业和信息化部、公安部、司法部、农业农村部、商务部、国家市场监督管理总局、中国消费者协会等政府部门和机构共同主办。**昨晚，被点名曝光的重点现象有：**

- 海参“水深”：海参养殖放敌敌畏、南方海参当北方的卖
- “过期”的汉堡王：用过期面包做汉堡，鸡腿排保质期随意改
- 毛巾的正反面：生产线的暗黑面，旧袜子旧内衣竟是毛巾生产原料
- 没完没了的变速箱故障：变速箱故障频发，消费者投诉无门
- 精装修还是“惊”装修：精装房漏成水帘洞
- 套路推销，插翅难逃：美容院推销“步步惊心”
- 趣头条广告藏猫腻，赌博广告暗藏其中
- 手机软件藏窃贼，SDK 插件偷窥用户隐私
- 嗨学网退费为何这么难

其中，在线教育、AI 广告推送、手机 APP 等科技业态，早已渗透人们的日常生活，但是嗨学网难退费、趣头条常违规、手机插件窃取隐私等问题，却在“隐秘的角落”里威胁着人们的信息安全和利益。

手机“窃贼”插件

据 3·15 晚会报道，SDK，是在手机软件中，提供某种功能或服务的插件，2019 年 11 月，上海市消费者权益保护委员会委托第三方公司对一些手机软件中的 SDK 插件进行了专门的测试，却发现一些 SDK 暗藏玄机。

据悉，技术人员检测了 50 多款手机软件，这些软件中分别含有上海氪信信息技术有限公司和北京招彩旺旺信息技术有限公司两家公司的 SDK 插件。这两个插件，都存在在用户不知情的情况下，偷偷窃取用户隐私的嫌疑，涉及国美易卡、遥控器、最强手电、全能遥控器、91 极速购、天天回收、闪到、萝卜商城、紫金普惠等 50 多款手机软件。

天天回收	1.4.0	闪到	
萝卜商城	2.0.0	紫金普惠	
信用金库	1.1.7	有货淘	
秒贷钱包	1.0.8	口袋钱包	
蜂王贷	1.0.0	小猪花	
我闪花	1.0.3	有钱用	
青木易贷	1.0.0	秒贝	
莫愁花	3.45	乐趣	
捷云速贷	1.0.0	来闪贷	
银河闪贷	2.1.0	贷钱吧	
抱金猪	2.2.1	千禧一贷	
小蟹钱	1.0.3	芝麻海购	

检测人员表示：“这些插件会读取设备的 IMEI、IMSI、运营商信息、电话号码、短信记录 、通讯录、应用安装列表和传感器信息。”而这只是第一步而已，读取完成后，其还会悄悄地将数据传送到指定的服务器存储起来。北京招彩旺旺信息技术有限公司的 SDK 甚至涉嫌通过菜谱、家长帮、动态壁纸等多款软件，窃取用户更加隐私的信息。

检测人员解释道：“（插件）还会未经用户同意，收集用户的联系人、短信、位置、设备信息等等。尤其短信，短信内容被全部传走，这个是很严重的。”

因为 SDK 能够收集用户的短信，以及应用安装信息，一旦用户有网络交易的验证码被获取，极有可能造成严重的经济损失。此外，虽然 SDK 只是一个看似普通的插件，但是因为它对所有的手机 APP 具有通用性，很多手机软件可能都嵌入了同一个 SDK，因此一旦某个 SDK 窃取用户个人隐私，将会涉及众多手机软件。在此次检测当中，除了内嵌 SDK 插件以外，工作人员还发现一些知名手机 APP 也有收集用户隐私的现象，涉及酷音铃声、手机铃声、铃声大全等多款软件。

趣头条广告乱象

趣头条是一款知名内容资讯 App，公司成立于 2016 年，2018 年 9 月 14 日登陆美股纳斯达克。趣头条靠网赚模式起家，瞄准下沉市场，两年积累上亿用户，其收入主要来自广告。央视记者调查发现，趣头条平台存在很多违法违规广告，涉嫌虚假推广，比如号称 10 万瘦身体验装免费领取，可快速减肥，月瘦 30 斤，永不反弹的“代用茶”。但是，这样的“代用茶”根本不符合规范，属于虚假产品。

记者找到一家名叫广州天拓网络技术公司的中间方，提供了一款杜撰的减肥产品名称，天拓公司根本不经审核，就自动生成了一条图文并茂的广告，并轻松投放到趣头条。天拓公

司表示，广告投放商就算没有资质，也可以为其在趣头条开户，这样的广告在趣头条上一般都能收到很好的广告效果。

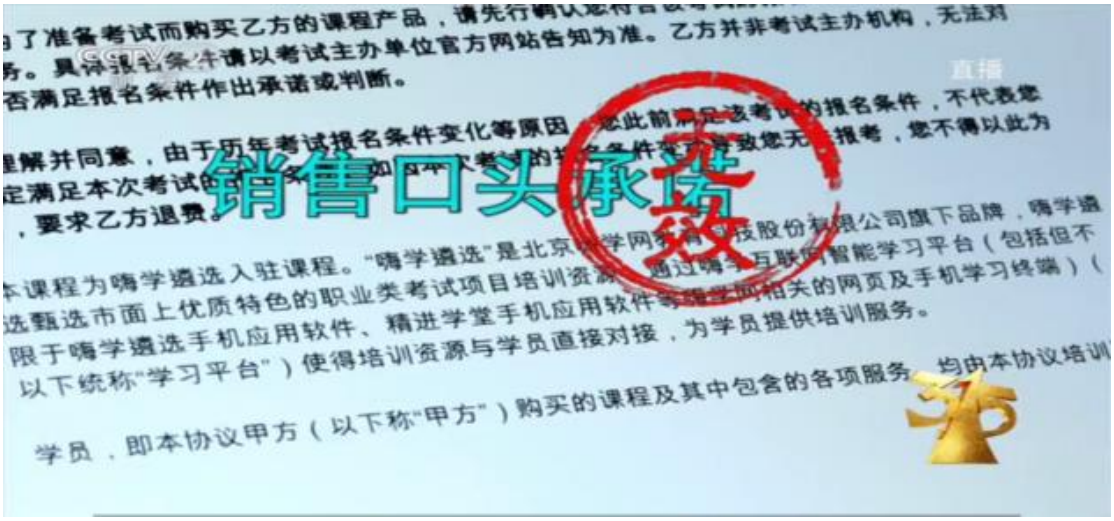
报道显示，在趣头条的推荐、视频、育儿、养生等栏目均充斥着类似的广告。为了逃避监管，此类广告投放一般规避审核严格的一线城市。

除了虚假减肥产品，在趣头条上，还充斥着很多宣称轻松赚钱的夸张视频广告。但是，通过广告所提供的联系方式与对方取得联系后，打开对方提供的网址，看到的却是非法赌博平台。

一家号称专注企业全媒体智能广告投放的聚亿媒网络科技有限公司，就提供将非法赌博的平台链接通过网赚形式的广告投放至趣头条的服务。投放同样会规避风险期，规避监管。对此，趣头条昨日晚间表示，对于央视指出的问题，公司(上海基分文化传播有限公司)已迅速成立广告生态治理专项工作组，正在对平台涉及的广告进行全平台彻查，一旦发现相关问题，坚决严厉清查和封禁。

嗨学网成在线教育新“忽悠”

2019 年初，成都的潘女士被嗨学网的广告所吸引，声称只要通过嗨学网的培训，就有机会考到国家一级注册消防工程师证，每年都会有一笔不小的收入。潘女士在中国人事考试网查询发现，自己根本没有参加该项考试的资格。但嗨学网销售却表示，找代报名机构肯定能报上名。于是潘女士交了 4498 元，购买了嗨学网的网络培训课程。然而考试日期临近，她的报名信息一直没有通过，退款又困难重重。



之后，在记者的陪同下，潘女士前往嗨学网总部申请退款。面对确凿的证据，嗨学网客户投诉部门鲁经理在仔细看了潘女士提供的和嗨学网销售的聊天记录后，承认是他们的销售存在违规，但多只能退 80%的费用。但很快，出现的另一位女负责人直接推翻了鲁经理退款 80%的承诺，并表示只能退 50%。

在进行深度揭秘后，记者发现，嗨学网的销售在推销时，信口开河虚假宣传，并且故意选择微信语音等难以留存实际证据的方式，并在引导用户付款时故意让用户忽略查看协议具体内容。一旦交了钱，当学员们发现上当受骗要求退钱时，嗨学网的投诉部门则会拿出协议，否定之前销售们的各种口头承诺。

嗨学网的销售人员最后还表示：“这些事情你自己弄明白了就知道，其实根本是在骗他们。说白了，就是在骗人。没关系，反正我们公司这么大，我们都可以帮你解决的，什么大风大浪没见过。”

疫情给了在线教育一次高速发展的机会，在线教育用户规模从 2016 年的 1.04 亿人，增加到 2019 年 2.61 亿人，预计 2020 年将突破 3.09 亿人。有机构预测在线教育的市场规模在两年后将达到 5400 亿元。然而，任何产业是否能够走得更远、走的更好，完全在于能否真正满足消费者的需求，为用户提供更诚信的商品，一旦用户失去了信任，则为时晚矣。

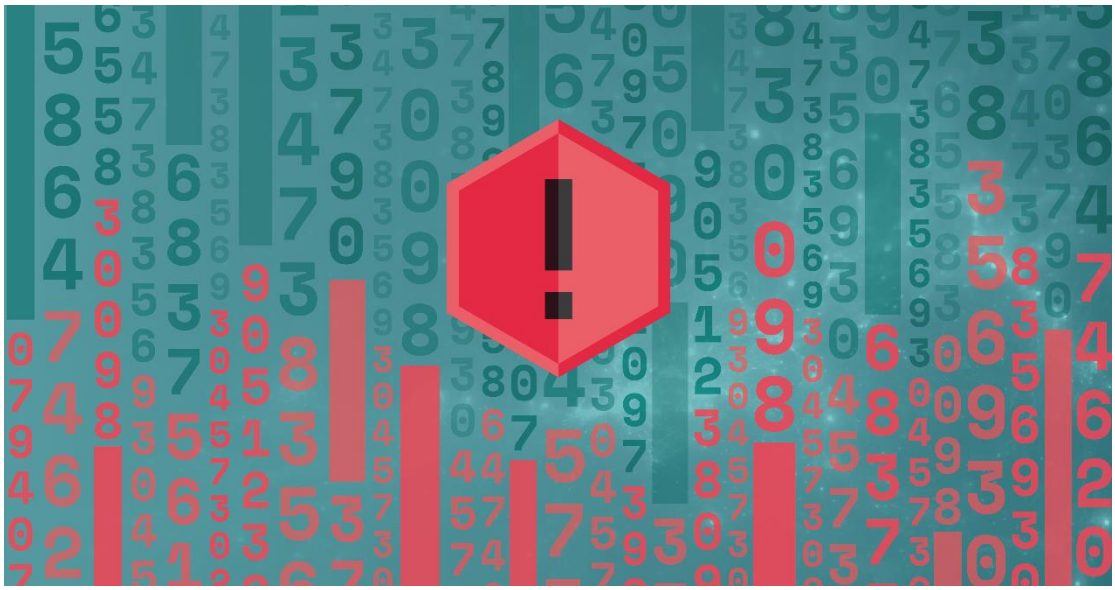
写在最后

今年 3·15 晚会也提到，根据国家统计局刚刚发布的数据，今年二季度中国 GDP 由负转正，同比增长 3.2%。在中国经济稳步增长的过程中，数字经济功不可没。但与此同时，还有很多新的消费需求需要满足。在今年前半年中，厨师机、VR 健身环等产品销量增长迅速，乡村电商、带货直播等逐步流行，AI+在线教育也成为满足个性化需求的关键手段，在线教育、在线办公、互联网诊疗成为数字时代新时尚。毫无疑问，科技将进一步解放人们的生产

力，数字经济也将成为增强中国经济长期向好新动能。但科技向善，在用好技术的同时，切勿走向歧途……（来源：爱心学社）

➢ 数据安全法：不能等到数据泄露、滥用到危害安全的地步才开始治理

2020 年 7 月 2 日，工业和信息化部信息通信管理局发布《关于侵害用户权益行为的 APP 通报（2020 年第二批）》，曝光智慧树、纳米盒、乐学高考、洋葱学院等 15 款 App 存在过度索取权限、私自收集个人信息等问题。而就在一个多月前的 5 月 14 日，工业和信息化部信息通信管理局才发布《关于侵害用户权益行为的 APP 通报（2020 年第一批）》，点名知乎日报、当当、e 代驾、好医生等 16 款 App 存在私自收集个人信息、私自共享给第三方等问题。



2019 年 12 月，App 专项治理工作组经评估发现，57 款 App 存在收集使用个人信息问题，其中包括链接、搜狐浏览器、有道云笔记、猎聘、腾讯课堂、浦发信用卡、时光网、微医等。在这 57 款 App 中，有 49 款 App 涉及既未经用户同意，也未作匿名化处理，通过客户端嵌入软件开发工具包（SDK）向第三方提供用户设备 IMEI 号、MAC 地址、地理位置、通讯录、应用程序列表等个人信息。

当个人信息被手机 App、各类网站等频繁私自收集之时，一个更令人不安而且愤怒的事是，个人信息被打包在数据黑市上兜售。央视早前就曝光过，个人全套信息在黑市上仅售三元。这些被泄露的个人信息不仅仅被用于精准营销，更为犯罪分子实施违法犯罪提供了便利。

一、数据安全问题频发

中国消费者协会于 2018 年发布的《App 个人信息泄露情况调查报告》显示，遇到过个

人信息泄露情况的人数占比为 85.2%。侵犯公民个人信息已经逐渐形成了“源头—中间商—非法使用”的庞大地下黑色产业链。除了非法数据利用者，企业“内鬼”、数据中间商也在这条黑色产业链中扮演着重要角色。相较于传统个人身份识别类静态个人信息，个人活动类动态个人信息的比重开始增加；获取手段也从诱骗、脱库向非法爬取数据等方式转变。

在过去的两年中，数据隐私和数据安全问题频发。支付宝年度账单默认勾选《芝麻服务协议》被质疑侵犯隐私权；百度涉嫌侵害消费者个人信息安全被江苏省消保委提起公益诉讼；大规模数据泄露事件引发了全民的安全担忧，包括华住酒店集团近 5 亿条用户信息被泄露，12306 网站 470 余万条用户数据在网络上被贩卖。

与个人信息相关的犯罪也屡见不鲜，如上市公司数据堂涉嫌侵犯公民个人信息罪被查，简历大数据公司巧达科技非法交易个人信息达数亿条，猎头搜涉嫌非法交换就业者数据，魔蝎科技、天翼征信涉嫌利用网络爬虫技术侵犯个人隐私，拉卡拉征信涉嫌非法缓存公民个人信息，这些都引起社会的广泛关注。

另外，算法涉及的伦理问题也开始显现，“同房不同价”等大数据“杀熟”让相关企业备受争议，大数据让“价格歧视”具有了现实可能性；“精准营销”更是令人胆战心惊，明明只是在电商平台上搜索过某商品，新闻资讯类 App 上却出现了相同商品的广告。

近几年，包括 Facebook、英国航空公司、万豪集团等在内的公司也频频发生数据泄露事件，其泄露的数据量级惊人。根据调研机构 Audit Analytics 近期发布的报告《网络安全事件披露趋势》，2011 年以来的 639 起上市公司网络安全事件中，平均每起网络数据泄露事件的损失高达 1.16 亿美元。然而，遭遇数据泄露的公司中几乎有一半（43％）却选择隐瞒不报。

二、保持数据流动，但不能忽视对数据权利的保护

在大数据人工智能时代，数据作为基础生产要素的重要性是不言而喻的。在企业生产经营中，各类数据往往起着至关重要的作用。企业在制定战略、具体开展经营过程中，都必然以数据及数据分析作支撑。

数据泄露等事件的发生，不仅有损涉事企业的经营利益，更有害于个人利益和社会秩序，但这并不意味着应该组织数据的开发利用等数据流动行为。事实上，实现数据权利保护与数据流动的平衡是数据法学的首要核心议题。欧盟《通用数据保护条例》（GDPR）第 1 条第 1 款就开宗明义地指出，“本条例旨在确立个人数据处理中的自然人保护和数据自由流通的规范”；紧接着，第 1 条第 2 款强调，“本条例旨在保护自然人的基本权利和自由，尤其是保护个人的数据权利”；而第 1 条第 3 款则确认了平衡的重要性，即“个人数据在欧盟境内的自由流通不得因为在个人数据处理过程中保护自然人而被限制或禁止”。

2020 年 6 月 28 日，提交十三届全国人大常委会第二十次会议审议的《数据安全法（草案）》第 1 条也规定：“为了保障数据安全，促进数据开发利用，保护公民、组织的合法权益，维护国家主权、安全和发展利益，制定本法。”第 5 条更是明确规定：“国家保护公民、组织与数据有关的权益，鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以数据为关键要素的数字经济发展，增进人民福祉。”

可以说，让数据完全不流动是不可能的，也不符合国家利益，对于一般性数据在风险评估基础之上应该允许其流动，安全等级“一刀切”将会影响我国数字经济发展，所以要坚持安全与发展并重。安全是底线，发展是目标。

不过，数据流动和利用的前提和基础是个人数据权利的保护。虽然我国《民法典》第一编“总则”第五章“民事权利”提到了“数据”，第四编“人格权”第六章专门规定了隐私权和个人信息保护，但只是把“数据”和“个人信息”看作“民事权益”，“是否要上升为权利”有待于法律的另行规定。然而，保护个人的数据权利应该说是不容置疑的。

二战期间，美国总统罗斯福在发表国情咨文演讲时提出“免于匮乏的自由”和“免于恐惧的自由”，其关键点可以归纳为两个字“安全”，并且这种“安全”被视为实现基本权利和自由的条件和保证。这个原理在数据法领域也同样适用。

自由放任的数据市场只是神话，无法形成自生自发的自然秩序。在两极分化的数据世界里，能力受限的数据主体根本无力对抗作为数据垄断者的数据控制者和处理者。只有通过国家提供的法律框架，不断赋予数据主体各种数据权利，数据法律秩序才能实现。如果没有国家对数据权利的保障，数据黑市的流行将不可避免；如果没有国家通过法律提供一个“以数据权利为基础的安全环境”，数据主体将因缺乏控制数据的能力，不可能获得真正的数据自由。

因此，在个人数据广受威胁和侵害的人工智能时代，作为数据主体的我们非常有必要为数据权利而斗争。正如耶林所说的，“世界上一切权利都是经过斗争而得来的”。数据权利也是如此，斗争也正是数据法律的生命。为数据权利而斗争也是数据主体的义务，主张数据权利是道德上自我保护的义务，完全放弃数据权利，是数据世界的道德自杀。

同样，为数据权利而斗争对国家的数字经济发展具有重要意义，“只有每个人都拥有健全有力的法感，国家才会有丰富的力量源泉，才会在国内外具有最可靠的保障。法感就如同整棵大树的根，如果树根发挥不了作用，大树就会在岩石与沙砾中枯死，所有其他一切都会成为泡影。一旦暴风雨来临，整棵大树将会被连根拔起。”在数据法领域，数字经济就是具有“显而易见的优点”的“树干”和“数冠”，而数据权利则是“深藏土地不被人看见却发

挥重要作用”的“树根”。

三、要么坐牢，要么没事？

据全国人大常委会法工委发言人介绍，《数据安全法（草案）》主要涉及以下内容：一是，确立数据分级分类管理以及风险评估、监测预警和应急处置等数据安全管理各项基本制度；二是，明确开展数据活动的组织、个人的数据安全保护义务，落实数据安全保护责任；三是，坚持安全与发展并重，规定支持促进数据安全与发展的措施；四是，建立保障政务数据安全和推动政务数据开放的制度措施。其中，明确开展数据活动的组织与个人有数据安全保护的义务和责任，弥补了我国当前在这方面的法律空白。

当前我国刑法仅对买卖、交易个人信息作出处罚，并没有详细涉及数据泄露问题。面对诸如 2018 年华住酒店 5 亿条信息泄露这样的大范围数据泄露事件，我国目前法律框架不管是刑法还是网络安全法，都没有规定企业要承担什么责任。这使得实践中对于涉及数据问题，出现“要么坐牢，要么没事”的现象，导致一些企业、个人铤而走险。

《数据安全法（草案）》提出，开展数据活动的组织、个人不履行数据安全保护义务或者未采取必要的安全措施的，由有关主管部门责令改正，给予警告，可以并处一万元以上十万元以下罚款，对直接负责的主管人员可以处五千元以上五万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

这实际是在逼迫企业提升数据安全等级，否则一旦发生泄露就要面临相当严重的处罚。在 Facebook 剑桥分析事件中，美国监管机构对 Facebook 实施了 50 亿美元的处罚；英国航空公司仅泄露几百万数据就被欧盟罚了两亿美元。相比这种力度，我国对企业数据泄露的处罚力度还有待加强。（来源：数据法盟）

四、政府之声

➢ 国务院办公厅印发《国务院 2020 年立法工作计划》

2020 年 7 月 8 日，国务院办公厅关于印发国务院 2020 年立法工作计划的通知[国办发〔2020〕18 号]。**以下为通知全文：**


中华人民共和国中央人民政府
www.gov.cn

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 > 信息公开 > 国务院文件 > 公安、安全、司法 > 司法

索 引 号：000014349/2020-00054　　主题分类：公安、安全、司法\司法
发文机关：国务院办公厅　　成文日期：2020年06月26日
标　　题：国务院办公厅关于印发国务院2020年立法工作计划的通知
发文字号：国办发（2020）18号　　发布日期：2020年07月08日
主 题 词：

国务院办公厅关于印发
国务院2020年立法工作计划的通知
国办发〔2020〕18号

各省、自治区、直辖市人民政府，国务院各部委、各直属机构：
《国务院2020年立法工作计划》已经党中央、国务院同意，现印发给你们，请认真贯彻

2020 年是决胜全面建成小康社会和“十三五”规划收官之年。国务院 2020 年立法工作的总体要求是：在以习近平同志为核心的党中央坚强领导下，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、四中全会精神，认真贯彻习近平总书记全面依法治国新理念新思想新战略，增强“四个意识”、坚定“四个自信”、做到“两个维护”，坚持党的领导、人民当家作主、依法治国有机统一，围绕坚持和完善中国特色社会主义制度、推进国家治理体系和治理能力现代化，紧扣全面建成小康社会目标任务，助力统筹推进新冠肺炎疫情防控和经济社会发展工作，坚持稳中求进工作总基调，加强党对立法工作的领导，坚持底线思维，完善立法体制机制，提高立法质量，加快立法步伐，为全面建成小康社会和“十三五”规划圆满收官奠定坚实法律基础，为开启全面建设社会主义现代化国家新征程提供有力法治保障。

一、围绕坚持和完善中国特色社会主义制度、推进国家治理体系和治理能力现代化，科学合理安排立法项目

中国特色社会主义制度是党和人民在长期实践探索中形成的科学制度体系，具有强大生命力和巨大优越性，是当代中国发展进步的根本保障。坚持和完善中国特色社会主义法治体系，对于坚持和完善中国特色社会主义制度、推进国家治理体系和治理能力现代化具有重大意义。建设中国特色社会主义法治体系，必须加强和改进立法工作，发挥立法的引领和推动

作用，抓紧制定国家治理体系和治理能力现代化急需的制度、满足人民对美好生活新期待必备的制度，推动中国特色社会主义制度不断自我完善和发展、永葆生机活力。要突出坚持和完善支撑中国特色社会主义制度的根本制度、基本制度、重要制度，着力固根基、扬优势、补短板、强弱项，构建系统完备、科学规范、运行有效的制度体系。要全面贯彻实施宪法，深化宪法学习宣传教育，以完备的制度推动和保证宪法实施，维护宪法权威。要完善立法体制机制，坚持科学立法、民主立法、依法立法，完善党委领导、人大主导、政府依托、各方参与的立法工作格局，坚持立改废释并举，不断提高立法质量和效率。要完善以宪法为核心的中国特色社会主义法律体系，加强重要领域立法，加快我国法域外适用的法律体系建设，以良法推动发展、保障善治。要处理好改革与法治的辩证关系，以立法引领和保障改革，确保党中央关于全面深化改革的各项决策部署落到实处。**为此，对国务院 2020 年立法项目作出如下安排：**

——围绕坚持和完善社会主义基本经济制度，推动经济高质量发展，提请全国人大常委会审议印花税法草案，制定保障中小企业款项支付条例、私募投资基金管理暂行条例、非存款类放贷组织条例、城市公共交通条例、农作物病虫害防治条例，修订企业信息公示暂行条例、国家科学技术奖励条例、粮食流通管理条例，修订与外商投资法不符的行政法规。中国人民银行法修订草案、商业银行法修订草案、反洗钱法修订草案、保险法修订草案、公路法修订草案预备提请全国人大常委会审议。

——围绕坚持和完善繁荣发展社会主义先进文化的制度，巩固全体人民团结奋斗的共同思想基础，提请全国人大常委会审议著作权法修订草案，制定未成年人网络保护条例，修订水下文物保护管理条例。文化产业促进法草案预备提请全国人大常委会审议。

——围绕坚持和完善统筹城乡的民生保障制度，满足人民日益增长的美好生活需要，提请全国人大常委会审议退役军人保障法草案、社会救助法草案、教育法修正草案、农产品质量安全法修订草案，制定消费者权益保护法实施条例、医疗保障基金使用监督管理条例、生物技术研究开发安全管理条例、生物医学新技术临床研究和转化应用管理条例、化妆品监督管理条例、建设工程抗震管理条例，修订民办教育促进法实施条例、医疗器械监督管理条例。

——围绕坚持和完善共建共治共享的社会治理制度，保持社会稳定、维护国家安全，提请全国人大常委会审议治安管理处罚法修订草案、安全生产法修正草案、海上交通安全法修订草案、监狱法修订草案，制定社会组织登记管理条例、关键信息基础设施安全保护条例、无人驾驶航空器飞行管理暂行条例，修订地名管理条例。

——围绕坚持和完善生态文明制度体系，促进人与自然和谐共生，制定地下水管理条例，

修订土地管理法实施条例。

——围绕坚持和完善党对人民军队的绝对领导制度，确保人民军队忠实履行新时代使命任务，提请全国人大常委会审议兵役法修订草案。深化国防和军队改革需要提请全国人大常委会审议的其他法律草案，以及需要制定、修订的行政法规，适时提请国务院、中央军委审议。

——围绕坚持和完善独立自主的和平外交政策，推动构建人类命运共同体，制定领事保护与协助条例，开展有关国际条约审核工作。

——围绕坚持和完善党和国家监督体系，强化对权力运行的制约和监督，提请全国人大常委会审议审计法修订草案。

——围绕坚持和完善中国特色社会主义行政体制，构建职责明确、依法行政的政府治理体系，提请全国人大常委会审议行政复议法修订草案，制定政府督查工作条例。

为健全国家公共卫生应急管理体系、强化公共卫生法治保障，保护人民群众生命安全和身体健康，着力完善疫情防控相关立法，加强配套制度建设，构建系统完备、科学规范、运行有效的疫情防控法律体系。提请全国人大常委会审议国境卫生检疫法修订草案、传染病防治法修订草案、突发事件应对法修订草案。进出境动植物检疫法修正草案预备提请全国人大常委会审议。配合全国人大常委会制定生物安全法等法律，修改野生动物保护法、动物防疫法、畜牧法、执业医师法等法律，修改相关配套行政法规。

抓紧做好政府职能转变和“放管服”改革、优化营商环境等涉及的法律法规清理工作。对于党中央、国务院交办的其他立法项目，抓紧办理，尽快完成起草和审查任务。对于其他正在研究但未列入立法工作计划的立法项目，由有关部门继续研究论证。

二、完善立法体制机制，加强和改进新时代行政立法工作

牢牢坚持党中央对立法工作的集中统一领导。中国共产党领导是中国特色社会主义最本质的特征，是中国特色社会主义制度的最大优势，党是最高政治领导力量。要增强“四个意识”、坚定“四个自信”、做到“两个维护”，自觉在思想上政治上行动上同以习近平同志为核心的党中央保持高度一致。要严格执行立法工作向党中央请示报告制度，凡重大立法事项，立法涉及的重大体制、重大政策调整，以及需要由党中央研究的立法中的重大问题，按照规定向党中央请示报告。立法工作计划、重要立法项目按照要求提交中央全面依法治国委员会审议或审批。要推进党的领导入法入规，以立法推动完善党领导各项事业的具体制度，把党的领导落实到统筹推进“五位一体”总体布局和协调推进“四个全面”战略布局各方面。

建立健全立法风险防范机制。立法工作与国家安全、政治安全、社会稳定息息相关，必

须坚持总体国家安全观，坚持底线思维，高度重视、预先防范立法可能带来的重大风险隐患。要加强立法战略研究，对立法时机和各环节工作推进时机进行综合考虑和评估论证。要将党建工作与立法工作高度融合，筑牢党员干部思想防线，提升防范化解重大风险的本领和能力。

深入推进科学立法、民主立法、依法立法。建设中国特色社会主义法治体系，发挥立法的引领和推动作用，必须抓住提高立法质量这个关键。要把好立法入口关，加强对立法项目的评估论证，起草部门报国务院的制定类立法项目送审稿需附立法前评估报告，修改类立法项目送审稿需附立法后评估报告，充分考虑立法的必要性、可行性和潜在风险。要坚持立改废释并举，加强涉及人民群众生命安全和身体健康的立法修法工作，切实解决相关规定该硬的不硬、该严的不严、该重的不重等问题。在立法过程中，要科学评估拟设立制度对各类企业、行业可能产生的影响，充分听取有代表性的企业和行业协会商会以及律师协会的意见。要探索开展基层立法联系点建设，充分发挥基层立法联系点接地气、聚民智的作用，畅通民意反映渠道，丰富民主立法形式。要严格依法立法，确保立法符合宪法精神和上位法规定，确保权限合法、程序合法、内容合法。

切实做好法规规章备案审查工作。备案审查工作是维护国家法制统一、政令畅通的重要方式。要健全完善备案审查制度，提高法规规章备案审查工作科学化、制度化、规范化水平。要综合运用依职权审查、依申请审查等方式，着重对地方性法规、地方政府规章、部门规章是否超越权限、是否违反上位法的规定等进行审查，对发现的问题坚决依法作出处理。要提高信息化水平，探索运用信息技术手段提高审查精准度，提升工作质效。

大力加强行政立法宣传工作。立法宣传是普及法律法规、凝聚社会共识、推动全民守法的有效途径。要把法治宣传教育嵌入到立法工作当中，通过新闻发布、专家解读、媒体宣传、公开征求意见等丰富多样的形式，解读法律法规，回应群众关切，弘扬法治精神，把立法和修法的过程变成普法的过程。要探索建立年度重点新法专项宣传制度，配合立法进程开展集中普法宣传。要建立健全重点法律法规规章公布时同步解读机制，作为法律法规规章出台的必备配套环节。要积极开展我国法律法规规章对外宣传和翻译工作，讲好中国立法故事。

三、抓好立法工作计划的贯彻执行

国务院各部门要深刻认识做好立法工作对于坚持和完善中国特色社会主义制度、推进国家治理体系和治理能力现代化的重大意义，高度重视立法工作计划的贯彻执行。要加强组织领导、完善工作机制、压紧压实责任、加强沟通协调，集中精力高质高效按时完成重点立法项目。

起草部门要重视法制工作机构建设，配齐配强立法工作人员，提高立法工作能力和水平。

要提高送审稿质量，严格按照立法法、行政法规制定程序条例等规定，做好向社会公开征求意见工作，及时上报送审稿、立法评估报告等相关材料，为审查、审议等工作预留合理时间。送审稿涉及其他部门的职责或者与其他部门关系紧密的，起草部门应当与有关部门充分协商，涉及部门职责分工、行政许可、财政支持、税收优惠政策的，应当征得机构编制、审改、财政、税务等相关部门同意。报送送审稿前，起草部门应当与司法部做好沟通，如实说明征求意见、协调分歧等情况。未沟通就报送送审稿的，司法部可以就是否启动审查工作向国务院提出意见和建议。

司法部要加强与起草部门的沟通，及时跟踪了解立法工作计划执行情况，加强组织协调和督促指导。有关部门报送的送审稿存在行政法规制定程序条例规定的退件情形的，司法部可以按照规定将送审稿退回起草部门重新研究。对于争议较大的立法事项，司法部要加大协调力度，提高协调层级，妥善处理分歧，敢于在矛盾焦点问题上“切一刀”。经过充分协调仍不能达成一致意见的，司法部、起草部门应当将争议的主要问题、有关部门的意见以及司法部的意见及时按程序请示报告。（来源：中国政府网）

附件：《国务院 2020 年立法工作计划》明确的立法项目及负责起草的单位

- **国务院办公厅关于印发国务院 2020 年立法工作计划的通知**
- **全文：**http://www.gov.cn/zhengce/content/2020-07/08/content_5525117.htm

➢ 国家网信办启动 2020“清朗”未成年人暑期网络环境专项整治

2020 年 7 月 13 日，2020 年暑期在即，为给广大未成年人营造健康的上网环境，推动网络生态持续向好，国家网信办决定即日起启动为期 2 个月的“清朗”未成年人暑期网络环境专项整治。

国家网信办有关负责人介绍，此次专项将重点整治学习教育类网站平台和其他网站的网课学习版块的生态问题，深入清理网站平台少儿、动画、动漫等频道的不良动画动漫产品，严厉打击直播、短视频、即时通讯工具和论坛社区环节存在的涉未成年人有害信息，从严整治青少年常用的浏览器、输入法等工具类应用程序恶意弹窗问题，严格管控诱导未成年人无底线追星、拜金炫富等存在价值导向问题的不良信息和行为，集中整治网络游戏平台实名制和防沉迷措施落实不到位、诱导未成年人充值消费等问题，持续大力净化网络环境。

近日，根据网民举报，国家网信办针对“学而思网校”APP 存在低俗视频、教唆早恋内容等突出问题，指导北京市网信办会同属地教育主管部门，依法约谈网站负责人，责令限期整改，完善信息安全制度，加强内容审核，切实落实主体责任。

国家网信办有关负责人表示，我国未成年人网民数量与占比持续上升，对网络内容监督管理、家庭上网教育、互联网企业针对性保护机制提出了更高的要求，还需社会各界共同关注和参与。欢迎广大网民、媒体和社会各界积极参与监督举报，为广大未成年人营造健康的网络环境。（来源：中国网信网）

- **关于开展 2020“清朗”未成年人暑期网络环境专项整治的通知**
- **全文：**http://www.cac.gov.cn/2020-07/13/c_1596175859026231.htm

➢ 工信部印发《工业互联网专项工作组 2020 年工作计划》的通知

2020 年 7 月 10 日，工信部工业互联网专项工作组办公室印发《工业互联网专项工作组 2020 年工作计划》的通知[工信厅信管函〔2020〕153 号]。

《工业互联网专项工作组 2020 年工作计划》包含十项任务类别、具体举措五十四项，

涉及提升基础设施能力、构建标识解析体系、建设工业互联网平台、突破核心技术标准、培育新模式新业态、促进产业生态融通发展、增强安全保障水平、推进开放合作、加强统筹推进、推动政策落地。（来源：中华人民共和国工业和信息化部）

- **关于印发《工业互联网专项工作组 2020 年工作计划》的通知全文：**
- http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757020/c8001762/content.html

➢ 国家保密局《涉密信息系统集成资质管理办法》公开征求意见

2020 年 7 月 2 日，国家保密局指导管理司发布关于就《国家秘密载体印制资质管理办法（征求意见稿）》、《涉密信息系统集成资质管理办法（征求意见稿）》公开征求意见的通知。

《通知》称：为贯彻落实国务院行政审批“放管服”改革精神，进一步规范和加强保密资质管理工作，我们研究制定了《国家秘密载体印制资质管理办法（征求意见稿）》、《涉密信息系统集成资质管理办法（征求意见稿）》，现向社会公开征求意见。（来源：国家保密局）

- **关于就《国家秘密载体印制资质管理办法（征求意见稿）》、《涉密信息系统集成资质管理办法（征求意见稿）》公开征求意见的通知全文：**
- http://www.gjbmj.gov.cn/n1/2020/0701/c409099-31767212.html

五、本期重要漏洞实例

➢ Microsoft 发布 2020 年 7 月安全更新

发布日期：2020-07-14
更新日期：2020-07-14
描述：

CVE(CAN) ID: CNTA-2020-0014

7 月 14 日，微软发布了 2020 年 7 月份的月度例行安全公告，修复了其多款产品存在的 123 个安全漏洞。受影响的产品包括：Windows 10 2004 & WindowsServer v2004（86 个）、Windows 10 1909 & WindowsServer v1909（86 个）、Windows 10 1903 & WindowsServer v1903（86 个）、Windows Server 2012（48 个）、Windows 8.1 & Server 2012 R2（48 个）、Windows RT 8.1（42 个）、Microsoft Edge (EdgeHTML-based)（2 个）、Internet Explorer（2 个）和 Microsoft Office-related software（14 个）。利用上述漏洞，攻击者可利用漏洞进行欺骗，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。

CVE 编号	公告标题和摘要	最高严重等级和漏洞影响	受影响的软件
CVE-2020-1350	**Windows DNS Server 远程代码执行漏洞** Windows Domain Name System servers 未能正确处理请求时，存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在本地系统帐户的上下文中运行任意代码。配置为 DNS 服务器的 Windows 服务器存在此漏洞的风险。 要利用此漏洞进行攻击，未经身份验证的攻击者可以向 Windows DNS server 发送恶意请求。此更新通过修改 Windows DNS servers 处理请求的方式来解决该漏洞。	严重 远程执行代码	Server 2016 Server 2019 Server, version 1903 Server, version 1909 Server, version 2004 Server 2012 Server 2012 R2
CVE-2020-1032	**Hyper-V RemoteFX vGPU 远程代码执行漏洞** 当主机服务器上的 Hyper-V RemoteFX vGPU 未能正确验证 Guest 操作系统上经身份验证的用户的输入时，存在远程代码执行漏洞。要利用此漏洞，攻击者可通过在 Guest 操作系统上运行特制程序，攻击运行在 Hyper-V host 操作系统上的第三方视频驱动来利用此漏洞，成功利用此漏洞的攻击者可在 Host 操作系统上执行任意代码。	严重 远程执行代码	Server 2016 Server 2012 Server 2012 R2
CVE-2020-1463	**Windows SharedStream Library 权限提升漏洞** SharedStream Library 处理内存中对象的方式存在权限提升漏洞。成功利用此漏洞的攻击者可	重要 特权提升	Windows 10 Server 2016 Server 2019 Server, version 1903

	以使用提升的权限执行代码。要利用此漏洞进行攻击，本地身份验证的攻击者可以运行构建的应用程序。 安全更新通过确保 SharedStream Library 正确处理内存中的对象来解决该漏洞。		Server, version 1909 Server, version 2004
CVE-2020-1374	**Windows Remote Desktop Client 远程代码执行漏洞** 当用户连接到恶意服务器时，Windows Remote Desktop Client 中存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在连接客户端的计算机上执行任意代码。然后，攻击者可以安装程序；查看、更改或删除数据；或创建具有完全用户权限的新帐户。 要利用此漏洞，攻击者需要控制服务器，然后说服用户连接到服务器。攻击者无法强迫用户连接到恶意服务器，需要通过社会工程、DNS 中毒或使用中间人（MITM）技术诱骗用户连接。攻击者还可以危害合法服务器，在其上托管恶意代码，并等待用户连接。 此更新通过更正 Windows Remote Desktop Client 处理连接请求的方式来解决该漏洞。	严重 远程执行代码	Windows 10 Server 2016 Server 2019 Server, version 1903 Server, version 1909 Server, version 2004 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-1410	**Windows Address Book 远程代码执行漏洞** 当 Windows Address Book (WAB)未能正确地处理 vcard 文件时，存在远程代码执行漏洞。要利用此漏洞，攻击者可以发送恶意 vcard，受害者可以使用 Windows Address Book (WAB)打开该 vcard。成功利用该漏洞后，攻击者可以在受害者系统上执行。 安全更新通过更正 WWindows Address Book 处理绑定检查的方式来解决该漏洞。	严重 远程执行代码	Windows 10 Server 2016 Server 2019 Server, version 1903 Server, version 1909 Server, version 2004 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-1435	**Windows Graphics Device Interface (GDI)远程代码执行漏洞** Windows Graphics Device Interface (GDI) 处理内存中的对象时存在远程代码执行漏洞。成功利用此漏洞的攻击者可以控制受影响的系统。然后，攻击者可以安装程序；查看、更改或删除数据；或创建具有完全用户权限的新帐户。与使用管理用户权限操作的用户相比，帐户配置为在系统上具有较少用户权限的用户受到的影响较小。	严重 远程执行代码	Windows 10 Server 2016 Server 2019 Server, version 1903 Server, version 1909 Server, version 2004 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-1436	**Windows Font Library 远程代码执行漏洞** 当 Windows 字体库未能正确处理构建的字体时，存在远程代码执行漏洞。对于除 Windows 10 以外的所有系统，成功利用此漏洞的攻击者	严重 远程执行代码	Windows 10 Server 2016 Server 2019 Server, version 1903

	可以远程执行代码。对于运行 Windows 10 的系统，成功利用此漏洞的攻击者可以在 AppContainer 沙盒上下文中以有限的权限和功能执行代码。然后，攻击者可以安装程序；查看、更改或删除数据；或创建具有完全用户权限的新帐户。		Server, version 1909 Server, version 2004 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-1403	**VBScript 远程代码执行漏洞** VBScript engine 处理内存中对象的方式存在远程代码执行漏洞。该漏洞可能会损坏内存，从而使攻击者能够在当前用户的上下文中执行任意代码。成功利用此漏洞的攻击者可以获得与当前用户相同的用户权限。如果当前用户使用管理用户权限登录，成功利用此漏洞的攻击者可以控制受影响的系统。然后，攻击者可以安装程序；查看、更改或删除数据；或创建具有完全用户权限的新帐户。	严重 远程执行代码	Internet Explorer 11 Internet Explorer 9
CVE-2020-1439	**PerformancePoint Services 远程代码执行漏洞** 当 PerformancePoint Services for SharePoint Server 无法检查 XML 文件输入的源标记时，该软件中存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在负责 XML 内容反序列化的进程上下文中运行任意代码。要利用此漏洞，攻击者可以使用受影响的产品将编制的文档上传到服务器以处理内容。 安全更新通过更正 PerformancePoint Services 如何验证 XML 内容的源标记来解决此漏洞。	严重 远程执行代码	SharePoint Enterprise Server 2013 SharePoint Server 2019 SharePoint Foundation 2013 SharePoint Enterprise Server 2016 Business Productivity Servers 2010
CVE-2020-1025	**Microsoft Office 权限提升漏洞** 当 Microsoft SharePoint Server 和 Skype for Business Server 不正确地处理 OAuth 令牌验证时，存在权限提升漏洞。成功利用此漏洞的攻击者可以绕过身份验证并实现不正确的访问。要利用此漏洞进行攻击，攻击者需要修改令牌。此更新通过修改 Microsoft SharePoint Server 和 Skype for Business Server 验证令牌的方式来解决此漏洞。	严重 特权提升	Skype Business Server 2019 CU2 Skype Business Server 2015 CU 8 Lync Server 2013 SharePoint Enterprise Server 2016 SharePoint Server 2019 SharePoint Foundation 2013
CVE-2020-1349	**Microsoft Outlook 远程代码执行漏洞** Microsoft Outlook 软件未能正确处理内存中的对象时存在远程代码执行漏洞。成功利用此漏洞的攻击者可以使用巧尽心思构建的文件在当前用户的安全上下文中执行操作。例如，该文件随后可以代表具有与当前用户相同权限的登录用户执行操作。	严重 远程执行代码	365 Apps Enterprise Office 2019 Outlook 2016 Outlook 2013 Outlook 2010

CVE-2020-1446	**Microsoft Word 远程代码执行漏洞** Microsoft Word 软件未能正确处理内存中的对象时存在远程代码执行漏洞。成功利用此漏洞的攻击者可以使用巧尽心思构建的文件在当前用户的安全上下文中执行操作。例如，该文件随后可以代表具有与当前用户相同权限的登录用户执行操作。	重要 远程执行代码	SharePoint Server 2010 SharePoint Enterprise Server 2013/2016 SharePoint Server 2019 Office Online Server 365 Apps Enterprise Office 2010/2019 Office Web Apps 2010/2013 Word 2010/2013/2016 Office 2016/2019 for Mac

参考信息：

https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Jul

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200008

➢ 多款 Cisco 产品缓冲区溢出漏洞

发布日期：2020-07-06
更新日期：2020-07-06
受影响系统：
Cisco Cisco Small Business RV016 Multi-WAN VPN <=4.2.3.10
Cisco RV042 Dual WAN VPN <=4.2.3.10
Cisco RV042G Dual Gigabit WAN VPN <=4.2.3.10
Cisco RV082 Dual WAN VPN <=4.2.3.10
Cisco RV320 Dual Gigabit WAN VPN <=1.5.1.05
Cisco RV325 Dual Gigabit WAN VPN <=1.5.1.05
描述：

CVE(CAN) ID: CVE-2020-3295
Cisco Small Business RV016 Multi-WAN VPN 等都是美国思科（Cisco）公司的一款 VPN 路由器。
多款 Cisco 产品中的 Web 管理界面存在缓冲区溢出漏洞，该漏洞源于程序未能正确限制用户输入边界，远程攻击者可借助特制请求利用该漏洞导致设备崩溃或以 root 用户特权执行任意代码。
建议：

厂商补丁：
cisco
厂商已发布了漏洞修复程序，请及时关注更新：
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-routers-stack-vUxHmnNz

➢ Linux kernel 缓冲区溢出漏洞

发布日期：2020-07-10
更新日期：2020-07-10
受影响系统：Linux Linux kernel <5.6.7
描述：

CVE(CAN) ID: CVE-2020-12659
Linux kernel 是美国 Linux 基金会发布的开源操作系统 Linux 所使用的内核。Linux kernel 5.6.7 之前版本中的 net/xdp/xdp_umem.c 文件的‘xdp_umem_re’函数存在缓冲区溢出漏洞，本地攻击者可借助特制请求利用该漏洞在系统上执行任意代码或导致拒绝服务。
建议：

厂商补丁：
Linux
厂商已发布了漏洞修复程序，请及时关注更新：
https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.6.7

➢ IBM DB2 缓冲区溢出漏洞

发布日期：2020-07-06
更新日期：2020-07-06
受影响系统：
IBM IBM DB2 V9.7
IBM IBM DB2 V10.1
IBM IBM DB2 V10.5
IBM IBM DB2 V11.1
IBM IBM DB2 V11.5
描述：

CVE(CAN) ID: CVE-2020-4363
IBM DB2 是美国 IBM 公司的一套关系型数据库管理系统。该系统的执行环境主要有 UNIX、Linux、IBMi、z/OS 以及 Windows 服务器版本。基于 Linux、UNIX 和 Windows 平台的 IBM DB2 (包括 DB2 Connect Server) 中存在缓冲区溢出漏洞，该漏洞源于错误的边界检查。本地攻击者可利用该漏洞以 root 权限执行任意代码。
建议：

厂商补丁：
IBM
目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://www.ibm.com/support/pages/node/6242332

六、本期网络安全事件

➢ 0.5 元一份！谁在出卖我们的人脸信息？

2020 年 7 月 13 日，“要的话五毛一张打包带走，总共两万套，不议价。”一位卖家用微信语音对记者说。他还发来两套手持身份证的人脸照片截图。记者近日调查发现，一些网络黑产从业者利用电商平台，批量倒卖非法获取的人脸等身份信息和“照片活化”网络工具及教程。专家提醒，这些人脸信息有可能被用于虚假注册、电信网络诈骗等违法犯罪活动。

人脸数据 0.5 元一份、修改软件 35 元一套

记者调查发现，在淘宝、闲鱼等网络交易平台上，通过搜索特定关键词，就能找到专门出售人脸数据和“照片活化”工具的店铺。在淘宝上，部分卖家以“人脸全国各地区行业可做，信誉第一”“出售人脸四件套，懂的来”等暗语招徕买家。记者随机点进一家出售“××同城及各大平台人脸”商品的店铺，旋即跳转到闲鱼界面。在该卖家的闲鱼主页中，售卖的商品为部分平台包含用户人脸的信息数据。

在闲鱼平台，不少卖家公开兜售人脸数据。为了保证店铺的“正常运营”，卖家常怂恿买家通过微信或 QQ 沟通议价。记者近日随机咨询其中一位卖家，对方用语音答复道“加微信聊吧，这个说多了会被封”，并向记者发来了微信号。

除售卖人脸数据外，一些“胆大”的闲鱼卖家还出售“照片活化”工具，利用这种工具，可将人脸照片修改为执行“眨眨眼、张张嘴、点点头”等操作的人脸验证视频。

“一套（‘照片活化’）软件加教程 35 元，你直接付款，确认收货后我把链接发你。”一位闲鱼卖家在闲鱼对话框内使用语音与记者议价。在记者完成支付并确认收货后，卖家通过百度网盘给记者发来一个文件大小约 20GB 的“工具箱”，“工具箱”里有虚拟视频刷机包、虚拟视频模拟器和人脸视频修改软件等工具，还有相关工具的操作教程文件。

还有一位卖家在添加记者 QQ 好友后，先发来了一些单人手持身份证的样本照片，随后向记者展示了其利用工具修改上述照片后欺骗某网络社交平台人脸识别机制的效果视频。目前，记者已将调查中发现的一些线索移交有关公安机关。

倒卖的人脸数据拿来做什么？

“如果只是采集个人的人脸信息，比如在马路上你被人拍了照，但是没有获得你的其他身份信息，隐私泄露风险并不大。”中国电子技术标准化研究院信安中心测评实验室副主任何延哲说，问题在于，当前网络黑市中售卖的人脸信息并非单纯的“人脸照片”，而是包含公民个人身份信息（包括身份证号、银行卡号、手机号等）的一系列敏感数据。

一位倒卖“人脸视频工具箱”并声称可以“包教会”的卖家告诉记者，只要学会熟练使用“工具箱”，不仅可以利用这些人脸数据帮他人解封微信和支付宝的冻结账号，还能绕过知名婚恋交友平台及手机卡实名认证的人脸识别机制。这位卖家还给记者传来了帮一些“客户”成功解封冻结账号的截图。

“从技术角度看，将人脸信息和身份信息相关联后，利用系统漏洞‘骗过’部分平台的人脸识别机制是有可能的。”人脸识别技术专家、厦门瑞为信息技术有限公司研究中心总监贾宝芝博士认为，尽管一些金融平台在大额转账时需要多重身份认证，但“道高一尺魔高一丈”，网络黑产技术手段也在不断更新，绝不能因此忽视账户安全。

何延哲向记者举例：如果人脸信息和其他身份信息相匹配，可能会被不法分子用以盗取网络社交平台账号或窃取金融账户内财产；如果人脸信息和行踪信息相匹配，可能会被不法

分子用于精准诈骗、敲诈勒索等违法犯罪活动。

这些包含人脸信息和其他身份信息的数据从何而来？有卖家向记者透露，自己所售卖的人脸信息来自一些网贷和招聘平台；至于如何从这些平台中获取此类信息，对方没有作答。

需警惕利用人脸信息进行的违法犯罪活动

近年来，人脸识别技术被用于金融支付、小区安防、政务服务等诸多场景，既提高了便利性，也通过数据交互在一定程度上增强了安全性。但是，人脸数据如果发生泄露或被不法分子非法获取，就有可能被用于违法犯罪活动，对此应保持警惕。

去年 8 月，深圳龙岗警方发现有辖区居民的身份信息被人冒用，其驾驶证被不法分子通过网络服务平台冒用扣分。

在开展“净网 2020”行动中，龙岗警方经多方侦查发现，有不法分子使用 AI 换脸技术，绕开多个社交服务平台或系统的人脸认证机制，为违法犯罪团伙提供虚假注册、刷脸支付等黑产服务。截至目前，龙岗警方在广东、河南、山东等地已抓获涉案犯罪嫌疑人 13 名。据警方介绍，在上述案件中，犯罪嫌疑人利用非法获取的公民照片进行一定预处理，而后通过“照片活化”软件生成动态视频，骗过人脸核验机制。随后，通过网上批量购买的私人社交平台账号登录各网络服务平台注册会员或进行实名认证。

人脸信息关系到每个人的生命财产安全。业内专家认为，对倒卖人脸信息的黑色产业链必须予以严厉打击，立法机关需统筹考虑技术发展与信息安全，划定人脸识别技术的使用红线；监管部门也应对恶意泄露他人人脸和身份信息的违法行为予以坚决制止。

明年将施行的民法典，对自然人个人信息的范畴进行了专门说明，生物识别信息被纳入其中。中国信息安全研究院副院长左晓栋认为，除民法典外，正在制定的个人信息保护法和数据安全法也应对人脸等生物特征信息的保护作出安排；立法要充分考虑人脸这一特殊身份信息的可获得性，不能让制定出来的法律因执行难而流于形式。

北京师范大学网络法治国际中心执行主任吴沈括认为，网络平台对平台上的交易行为负有监管义务，应严谨审核卖家资质，对平台内经营者的合规情况进行监控、记录，不应允许发布任何侵犯他人人身财产权利或法律法规禁止的物项。

贾宝芝建议，相关平台在制定人脸识别安全规范的过程中，要强调“人脸数据等生物特征信息”与“其他身份信息”实行完全隔离存储，避免将人脸数据与身份信息相关联后发生批量化泄露。

对于曾经上传过清晰手持身份证照片或同时上传人脸照片并填写身份证、银行卡信息的用户，专家建议，应在开启人脸验证的同时，尽可能选择多重验证方式，减轻单重人脸验证

风险。（来源：新华社）

➢ 上海检察院：揭秘黑客入侵第三方支付平台盗窃案涉案超 1 亿

2020 年 7 月 10 日，从上海市人民检察院第一分院获悉，由该院提起公诉的一起利用黑客技术侵入第三方支付平台计算机系统盗窃案近日宣判。两名被告人均被判处无期徒刑，剥夺政治权利终身，并处没收个人全部财产。上海市人民检察院第一分院起诉指控，2018 年 4 月 28 日至 6 月 1 日，被告人黎某、温某利用上海某理财平台和 P2P 公司之间充值系统漏洞，采用变造方法将小额实际充值虚增为巨额金额，再从备付金账户将巨额资金划转至 P2P 账户，进而非法占有。黎某、温某盗窃数额分别为 5731 万余元和 5311 万余元，其犯罪事实清楚、证据确实充分，应当依法予以严惩。日前，上海市第一中级人民法院作出一审判决：黎某、温某分别伙同他人，以秘密手段非法窃取他人财物，其行为已构成盗窃罪，并系共同犯罪。黎某、温某均被判处无期徒刑，剥夺政治权利终身，并处没收个人全部财产。

以下来自上海检察一分院对该案件的揭秘：

攻克重重壁垒联手窃得巨款

2018 年 6 月 1 日，是总部设在上海的“天兑”理财公司月度盘账的日子，员工发现其备付金第三方平台账目出现 5 千多万亏空，经过紧急核查，排除内部原因。5 千多万在计算

机系统被神不知鬼不觉地划走了——员工们顿时惊出一身冷汗。6 月 3 日报警，案发!

警方迅速立案，经过 10 多天侦查，6 月 13 日将有重大作案嫌疑的黎一、温迪 2 人缉拿归案。黎一，男，八零后，大学文化，是一家小型计算机技术服务公司的老板，主要从事网站漏洞检测业务。警方经过调查发现，黎一曾就职于某专业网络机构下属单位，是负责电脑网络的技术总监，擅长网站漏洞检测。温迪，黎一的朋友，男，八零后，大学文化，无业人员。

相貌普通的黎一，在网络“黑客”界却是“大师级”的存在。在他眼里，绝大多数“网虫”皆为“屌丝”，一般的专业工程师，与他“过手”的结局无不如“菜鸟”般被“秒杀”。虽然在网络虚拟空间里是神一般的人物，可在现实世界中仅靠经营一家小公司过着不温不火的日子。“赚钱不多，来钱太慢”，这种状况如何改变呢?去抢银行吗?何不施展自己的“黑客”绝技，到“金库”去“扫荡”一番，打打键盘百万千万轻松到手……，于是，一个个罪恶的念头占满脑海并逐渐酿成越来越具体的方案。

黎一的作案计划主要由三部分组成，一是通过网络偷钱、二是用银行卡将其偷来的钱变现、三是把钱兑换和洗白。梦想“一夜暴富”的温迪、笃信“富贵险中求”的袁鹏(另案处理)被其相中，彼此一拍即合，于是“三人成虎”。明确分工后，各自紧锣密鼓地进行作案准备。黎一着手寻找防范薄弱的“软柿子”和进入系统的“假面具”;温迪负责筹备银行卡、手机号和必要的设备器材;袁鹏则负责物色持卡取现的人员。他们约定，以后尽量少见面少联系，相互通信时使用十分冷门、不易跟踪的社交软件。

经过一段时间的“嗅探和窃听”，黎一发现“天兑”理财平台和 P2P 公司之间充值系统的漏洞比较容易被利用，并可改变一级账户的充值数额，然后通过与一级账户绑定的二级账户(银行卡)随时随地地取现，另外，黎一还筛选出山西某大学(VPN)作为进入“天兑”理财系统的公共服务器，并在网络上盗得该大学一名员工的电子账号及密码，这意味着黎一可以戴着“假面具”大摇大摆地到达“金库”随意“搬钱”。温迪的本事也不小，他采取各种办法搞到了 10 多张银行卡和一些电话卡，当然登记的持卡人与他们一点关系都没有，还考察了兑换外币和洗钱渠道并购置了笔记本电脑、随身无线 wifi 等。袁鹏的动作也不慢，黎一和温迪拉其入伙时，借口有数额较大赌资让他帮助取现，并许以取款金额的 5%作为好处费，袁鹏便以取款金额的 1.5%作为报酬找来了其他 6 人(均另案处理)，随时准备用银行卡到各地取钱。

2018 年 5 月 4 日，黎一、温迪觉得万事俱备，决定对“天兑”理财公司备付金第三方平台下手!先小试牛刀。在广西南宁的一间办公室里，黎一打开了他的笔记本电脑，在温迪

的辅助下，熟练地连上移动 wifi，用事先盗取的账号和密码登陆某大学的 VPN(网络服务器)，然后攻破“天兑”理财公司的防火墙，侵入第三方支付平台计算机系统。黎一的手指在笔记本电脑上时而上下翻飞，时而停顿观察屏幕上一串串眼花缭乱的数据，如同网络游戏中的超人，逢山开路、遇水架桥，绕过层层陷阱跃过重重障碍，直插对方的心脏——“金库”。

开始时有点紧张，毕竟就像真的潜入银行金库似的，既怕攻击受阻又怕引来警察，但随着对方系统被一点点攻破，目标账户里的数额不断增加，“成功”的喜悦逐渐盖过了恐惧，黎一说。两天不到的时间，预先开具的理财账户上的金额由几块钱变成了几十万元。第一次作案到手的钱，黎一、温迪各分一半，以后基本也是五五分账。初战告“捷”、欣喜万分。特别是黎一感慨万千：想自己练就的一身绝技原来只是落得“拾漏补缺”、“为人作嫁”，得利甚薄，而今却能利用漏洞直入“金库”，肆意转款归为己有，真是“酷毙了、帅呆了、爽翻了”！

然而，区区几十万对“黑客”大盗来讲连塞牙缝都不够。兴奋之余，黎一、温迪不失冷静，他们仔仔细细反反复复地查验，确认被盗的网络平台没有任何反应，才放下心来，并决意放开手脚、大干一场。温迪提议，到广州去搞，那里洗钱门路多，可以快速将钱变现和兑换。于是黎一和温迪从南宁乘高铁到广州，辗转多家宾馆酒店，两人深居简出，表面上行色如常，但谁也想不到他们干着“江洋大盗”的勾当。20 多天时间里、他们故伎重演，疯狂作案，在“天兑”理财公司第三方支付平台用 200 余元变造了 400 多笔下单金额，总共窃取 5000 多万元。就这样，上海“天兑”理财平台巨额钱款，被人悄无声息地偷走了。等到次月盘账发现时，窃贼留下的只有淹没在海量电子数据中的一些异样字符。“黑客”大盗终于作下惊天大案。

布置层层迷雾施展脱身诡计

“黑客”是靠玩电脑扬名立万的，那可是一个“烧脑”的行当。黎一认为，小偷扒手偷钱尚讲究“技术含量”，作为“黑客大师”，理所当然要将偷钱富有“设计感”。常言道：捉贼捉赃。廓清全案，看得出黎一、温迪在“贼”和“赃”这两个字上做足了文章、下尽了功夫。

销声匿迹，隐藏“贼”踪是他们的设计之一。黎一在作案过程中，戴的是“假面具”、“走”的是公共网、用的是“抓包”软件、使的是“独门绝技”，来去自由、收放自如、无踪无影，作案后将使用过电脑等硬件设备器材悉数销毁。一旦被抓，完全可以用“贼”不是我、我没做“贼”来蒙混。

借手取“赃”、变幻“赃”影是他们的设计之二。赃款提现的任务他们安排不知内情的

袁鹏和其雇来 6 人执行，接到袁鹏汇聚的钱款后火速进行套现、转移和兑换。他们认为，取“赃”之人不知“赃”，“赃”过手即不为“赃”，何况偷的是人民币，拿在手上的却是美元，何以确“赃”？

网上网下、“贼”“赃”分离是他们的设计之三。一方面他们在人员上采取 1+1+1+X 的结构，最容易暴露的袁鹏等 7 人不知“赃”从何来、“贼”在何方，另一方面黎一、温迪即使被擒，也可凭有“贼”无“赃”、或借有“赃”无“贼“的理由得以全身而退。

由此看来，黎一、温迪作案前就已设好“假想敌”，并进行了周密的反侦查设计，作案中他们一路在网上偷钱、一路在网下取赃、一路在地下洗钱，各个环节配合默契、进退有序，简直可以达到“天下无贼”的境界。黎一曾自诩，“黑客”最不怕的就是“烧脑”。

神技屡屡破功终被定罪惩罚

黎一、温迪到案后，警方根据黎一的交代从其久不住人的老宅内，搜到藏匿的 248 万美元。袁鹏等人也相继落网。如果这是一件普通的盗窃案，办理起来并不很难。然而，由于此案特殊的作案手法和较为周密的反侦查设计，加上黎一对犯罪事实先交代后翻供，温迪始终矢口否认，而侦查取得的证据又颇为“零星、零散和零乱”，给办案工作带来了更多的复杂性。

负责该案审查起诉工作的是上海市检察一分院第一检察部检察官张政斌和助理检察官陆玥，这对办案组合一位睿智细腻、经验丰富，另一位外柔内刚、坚韧不拔。“接手这个案子时，因为直接证据相当缺少，我们都觉得是十分棘手，但是越是棘手越激发了我们一定要把罪犯绳之以法的决心”，检察官张政斌说。陆玥说：“这次，与他们‘杠上’了。”

雁过必留痕!检察官更新了思路和方法，不断克服困难打破僵局。“那段时间里，我们几乎时时刻刻都在寻找突破口，反复论证完善证据体系”，检察官说。鉴于此案的主要犯罪事实虚拟空间和现实空间相互交错特点突出，检察官绘制了人物关系图、作案活动图、赃款走向图、电子数据图等多张案情图表，用时间坐标进行串联，使“零星”的证据绽发闪光、“零散”的证据整序归列、“零乱”的证据串珠成链，三维空间+一维时间的“四维”参考系让案件事实脉络一目了然、每个作案细节定位准确，不同空间不同维度证据的关联性纵横分明。整个证据体系在时间法则的连接下更加全面和稳固。在此基础上，按图索骥，提出更有针对性指导性的补充侦查意见，引导公安机关补全补强证据。

针对该案原来的证据中有大量的技术性结论，司法证明作用严重不足的短板，检察官要求公安机关增加司法鉴定，将机器语言向法律文书转换，提升证据的直观性和证明力，增强证据的支撑力。检察官说，此案对我们提出了许多新挑战，案后也留下了许多新课题。

虽然黎一、温迪态度对立，但每次提审中检察官都劝其交代、认罪，可惜他们依然执迷不悟。而另案处理的袁鹏等 7 人先前已纷纷认罪。2019 年 8 月 2 日，上海市检察一分院将此案向上海市第一中级法院提起公诉。同年 9 月 9 日，法院公开开庭审理。

法庭上，法官正襟危坐、检察官胸有成竹、辩护人踌躇满志、两名被告人抱定一副“你奈我何”的模样。黎一当庭翻供，温迪以沉默和“不知道”作回应，但当听到检察官运用时间坐标将他们在网上网下两个空间作案的证据相互比照印对时，他们作案中费尽心思的“辗转腾挪”和绞尽脑汁的反侦查设计，反而为检察官提供了更多的证据点，终于明白一条法理严谨、环环相扣的锁链已将其紧紧套住，在检察官的“四维场景”中，他们的“三维设计”只会是被“碾压”的下场，此时他们觉得再辩解也没多大意义了。

检察官又特别指出，他们为犯罪合谋合伙、冒用他人名义非法侵入理财公司的网络系统多次盗窃，冒名取现、洗白赃款，并在到案后对客观的犯罪事实拒不承认的行为，进一步证明其犯罪故意的强烈和对抗法律的嚣张。此刻，两名被告人的身形一下子“佝偻”起来。一位参加旁听的人士说：“看得出来，他们是口不服心服。”

检察机关认为，被告人黎一、温迪利用上海“天兑”理财平台和 P2P 公司之间充值系统漏洞，采用变造方法将小额实际充值虚增为巨额金额，再从备付金账户将巨额资金划转至 P2P 账户，从而非法占有，黎一、温迪盗窃数额分别为 5731 万余元和 5311 万余元，其犯罪事实清楚、证据确实充分，应当依法予以严惩。日前，法院作出一审判决：黎一、温迪分别伙同他人，以秘密手段非法窃取他人财物，其行为已构成盗窃罪，并系共同犯罪。黎一、温迪均被判处无期徒刑，剥夺政治权利终身，并处没收个人全部财产。司法机关将继续追赃挽损。（来源：新华社）

➢ 广东足协数据库被入侵，积分数据被恶意篡改！

2020 年 7 月 14 日，在广东足协官网的男足排名列表中，中国积分达到 1602，排名世界第一。如今，广东足协官方给出回应，真相终于揭晓了！在国际足联的最新一期排名中，国足排名亚洲第 9，世界第 76 名。此外，因为王兴、董方卓等人的发声，中国足球热度不减，因此，国足也是备受关注。加上中超即将回归，中国足球再次成为热议话题。


男足排名 女足排名

世界排名	国家	积分	席位变化
1	中国	1602	+0
2	巴西	1484	+1
3	葡萄牙	1358	+0
4	阿根廷	1348	+0
5	比利时	1325	+0
6	西班牙	1231	+0
7	波兰	1213	+4
8	瑞士	1190	+0
9	法国	1183	+0
68	中国	504	+2

没想到，平常压根没人关注的广东足协官网引发热议，在广东足协官网的男足排名列表中，中国积分达到 1602，排名世界第一。2-9 位分别是巴西、葡萄牙、阿根廷、比利时、西班牙、波兰、瑞士和法国。显然，广东足协闹了大笑话，国足根本不可能排名世界第一，现在的世界排名是第 76 位，在亚洲，国足连二流都算不上，又怎么可能是世界第一呢。

如今，广东足协给出回应：“7 月 13 日，我协会官方网站出现异常情况。经查，是个别人员通过一些手段进入网站后台，对数据库进行恶意篡改，导致网站国际足联男足排名显示出现错误。经技术人员修复，现已经恢复正常。接下来，我们将进一步提升网络管理，加强技术防护手段，避免再出现类似情况。衷心感谢广大足球爱好者对我协会工作的关注，也希望大家能够一如既往地支持广东足球的发展。”（来源：南方日报）

➢ 江南农商行：因网络安全问题被罚 30 万元

2020 年 7 月 8 日，日前，江苏银保监局公布了对于江苏江南农村商业银行股份有限公司（以下简称“江苏江南农商行”）的行政处罚。处罚信息显示，江苏江南农商行因网络安全工作严重不足，江苏银保监局根据《中华人民共和国银行业监督管理法》第四十六条第（五）项，罚款人民币 30 万元。

如无疏漏，根据银保监会官网查询结果，江苏江南农商行是首家因为网络安全问题被处

罚的银行，这张罚单也是银行业第一张网络安全罚单。

或因内部组织建设存在问题

江苏银保监局行政处罚信息公开表

（江苏江南农村商业银行股份有限公司）

行政处罚决定书文号			苏银保监罚决字〔2020〕20号
被处罚当事人	个人	姓名	
		单位	
	单位	名称	江苏江南农村商业银行股份有限公司
		法定代表人姓名	陆向阳
主要违法违规事实（案由）			网络安全工作严重不足
行政处罚依据			《中华人民共和国银行业监督管理法》第四十六条第（五）项
行政处罚决定			罚款人民币30万元
作出处罚决定的机关名称			中国银行保险监督管理委员会江苏监管局
作出处罚决定的日期			2020年6月16日

案由为：网络安全工作严重不足，处罚依据为《中华人民共和国银行业监督管理法》第四十六条第（五）项。《中华人民共和国银行业监督管理法》第四十六条规定银行业金融机构有下列情形之一，由国务院银行业监督管理机构责令改正，并处二十万元以上五十万元以下罚款；情节特别严重或者逾期不改正的，可以责令停业整顿或者吊销其经营许可证；构成犯罪的，依法追究刑事责任：

（一）未经任职资格审查任命董事、高级管理人员的；

（二）拒绝或者阻碍非现场监管或者现场检查的；

（三）提供虚假的或者隐瞒重要事实的报表、报告等文件、资料的；

（四）未按照规定进行信息披露的；

（五）严重违反审慎经营规则的；

“严重违反审慎经营规则”是一个非常宽泛的条款，有很多问题都会触发这项条款，比如将消费性贷款放入楼市等等。因此，虽然知道江苏江南农商行存在网络安全问题，但具体是什么问题，我们无从得知，只能进行猜测。

《网络安全法》第三十一条规定，国家对金融等重要行业和领域，在网络安全等级保护制度的基础上，实行重点保护。根据《关键信息基础设施确定指南（试行）》要求，银行运营为金融行业中的关键业务。

因此，银行一般应被认定为关键信息基础设施运营者，在履行网络运营者的一般安全保护义务的基础上，还需履行关键信息基础设施运营者的特殊义务。从这个角度出发，银行需承担网络安全义务非常重，而相关的规范规定更是数不胜数，在今年就发布有《个人金融信息保护技术规范》、《网上银行系统信息安全通用规范》、《商业银行应用程序接口安全管理规范》等等多个规范。

大致上，银行业网络安全分为两个部分，一部分是技术建设，包括信息系统开发，相关安全技术使用，风控系统建设等等。另外一部分是制度建设，包括银行部门架构、员工管理制度、内部风险控制等等。据业内人士透露，江苏江南农商行购买了不少安全产品，覆盖多个领域。因此，此次江苏江南农商行被罚不太可能是因为安全风控技术问题，更有可能是内部组织建设没有到位。

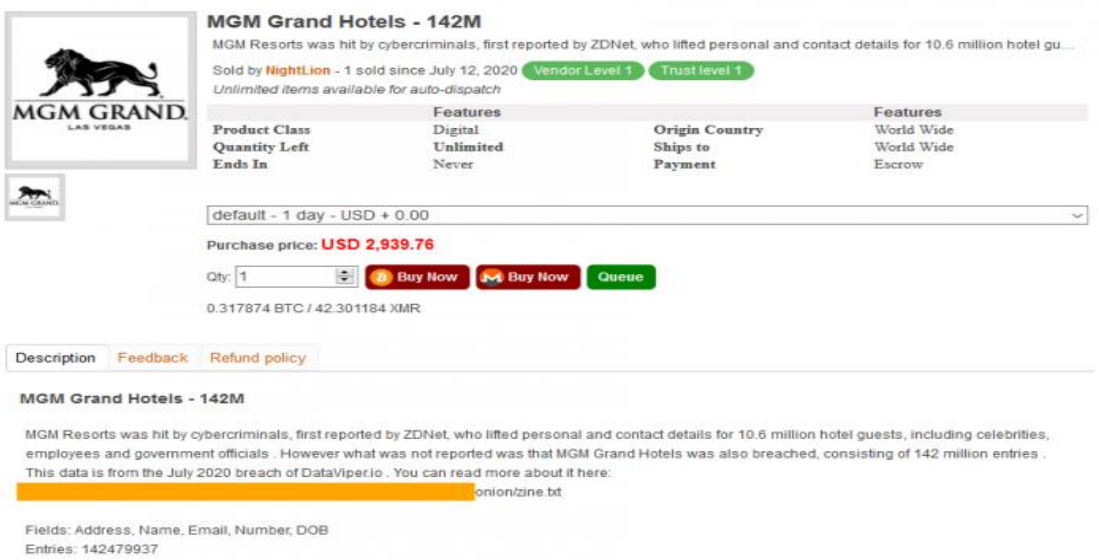
但是也有媒体爆出，江苏江南农商行的安全系统在 2015 年就存在重大漏洞，其中一个漏洞是中间件弱口令漏洞，可以通过它轻而易举地进入数据库，从而获取用户信息。目前为止，对江苏江南农商行被处罚的具体原因还处于猜测当中。（来源：移动支付网）

➢ 超过 1.42 亿美高梅酒店客人详细资料在暗网上出售

2020 年 7 月 15 日报道，一个数据泄露，影响的人比最初报道的多得多。这就是美高梅国际酒店集团发现自己的情况，在 2019 年的一次黑客攻击中，最初说影响了 1060 万客人，现在相信已经涉及超过 1.42 亿人。早在 2 月份，就有报道称，超过 1060 万名入住美高梅国际娱乐平台酒店的个人资料被公布在一个黑客论坛上。

现在，暗网上出现了一则广告，提供 142479937 名美高梅酒店客人的详细资料，价格仅为 2900 多美元，之后人们发现实际要价要高得多。据称，这些信息包括名人和政府雇员的数据，包括姓名、地址、电子邮件、电话号码和出生日期。美高梅表示，财务信息、身份证或社会安全号码以及酒店住宿细节都不在此次漏洞之列。ZDNet 联系了一些过去的酒店客人，确认名单的准确性。

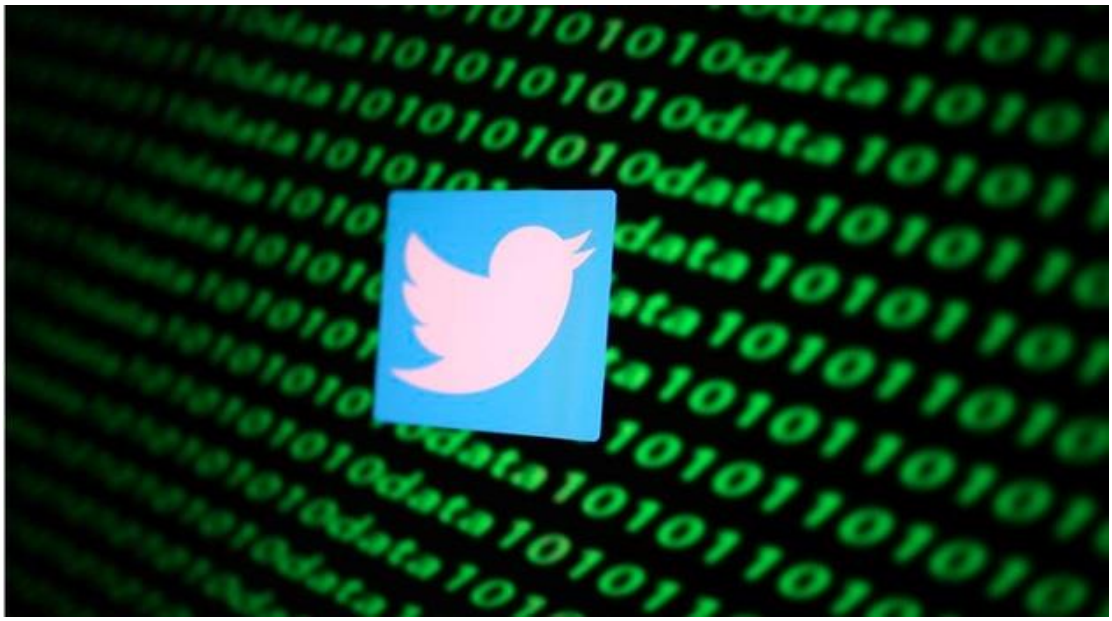
美高梅的细节来自于去年该酒店的一次数据泄露，一名黑客未经授权访问了一个云端服务器，其中包含了以往客人的信息。该连锁店表示，已经按照国家法律的要求，通知了所有受影响的人。发布广告的人声称，这些数据实际上来自于数据泄露监测服务 DataViper 最近的一次攻击，但该公司否认拥有一份完整的美高梅数据库，并表示黑客试图破坏该公司的声誉。



米高梅表示：它一直都知道有多少客人的数据在此次泄密事件中被泄露，但法律上并没有要求它透露这个数字。美高梅国际酒店集团知道去年夏天之前报道的这起事件影响范围，并且已经处理了这一情况。令人惊讶的是，实际受影响的客人数量可能会更多，俄罗斯黑客论坛上的帖子称，名单上有 2 亿人的详细信息。（来源：cnBeta）

➢ Twitter 被黑客攻击前 已有账号买卖的灰产市场

2020 年 7 月 17 日，据外媒报道，在周三黑客攻陷 Twitter 并对一些高知名度账户造成损害之前，就有人在灰色市场网站上发布了账户售卖广告。这个灰色网站专门为一些热门网站的账户交易提供便利，热门网站包括 Twitter，还有 Netflix、Instagram、Minecraft 等。



广告卖家承诺，只要花费 250 美元，他们就会把链接到一个 Twitter 帐户的电子邮件泄露给买家。而只要花费 2500 美元，买家就可以拥有该帐户，并保证买家满意。发布的广告声称：“如果您没有收到邮件/@，那么不管什么原因，您都将得到全额退款。”这则广告上还用@符号描述了 Twitter 账户。

以色列公司 Hudson Rock 将这则广告的截图提供给了媒体。该公司负责监控网络论坛上的被盗凭证和数据泄露。这则广告表明，Twitter 目前的状况并不太好——这个广告的出现正是一个早期迹象。

Twitter 公司目前仍在因为这个大量 VIP 账户被劫持事件而心有余悸。这些被劫持的 VIP 账户包括了真人秀明星金·卡戴珊（Kim Kardashian）、饶舌歌手坎爷·维斯特（Kanye West）、亚马逊创始人杰夫·贝索斯和微软联合创始人比尔·盖茨等人的账户。

尽管本次黑客攻击的细节受到关注，并且正被 Twitter 和 FBI 调查，但关于黑客攻击的消息早早就在一个游戏玩家和 Instagram 账户交换者论坛上传播——这说明这起事件很可能与低级网络犯罪有关，而非国家级的攻击行动。

“这看起来不像是一个精密复杂的黑客组织，”Hudson Rock 的首席执行官罗伊·卡西（Roi Carthy）说。帐户交易论坛 OGUsers 的一名管理员证实了广告截图的真实性，他告诉媒体，在论坛的管理者意识到发生了什么事后，他们立即冻结了发布广告的用户账号。他并补充说，该网站明确禁止交易经由黑客攻击而获得的账户。理论上，像 Twitter 和 Instagram 这样的社交媒体公司是禁止交易账户的，但这名管理者表示，互联网公司可以“选择何时执行这一规定”，这种做法被广泛接受。卡西说：“如果真是一个比较复杂的攻击的话，那就是在操纵股市了。”（来源：新浪科技）

信息安全意识产品服务

021-33663299