国盟信息安全通报

2019 年 6 月 10 日第 194 期

国盟信息安全通报

（第 194 期）

国际信息安全学习联盟

2019 年 6 月 10 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 293 个，其中高危漏洞 97 个、中危漏洞 167 个、低危漏洞 29 个。漏洞平均分值为 5.81。本周收录的漏洞中，涉及 0day 漏洞 134 个（占 46%），其中互联网上出现“Joomla Com_Attachments 组件文件上传漏洞、VFront 跨站脚本漏洞”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 1605 个，与上周（2475 个）环比下降 35%。

主要内容

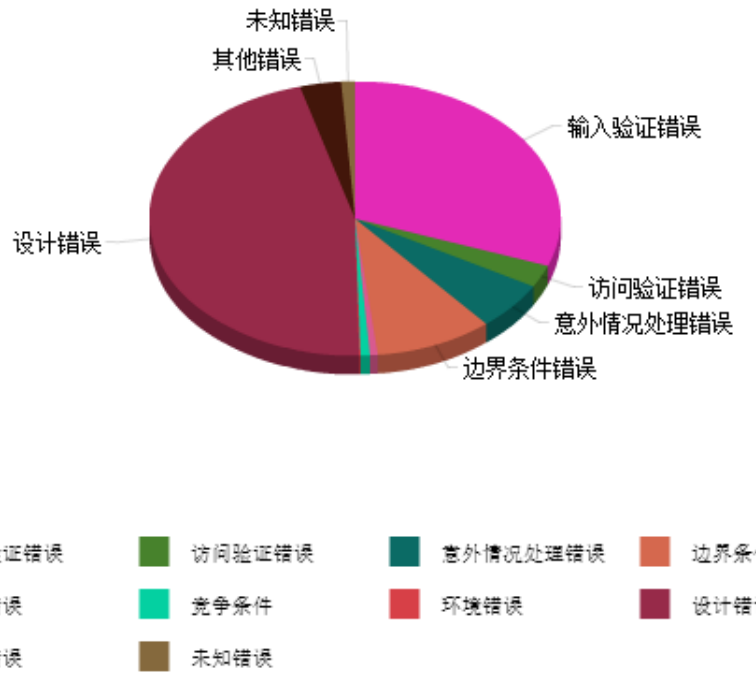
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

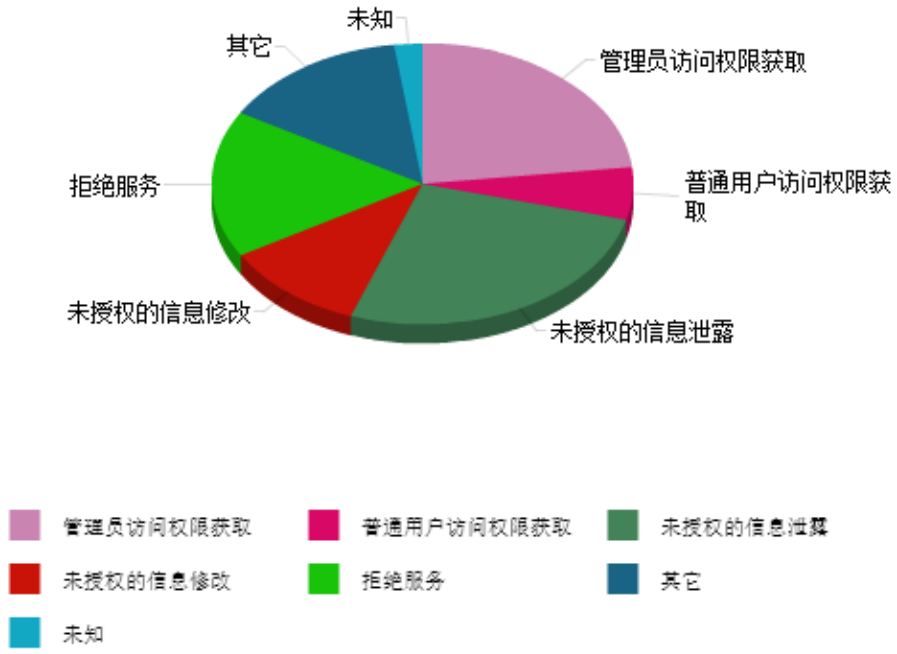
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 293 个，其中高危漏洞 97 个、中危漏洞 167 个、低危漏洞 29 个。漏洞平均分值为 5.81。本周收录的漏洞中，涉及 0day 漏洞 134 个（占 46%），其中互联网上出现“Joomla Com_Attachments 组件文件上传漏洞、VFront 跨站脚本漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 1605 个，与上周（2475 个）环比下降 35%。

二、安全漏洞增长数量及种类分布情况

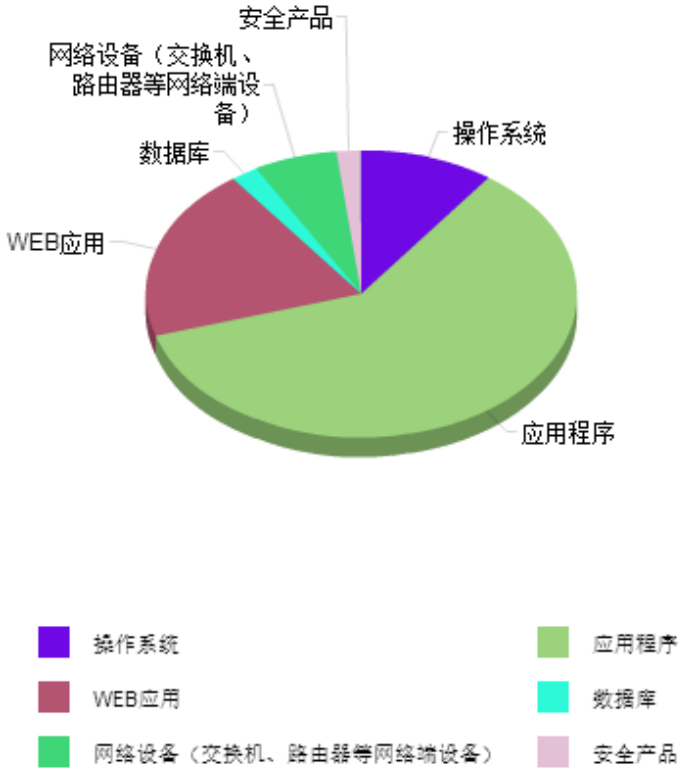
➢ 漏洞产生原因（2019 年 5 月 27 日—2019 年 6 月 10 日）



➢ 漏洞引发的威胁（2019 年 5 月 27 日—2019 年 6 月 10 日）



➢ 漏洞影响对象类型（2019 年 5 月 27 日—2019 年 6 月 10 日）



三、安全产业动态

➢ 网络强国路上的数字人才梦想

功以才成，业以才兴。建设新时代网络强国，实施国家大数据发展战略，助力中国经济的高质量发展，需要不断造就出一支支有梦想、有本领、有眼界的高素质数字人才队伍。从根本上说，数字时代的综合国力和区位竞争在根本上可以说是数字人才的质量、存量与盘活量之争。当前，以掌握、运用和创新 ICT 专业技能和补充技能，从事互联网、物联网+、大数据、云计算、人工智能等数字行业为基本标志的数字人才，正在以新时代奋斗者和追梦者的昂扬姿态，铺就着从工业 4.0 和机器人到数据科学、虚拟现实、数字化商业模式的“智造金带”。建设网络强国的时代渴望和呼唤着越来越多的数字弄潮儿投身其中，建功立业，追逐梦想；越来越多的新时代奋斗者们也将自己的职业、事业和志业凝聚成一个个数字人生、数字梦想，共同践行出“不拘一格出数才，江山代有数才出”的数字人才之梦。

数字人才建设已然成为建设网络强国与实现数字经济健康发展的“定心丸”和“准心盘”。当前，数字人才的严重不足已经成为制约数字经济创新创业、数字产业发展壮大、传统产业数字化转型的关键要素。美国高德纳（Gartner）公司的研究报告预测，到 2020 年，数字人才的短缺将会导致 30%以上的技术岗位空缺，数字人才将会分外抢手。可见，数字人才需求强劲与储备不足的结构性矛盾，已然成为当代社会实现创新持续发展所不得不重视的“针尖麦芒”。为此，国家发改委等 19 部门去年出台的《关于发展数字经济稳定并扩大就业的指导意见》指出，到 2025 年我国要实现数字人才规模的稳步扩大，要让数字经济领域成

为吸纳就业的重要渠道。达成这一目标的关键，既在于从育出发，坚持强化数字人才的培育与培训之道，拓展多层次、多类型、全方位的数字人才培育模式，也在于引育结合，搭建人才聚集高地，以事业、热忱和待遇引才筑梦，实现数字人才建设的“马太效应”。“数谷”贵阳的转型跨越发展之路，正映衬出了数字人才建设的引育结合之道。一方面，贵阳牢牢抓住“大数据人才十百千万培养计划”，选拔出 10 名大数据领军人才和 120 名大数据创业创新人才，夯实“数谷”的本土人才地基。另一方面，贵阳紧跟形势出台《关于创新产业人才聚焦机制 助推大数据大工业大招商行动的十条措施》，成立贵州师范大学 360 大数据网络安全学院等一大批数据人才实训基地，与 NIIT 签署战略合作协议，不断拓宽“数谷贵漂”的储备人才来源。贵阳的数字人才梦想，正经历着由“低地”、“洼地”到“高地”、“领地”的转型跨越和华丽转身。

数字人才建设需要有一种“只争朝夕，久久为功”的紧迫感与使命感。随着“互联网+”、“大数据+”的发展理念与运营模式日趋成熟，新时代的企业运行、社会治理、资源管理、民生服务等各方面无不打上了“数字化”、“数据化”的时代烙印。如何建设一支合用、合适、合理的数字人才队伍，打破数字人才流动的地域、行业和结构壁垒，使得数字人才能真正才尽其用、用尽其才，业已成为各行各业人才战略的共识性难题。德勤公司 2018 年的一份调研报告显示，追赶网络联结、大数据、数字化系统等技术变革速度是新时代人才管理工作的重大挑战。因此，数字人才建设就必须要有一种“只争朝夕”的紧迫感与使命感，要从速运用数字思维和数据手段，快速搭建数字人才管理与服务的线上技术研发与软件研制平台，高速实现数字人才培养与培训、分类与跨层、使用与流动的云计算式标准化、规范化和模式化，使得数字人才建设能跑上“快车道”。同时，数字人才建设难以一蹴而就、一劳永逸的现实也提醒我们，数字人才的健全和发展还必须有“久久为功”的情怀和使命。数字人才在本质上是追求学习了再学习、创新了再创新、卓越了再卓越的不竭不尽之才，“活到老，学到老”的终生学习理念，“学以致用，用以致智”的智慧学习理念，“人人皆可成才，皆能成才”的人才发展理念，也都生动诠释着新时代数字人才的基本精神风貌。数字人才建设的宽口径、多层次、全类型、高质量、大基数的工作格局形成，也只能由“一代接着一代干，生生世世追梦人”的“久久为功”情怀来托底筑基。追逐数字人才建设的时代梦想，不只要有“只争朝夕”的干劲与创劲，还需要有“久久为功”的担当与气度。

“创新发展，数说未来”。建设网络强国，实现数字经济、智能社会的蓬勃发展，需要有如雨后春笋般的数字人才不断投身其中，追逐使命、光荣与梦想。“逐梦时代，学习为本”。数字人才的锻造练就，则需要不断培育“只争朝夕”和“久久为功”的眼界与境界。建设网

络强国，打造数字中国，实现中国智造，要在造就源源不断、代代相续的数字人才，根在敢于、善于、乐于追逐数字人才建设的时代梦想！（来源：央视网）

➢ 网络安全产业的再思考

网络安全正在变得越来越重要。网络安全产业和人才，是网络安全能力的两大基础。因为有了丰富的优秀人才，才可能有持续的技术创新，而有了繁荣的产业，才能让创新的技术成为产品和服务真正发挥作用，也才能让网络安全形成良好的可持续发展的生态。然而我国的网络安全产业经过二十多年的发展，尽管很多专家学者或者业界精英一直在不断大声疾呼和持续努力，到今天为止却依然发展得不尽人意。这背后到底是什么原因、我们的思路是否有需要调整的地方，可能需要重新思考。

一、我国网络安全产业的几个现象

1、关于产值。有一组数字比较有趣。一般认为，我国网络安全产业到目前为止大概在 300 亿到 500 亿人民币左右的规模；我国每年黑灰产的“产值”至少达到 1000 亿人民币。根据以前的调研结果估算，黑灰产每获取 1 元钱，其造成的损失在 10-30 倍左右。也就是说，每年我国黑灰产造成的损失是万亿级别的。这几个数字放在一起就比较耐人寻味了：如果每年有万亿级别的损失，为什么网络安全产业才能做到百亿级别？网络安全产业界能帮助客户挽回多少损失？

2、关于产业构成。全球网络安全市场中主要收入来源于安全服务，而我国的网络安全市场安全硬件是主要收入来源。这个现象反映的是我国网络安全用户依然认为可以看到的

“盒子”才是货真价实的，而对更具安全保障实效的软件、运营和服务缺乏重视。

3、关于安全现状。我国的网络安全现状不容乐观。以数据安全为例，过去几年，在数据安全能力成熟度模型（DSMM）的试点推广过程中我们进行了大量的测评，数据表明，从数据安全的视角来看绝大部分企业或者组织的能力非常欠缺，全社会的数据安全保护能力比较低。各类不断出现的数据安全事件也从另一个侧面验证了这一点。然而我国传统网络安全产业在满足今天不断增长的数据安全需求方面却还存在很大不足。

从以上现象我们看到，网络安全产业存在几种矛盾交织的现象：一是网络安全问题很突出、客户损失很大，二是客户对安全的理解存在偏差，三是网络安全产业在帮助客户减少损失方面似乎或者有劲使不上，或者心有余而力不足和。

二、我国网络安全产业存在问题的重新思考

1、网络安全产业需要真正从满足客户需求出发，才能实现良性可持续发展和繁荣。政策扶持可以起到早期技术突破或者产业孵化的作用，但是长远的发展或者产业做大还是要依靠真正给客户带来价值。整个世界都在进入快速变化和不确定的第四次工业革命时代，我国目前是数字经济发展最快的国家，也是数字经济最发达的国家之一，因此我国也是网络空间安全遇到问题最多最复杂的国家，对网络安全产业界来说这也意味着全球难得的机会。我国的网络安全产业是否需要调整自己，找准当前时代的客户的安全痛点？面对那万亿级别的损失，或者黑灰产千亿级别的“收入”，网络安全产业界能做些什么？

2、网络安全产业需要服务广大社会客户。当我们说到国家关键信息基础设施安全、说到一些特定重要信息系统安全的时候，我们很容易理解网络安全关系到国家安全。但是这不等于说网络安全产业的客户就仅仅是和国家安全相关的党政军等部门。因为如今的数字时代网络安全和每一个行业都开始发生深刻关联，每个部门、机构、企业甚至个人都将有网络安全需求。一方面，这些需求关系到每个企业和普通百姓的利益，这也是网络安全产业界应该肩负的责任，另一方面，这种市场需求也是网络安全产业生存和发展的基础。所以，满足人民群众日益增长网络安全需求是网络安全产业责无旁贷的任务，也是产业生存和发展的动力源泉。

3、网络安全更多地变成内需，才能让网络安全产业健康持续发展。传统的思路习惯于制定网络安全法律法规或者标准要求，然后用检查和处罚的方式“逼迫”客户进行网络安全投入，进而带动网络安全产业发展。这种方式是一定历史时期的必然，在今天一些特定场景下也依然存在必要性，但无法保证网络安全产业的健康持续发展。因为这种思路下，客户只是被动执行、以实现合规免责为目标，而不是从保护自身利益、以实现安全风险可控为目标。

面对不断变化的安全对抗，前者比较机械和表面功夫，后者才能适应自己的情况、适应对抗的变化和解决客户问题。由于网络安全中的不少威胁类型会直接给企业带来严重损失，越来越多的企业其实不需要别人替他着急，自己就会有强烈需求，而这部分需求会成为网络安全产业最有活力的部分。当然，网络安全十分复杂，从让我做，变为我要做，使网络安全更多地变成内需，需要一个持续教育和发展的过程。

4、简单化的处罚政策无助于网络安全，需要更加细分。有一种观点认为网络安全产业做不起来是因为处罚不够大，这是一个过于粗放的结论。既然网络安全是和攻击者之间的对抗，那么我们就都理解“没有百分之百的安全”，也理解“魔高一尺、道高一丈”和攻防相长的道理。因此，简单化地施行“谁出事谁挨罚”的结果就是，谁今天刚被攻击者狠砍了一刀后，明天就要再被处罚一遍。这就如同家里孩子被坏人欺负了之后，家长不问缘由就再把孩子打一顿，这个逻辑是不是有点问题？或者换句话说，如果被攻破的企业使用了某个网络安全公司的产品，这个罚款就由这个网络安全公司来承担？中国今天大约五千万家企业，80%估计都能很容易被攻破，如果只是处罚的话，今天这 80%的企业要被关门，一年后可能 90%要关门，因为攻击者的能力又增长了。因此，处罚政策需要细化，参考阿里巴巴平台治理的做法，就是“帮助弱的、纠正错的、处罚恶的”。现实中大量的企事业单位是因为不具备足够的资源和条件来完成必要的安全能力建设，对他们应给予帮助，寻找更适合的方案来应对安全威胁。还有一些企事业单位是存在理解或者认知错误，对他们应提供更好的教育或者支持，让他们提早升级适应安全的变化。只有那些故意做恶的或者不作为的企事业单位，才应该是受到严重处罚的对象。谁去帮助那些需要帮助的对象呢？就是网络安全产业界。

5、满足广大中小企事业单位的网络安全需求是重大的挑战和难得机遇。在今天广泛互联融合的数字化时代，网络安全能力相对薄弱的中小企事业单位会成为网络攻击者更“偏爱”的洼地，也会是网络安全威胁的重灾区，同时也会成为攻击者绕过大企业大机构安全防线达到攻击目的的路径。可以说在今天这个时代，不要说各企业、机构，甚至连不同的国家都是网络安全“荣辱共存”的关系了。大企业大机构通常有相对更大的网络安全资源和力量，那些缺乏力量缺乏资源的中小企事业单位的安全需求怎么解决？这既是网络安全产业界的挑战，也是机遇。

6、网络安全要求不能仅看“表面”，还要关注更深的产业链环节。我们过去容易看到“网站”安全，或者“平台”安全，然后将这里作为监督管理的重点。但是今天的网络服务产业链变长，网站或者平台只是其中一部分。例如一个网络购物的行为，表面上是购物平台的网站或者应用，其实完成这个行为还需要商家、独立软件供应商、物流、金融服务等很多环节。

这些看不见的环节的安全也需要关注。

三、我国网络安全产业发展的若干建议

1、重新认识安全。我们正处在第四次工业革命的上半部分，各行各业都在发生快速变化，都在被重新定义，网络安全作为与各行各业都相关的领域，也必须要重新定义。网络安全需要适应今天的业务安全需要、适应大数据时代的数据安全需要，而不再仅仅是过去 IT 时代的思路了。网络安全不再仅仅是国家需要或者大企业的事情，中小企业也有大量的需求。

2、重新考虑制度设计。由于网络安全会变成一个普适需求，而且具有持续对抗的属性，因此传统的特殊行业管理，或者传统的自上而下进行“施压-检查-处罚”的制度设计，可能需要重新考虑。我们越来越有机会通过制度设计激发企事业单位的网络安全内需，让网络安全成为自发的动力获得自下而上的主动式发展，让网络安全和企业的发展机会正相关而不仅仅是成本和责任，这样才能形成真正繁荣的网络安全产业市场，提升整体网络安全水平。

3、调动各方力量实现治理模式。至少未来的三十年左右，社会依然会处于快速发展和不确定的阶段，网络安全也只会越来越复杂。我们无法预见未来技术、业务或者安全的具体情况，然后根据这些情况提前制定好统一的政策标准并且储备好能力，而出现重大偏差却大规模实施的政策标准带来的危害恐怕比网络安全威胁更加致命。唯一的出路在于充分发展和调动各种社会力量，通过多方参与的治理模式，不断进行小范围快速尝试、总结经验、迭代发展。网络安全产业界需要贴近客户，和客户一起积极探索和创新。

如前所述，在这场数字革命中，我国正在面临最复杂的网络安全挑战，但这恰恰也是我们最大的机会。我国网络安全产业界如果能够抓住这个机会，积极创新，不断探索，那么不但有可能在我国建立一个繁荣的网络安全市场，更有可能让我国实现在这个领域的全球引领。因为只有最熟悉数字经济时代最新的业务生产模式、产品技术细节和安全威胁对抗，才可能最懂未来网络安全究竟该怎么做，而这三方面条件，我国是最好的。（来源：杜跃进　阿里巴巴数据安全研究院）

➢ 为个人数据安全加把锁

近日，国家互联网信息办公室发布《数据安全管理办法（征求意见稿）》，不仅对公众关注的个人敏感信息收集方式、广告精准推送、APP 过度索权、账户注销难等问题作出了直接回应，还对网络运营者在数据收集、处理使用、安全监督管理等方面提出了要求，为个人数

据安全加上了一把锁。

随便注册一个应用就要身份证号，推送来的广告好像会“读心”，大数据“杀熟”防不胜防，注销账号“难于上青天”……这些在个人数据保护中频频出现的难题有望迎刃而解。

国家互联网信息办公室日前发布《数据安全管理办法（征求意见稿）》（以下简称《办法》），对网络运营者在数据收集、处理使用、安全监督管理等方面提出了要求，为个人数据安全加上了一把锁。

为啥出台《办法》？这与当前日趋严峻的个人信息滥用和泄露的状况显然息息相关。根据官方对百款常用手机应用统计数据显示，其中相当一部分手机应用存在强制超范围索要权限情况，平均每个应用申请收集个人信息相关权限数有 10 项，但实际上用户不同意开启则 APP 无法安装或运行的权限数平均仅为 3 项。

来自“电子商务消费纠纷调解平台”的大数据同样显示，近年来包括天猫、淘宝、京东、苏宁易购、唯品会等电商平台，以及大众点评、百度糯米、携程等生活服务平台，均曾出现过用户信息泄露事件。仅在 2018 年，就多次出现用户个人信息泄露事件，比如圆通、顺丰十几亿条个人信息在暗网被出售，12306 数百万条旅客信息在网上被出售等。

数据保护“有章可循”

在《办法》中，数据活动被界定为“利用网络开展数据收集、存储、传输、处理、使用等活动”。“与已经发布的《信息安全技术个人信息安全规范》和《互联网个人信息安全保护指南》相比，未来有可能作为部门规章发布的《办法》效力层级更高，既是大数据时代数据

安全的刚需体现，也在为 5G 市场铺平国内数据处理合规化道路。”上海汉盛律师事务所高级合伙人李旻说。

北京观韬中茂（上海）律师事务所合伙人王渝伟也认为，与《网络安全法》相比，此次征求意见稿更为详尽，也有望为未来个人信息保护方面的法律提供参考。

此次《办法》中的“亮点”提法，也让个人数据保护有章可循。一方面，《办法》强调了用户的选择权，如其中明确要求“制定并公开个人信息收集使用规则”，且强调“如果收集使用规则包含在隐私政策中，应相对集中，明显提示，以方便阅读”，突出信息使用规则的重要性，以便个人信息主体享有充分选择权。此外还特别规定，对“网络产品核心业务功能运行的个人信息”以外的信息，网络运营者不得因个人信息主体未同意收集而拒绝提供核心业务功能服务。也就是说，网络运营者不能在数据索取上“漫天要价”。

“这实际上就是为了避免网络服务提供者为了收集数据采取胁迫或者误导行为。”中国社会科学院信息化研究中心秘书长姜奇平表示，信息采集的主导权和选择权必须交给消费者，这是信息服务的原则性问题。

另一方面，《办法》也进一步强调了对用户隐私的保护，《办法》要求“网络运营者以经营为目的收集重要数据或个人敏感信息的，应向所在地网信部门备案”。根据《信息安全技术个人信息安全规范》，包括身份证信息、电话号码、邮箱地址、浏览记录、定位信息乃至个人指纹、声纹，这些都属于个人敏感信息。“通过国家强制力对隐私信息的收集使用予以限制，在隐私信息泄漏时亦有迹可循，以实现个人隐私信息的数据安全。”李旻说。

中国信息安全研究院副院长左晓栋表示，只有能对隐私信息的收集者追根溯源，才能从源头保护个人数据安全。

解决方法直面“痛点”

“《办法》对于近年来层出不穷的网络数据安全问题予以细化，针对新型数据安全管理的规定能及时填补因社会发展导致的法律漏洞，具有前瞻性。”李旻说。

从《办法》的具体规定来看，不少一直困扰用户的“痛点”被明确点名，比如刚订了一张机票，马上各个应用就开始推荐目的地相关信息，这种利用用户浏览历史，通过定向推送获得广告收入的“精准广告”，让不少用户觉得毫无隐私。对此，《办法》明确规定，要求利用用户数据和算法推送新闻信息、商业广告需显著标明“定推”字样，并为用户拒绝接受定向推送信息提供选择权，“用户选择停止接收定向推送信息时，应当停止推送，并删除已经收集的设备识别码等用户数据和个人信息”。

“广告主采集用户的信息难度会增加，但这也是全球范围内的大趋势，各个主要国家的

相关法规，也都在强调保护消费者的个人数据隐私。”网络广告平台 Marteker 创始人冯祺表示。

再比如，针对账号注销难，账号注销后个人信息消除难，《办法》也特别提出，要保护用户的“被遗忘权”。《办法》强调，“收集使用规则应突出个人信息主体撤销同意，以及查询、更正、删除个人信息的途径和方法”。“网络运营者收到有关个人信息查询、更正、删除以及用户注销账号请求时，应当在合理时间和代价范围内予以查询、更正、删除或注销账号。”

“突出‘被遗忘权’保护也是办法的一个亮点。‘被遗忘’是消费者的合理诉求。”左晓栋说。

在北京亿达（上海）律师事务所律师董毅智看来，“被遗忘权”仍需进一步细化，“比如，在用户注销账户后，网络经营者对于已经散发出去的信息如何处理？用户是否有权要求网络经营者对已经散发出去的信息予以删除或者负责？”

此外，包括“网络爬虫”访问收集流量不得超过网站日均流量的三分之一，限制“大数据杀熟”等歧视性推送行为，明确数据安全责任人的任职要求，要求提供数据安全责任人的姓名及联系方式等，《办法》中的相关规定，为个人数据保护中的一系列热点问题提供了解决方案。

“互联网行业头部企业的天然主导性，导致行业内部缺乏竞争，基于用户对平台服务的信任而建立起的黏性，不能成为某些平台实行差别定价、数据反复买卖的底气。从这个角度来讲，《办法》对同行业、跨行业之间企业联手利用用户信息的合规性提出了新要求。”董毅智表示。（来源：中国经济网）

➢ IPv6 是建设网络强国重要契机

依托飞速发展的各种通讯技术，互联网已经成为网络空间最重要的信息基础设施和网络信息体系最基础的承载平台。

互联网体系结构是互联网的关键核心技术，主要研究互联网的各部分功能组成及其相互关系。在这个体系结构中，网络层承上启下，保证全网通达，是核心。

网络层向下兼容当前各种通信系统，包括高速光纤通信系统、卫星通讯系统以及当前最热的 3G、4G、5G 等现代移动通信系统。各种各样的通信系统，使互联网自身的传输速度和带宽不断优化和发展。在网络层之上，由于信息技术的创新，新的应用层出不穷，使互联网

成为推动整个社会进步的重要支撑力量。

互联网是连接计算机的网络。目前在计算机技术领域，包括中央处理器的芯片技术以及软件的操作系统等信息社会发展中所依赖的最基础的关键核心技术，我们还处在艰苦的爬坡过坎阶段。

互联网体系结构包含三个基本要素。第一是全网统一的传输格式。IPv4 是现有互联网传输格式的协议，IPv6 定义了未来新的传输格式，通过 IPv6 的格式定义，网络层过渡到了新的一代，传输格式是网络层的最基本要素，从互联网发明到今天已经 50 年，传输格式的迭代只有 IPv4 和 IPv6 两个阶段。第二是转换方式。在统一的传输格式基础上，互联网要解决如何将数据和信息从网络的一个端点传送到另一个端点的传输模式。对于互联网的转换方式历史上曾经出现有连接、无连接两种不同的技术路线，经过长时间的比较竞争，互联网无连接分组交换技术成为主流，它保证了互联网的传输以最高效的方式得以实现。第三是路由控制。在传输格式和转换方式相对稳定的基础上，路由控制必须不断地满足不同应用和不同通讯手段、通讯方式变化的需求，以达到全网最优。

互联网体系结构的发明人、图灵奖获得者温登·瑟夫指出，互联网在设计之初，就定义了原型必须满足以下条件：

第一，互联网必须具有面向任何应用的普适性，不是为任何特殊应用设计，而是能支撑语音、视频、IP 电话……任何应用。

第二，互联网的信息传输可以针对任何通信技术实现兼容，包括电子电路、微波、光纤、无线、3G/4G/5G……

第三，允许在网络边缘创新，不需要为增加任何新的应用和服务而改变网络结构，这就是窄腰结构的优势，基本结构保持不变，应用可以无限扩展。

第四，可扩展。互联网需要支持用户规模的持续扩大，现在互联网上连接的用户已经近 40 亿，IPv4 的地址空间不足，因此发展 IPv6 势在必行。

第五，互联网向任何新协议、新技术和新应用开放。互联网的兼容、开放、可扩展特征，决定了它是一个不断演进，不断延伸，不断成长的网络，路由控制是互联网创新的最主要领域。

随着人工智能、万物互联的技术趋势，互联网上承载的应用将会日益繁多，从 IPv4 向 IPv6 迭代已经是大势所趋。

推动互联网技术发展的国际组织是 IETF（The Internet Engineering Task Force）。该机构最高领导层为 IAB （Internet Architecture Board）即互联网体系结构工作组，其使命是保证互联网平稳的发展。IAB 已经在全球确立了互联网从 IPv4 向 IPv6 演进的必然趋势。其演进过程还会出现各种各样的问题，IETF 的主要宗旨就是发现问题，并且有针对性地解决问题，将其确定为国际标准。截至到 2018 年 6 月 30 日，IETF 已完成 8439 项 RFC（Request For Comments），其中，由中国牵头的有 101 项。可见，中国在互联网体系结构和互联网关键技术领域还是初学者，发言权有限。

IPv6 是中国参与全球互联网技术发展的重要契机。为推进相关工作深入推进，我国确立了推动下一代互联网规模部署的行动计划，进一步明确了发展下一代互联网的必要性、主要目标、重点任务和保障措施，要求“从互联网应用、网络基础设施、应用基础设施、网络安全、关键前沿技术等五大领域深化 IPv6 发展。”其中特别强调了要强化网络安全，维护国家信息网络安全保障，突破关键前沿技术，构建自主创新的下一代互联网技术产业形态。

习近平总书记指出，美欧等主要国家正在加紧布局下一代互联网，我们要加快实施步伐，争取在下一轮竞争中迎头赶上。我们必须按此要求，大力推进从 IPv4 向 IPv6 的迭代演进，为建设网络强国打下更为坚实的基础。（来源：人民日报海外版 吴建平）

四、政府之声

➢ 国家互联网信息办公室发布《数据安全管理办法（征求意见稿）》

2019 年 5 月 28 日，国家互联网信息办公室发布为了维护国家安全、社会公共利益，保护公民、法人和其他组织在网络空间的合法权益，保障个人信息和重要数据安全，根据《中华人民共和国网络安全法》等法律法规，国家互联网信息办公室会同相关部门研究起草了《数据安全管理办法（征求意见稿）》，现向社会公开征求意见。

征求意见稿，其分总则、数据收集、数据处理使用、数据安全监督管理、附则五章，共包含四十条规定。“征求意见稿”在个人信息收集、爬虫抓取、广告精准推送、APP 过度索取权限、账户注销难等经常涉及隐私的问题上均做出了明确规定。（来源：国家互联网信息办公室）

- **《数据安全管理办法（征求意见稿）》**
- **全文：**http://www.cac.gov.cn/2019-05/28/c_1124546022.htm

➢ 工信部: 关于做好 2019 年电信和互联网行业网络安全行政检查工作的通知

2019 年 5 月 30 日，工业和信息化部网络安全管理局发布关于做好 2019 年电信和互联网行业网络安全行政检查工作的通知：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，中国广播电视网络有限公司，互联网域名注册管理和服务机构，互联网企业，有关单位：

为深入贯彻习近平总书记关于网络安全的系列重要讲话精神，切实做好新中国成立 70 周年网络安全保障工作，全面提升电信和互联网行业网络安全防护水平，根据《中华人民共和国网络安全法》《通信网络安全防护管理办法》《电信和互联网用户个人信息保护规定》等法律法规，决定组织开展 2019 年电信和互联网行业网络安全行政检查工作。现将有关要求通知如下：

一、总体要求

紧紧围绕加快推进网络强国建设战略目标，加快落实《中华人民共和国网络安全法》，坚持以查促建、以查促管、以查促防、以查促改，以防攻击、防入侵、防篡改、防窃密为重点，深入查找网络安全风险隐患并强化整改，落实基础电信企业、域名注册管理和服务机构、互联网服务提供者的主体责任，加强网络安全防护能力建设，着力防范重大网络安全风险，保证电信网和公共互联网持续稳定运行和数据安全。

二、检查对象

检查对象为依法获得电信主管部门许可的基础电信企业、互联网企业、互联网域名注册管理和服务机构(以下统称“网络运行单位”)建设与运营的网络和系统。重点是电信和互联网行业网络基础设施，通过公共互联网收集、存储与处理用户信息和网络数据的重要信息系统，包括但不限于：IP 承载网、支撑网、互联网数据中心、公共云服务平台、互联网内容分发网络、域名服务系统、工业互联网平台、企业门户网站、即时通信系统、网络交易系统、电子邮件系统、软件应用商店、移动应用程序及后台系统、公众无线局域网、公众视频监控平台等。

三、检查内容

检查网络运行单位落实《中华人民共和国网络安全法》《通信网络安全防护管理办法》《电信和互联网用户个人信息保护规定》等法律法规情况，电信和互联网安全防护体系系列标准符合情况，仍然存在的弱口令、漏洞和其他风险隐患等。主要包括：

(一)网络安全管理落实情况。重点检查内部安全管理制度制定与落实、网络安全责任部门和人员履职尽责情况，本单位网络与系统的定级备案、符合性评测和安全风险评估工作开展情况，网络安全教育和培训开展情况等。

(二)网络安全防护技术手段。重点检查网络隔离、身份鉴别、访问控制、口令管理、边界防护、数据保护、容灾备份、安全审计等网络安全防护技术措施的标准符合性和有效性，

以及网络安全监测手段的建设和运行情况。

(三)仍然存在的漏洞等风险隐患。重点检查软硬件系统存在的漏洞、弱口令、后门、被植入恶意程序、网站被篡改、被非法入侵、被非法远程控制等。

四、工作安排

(一)自查自纠。各单位全面梳理所有正式上线运行的网络与系统，7 月 10 日前，在“通信网络安全防护管理系统”(https://www.mii-aqfh.cn)完成定级备案，并核实已有备案信息的内容，对不准确、不完整的备案信息予以补正，定级备案完成情况将作为电信主管部门检查评估的重点内容。组织开展本单位网络与系统的自查评估，及时整改并做好自查总结，7 月 15 日前，基础电信企业集团公司和域名注册管理机构将本单位自查工作总结报告报部(网络安全管理局)，基础电信企业省级公司、域名注册服务机构和互联网公司根据属地通信管理局要求上报自查总结报告。

(二)检查评估。电信主管部门选取部分重要的网络和系统，委托专业技术机构采取现场访谈、资料查阅、现场检测、远程渗透、代码检测等方式进行现场检查;选取部分与公共互联网连接的重要信息系统进行远程技术检测。对检查过程中发现的问题，电信主管部门通过整改通知书等形式责令被检查单位限期整改。各地通信管理局除抽查基础电信企业省级公司外，还要抽查当地重点互联网企业和域名注册服务机构，并可对属地内基础电信企业集团公司直属专业公司进行抽查，将检查工作总结报告于 8 月 31 日前报部(网络安全管理局)。

(三)整改问责。各单位对检查发现的薄弱环节和安全风险进行深入整改，并及时向电信主管部门报告整改情况。对基础电信企业省级公司和专业公司，将其网络和系统检查结果作为 2019 年省级基础电信企业和专业公司网络与信息安全责任考核依据。对域名注册管理和服务机构、互联网企业，发现存在违反法律法规行为、问题拒不改正或导致危害网络安全等后果的，依法依规给予行政处罚。

五、工作要求

(一)高度重视，落实责任。各单位要充分认识到网络安全行政检查是电信主管部门依法开展行政管理和推进网络安全防护工作落实的重要举措，加强组织领导，制定工作方案，明确责任分工，全面深入开展自查自纠工作，积极配合电信主管部门做好监督检查，坚决确保重大活动期间网络安全。

(二)规范检查，严明纪律。按照《国务院办公厅关于推广随机抽查规范事中事后监管的通知》，随机抽取检查对象、随机选派检查人员，及时公开检查情况和结果。规范检查方法和程序，避免检查工作影响网络和系统的正常运行。被检查单位对检查工作中出现的违规违

纪行为，可通过电话(010-66022093)或邮箱(wac@miit.gov.cn)进行投诉。

(三)问题导向，注重实效。各单位要强化问题导向，改进自查评估和监督检查的方法，增强问题发现和整改能力，既要解决已发现的问题，又要注重挖掘问题背后的制度不健全、责任不落实、技术能力不足、人员队伍欠缺等深层次原因，举一反三，切实提升检查工作实效，健全网络安全问题闭环管理机制。（来源：中华人民共和国工业和信息化部网络安全管理局）

➢ 国家互联网信息办公室发布《儿童个人信息网络保护规定（征求意见稿）》

2019 年 5 月 31 日，国家互联网信息办公室（以下简称“网信办”）日前发布了关于《儿童个人信息网络保护规定（征求意见稿）》公开征求意见的通知。网信办称，此次征求意见是为了规范收集使用儿童个人信息等行为，保护儿童合法权益，为儿童健康成长创造良好的网上环境。此次意见反馈截止日期为 2019 年 6 月 30 日。

此次意见稿的适用对象为不满 14 周岁的未成年人。意见稿提出，网络运营者应当设置专门的儿童个人信息保护规则和用户协议，并设立个人信息保护专员或者指定专人负责儿童个人信息保护。适用于儿童的用户协议应当简洁、易懂。

同时，网络运营者使用儿童个人信息，不得超出约定的目的和范围。因业务需要，确需超出目的和范围使用的，应当再次征得儿童监护人的明示同意。

此外，意见稿规定，网络运营者发现儿童个人信息发生或者可能发生泄露、毁损、丢失的，应当立即启动应急预案，采取补救措施；造成或者可能造成严重后果的，应当立即向有关主管部门报告，并将事件相关情况以邮件、信函、电话、推送通知等方式告知受影响的儿童及其监护人，难以逐一告知的，应当采取合理、有效的方式发布相关警示信息。

违反本规定的，根据情节单处或者并处警告、没收违法所得、处违法所得 1 倍以上 10 倍以下罚款，没有违法所得的，处 100 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 1 万元以上 10 万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任。（来源：国家互联网信息办公室）

- **《儿童个人信息网络保护规定（征求意见稿）》**
- **全文：**http://www.cac.gov.cn/2019-05/31/c_1124568048.htm

➢ 工信部公开征求《网络关键设备安全检测实施办法（征求意见稿）》意见

2019 年 6 月 5 日，工业和信息化部为贯彻落实《中华人民共和国网络安全法》，推进网络关键设备安全检测工作顺利开展，工业和信息化部起草了《网络关键设备安全检测实施办法（征求意见稿）》（见附件），拟以规范性文件形式印发，现面向社会公开征求意见。

如有意见或建议，请于 2019 年 7 月 4 日前反馈。（中华人民共和国工业和信息化部网络安全管理局）

- **《网络关键设备安全检测实施办法（征求意见稿）》全文：**
- http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057724/n3057728/c6991606/part/6991612.docx

五、本期重要漏洞实例

➢ Cisco 多个产品拒绝服务漏洞

发布日期：2019-06-06
更新日期：2019-06-06
受影响系统：
Cisco Firepower Threat Defense Software
Cisco Cisco Firepower Threat Defense Virtual (FTDv)
Cisco Cisco Firepower Threat Defense Software 6.3
Cisco Cisco Firepower Threat Defense Software 6.2.3
Cisco Cisco Firepower Threat Defense Software 6.2.2
Cisco Cisco Firepower Threat Defense Software 6.2.1
Cisco Cisco Firepower 9300 Security Appliance
Cisco Cisco Firepower 4100 Series
Cisco Cisco Firepower 2100 Series
Cisco Cisco ASA Services Module for Cisco Catalyst 6500
Cisco Cisco ASA Services Module for Cisco 7600 Series Ro
Cisco Cisco ASA 5500-X Series Firewalls
Cisco Cisco Adaptive Security Virtual Appliance (ASAv)
Cisco Cisco Adaptive Security Appliance (ASA) Software 9.9
Cisco Cisco Adaptive Security Appliance (ASA) Software 9.9
Cisco Cisco Adaptive Security Appliance (ASA) Software 9.8
Cisco Cisco Adaptive Security Appliance (ASA) Software 9.8
Cisco Cisco Adaptive Security Appliance (ASA) Software 9.7
Cisco Cisco Adaptive Security Appliance (ASA) Software 9.7
Cisco Cisco Adaptive Security Appliance (ASA) Software 9.6
Cisco Cisco Adaptive Security Appliance (ASA) Software 9.6
Cisco Cisco Adaptive Security Appliance (ASA) Software 9.10
Cisco Cisco Adaptive Security Appliance (ASA) Software 9.10
Cisco Cisco 3000 Series Industrial Security Appliance (I
不受影响系统：
Cisco Firepower Threat Defense Software 6.3.0.3
Cisco Firepower Threat Defense Software 6.2.3.12
Cisco Cisco Adaptive Security Appliance (ASA) Software 9.9.2.50
Cisco Cisco Adaptive Security Appliance (ASA) Software 9.8.4
Cisco Cisco Adaptive Security Appliance (ASA) Software 9.6.4.25
Cisco Cisco Adaptive Security Appliance (ASA) Software 9.10.1.17
描述：

BUGTRAQ ID: 108182
CVE(CAN) ID: CVE-2019-1697

思科自适应安全设备（ASA）软件是为 Cisco ASA 系列提供强大功能的核心操作系统。它拥有多种外观，为 ASA 设备提供企业级防火墙功能 - 独立式设备(US)、刀片(US)和虚拟。ASA 软件还与其他关键安全技术集成，以提供功能全面的解决方案，满足不断发展的安全需要。
思科的 FirePower Threat Defense(FTD)软件整合了 ASA 特性以及 FirePower 特性的软性。
思科自适应安全设备（ASA）软件和 Firepower 威胁防御（FTD）软件中轻量级目录访问协议（LDAP）功能实施中的漏洞可能允许未经身份验证的远程攻击者导致受影响的设备重新加载，从而导致拒绝服务（DoS）条件。这些漏洞是由于对发送到受影响设备的 LDAP 数据包的解析不当造成的。攻击者可以通过使用基本编码规则（BER）发送精心设计的 LDAP 数据包来利用这些漏洞，以便受影响的设备进行处理。成功利用可能允许攻击者重新加载受影响的设备，从而导致 DoS 状况。
<*来源：Marcelo Coelho
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-asa-ftds-lda
*>
建议：

厂商补丁：
Cisco

Cisco 已经为此发布了一个安全公告（cisco-sa-20190501-asa-ftds-ldapdos）以及相应补丁：
cisco-sa-20190501-asa-ftds-ldapdos：Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Lightweight Directory Access Protocol Denial of Service Vulnerability
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-asa-ftds-lda

➢ Oracle E-Business Suite cpuapr2019 多个安全漏洞

发布日期：2019-06-06
更新日期：2019-06-06
受影响系统：
Oracle E-Business Suite 12.2.8
Oracle E-Business Suite 12.2.7
Oracle E-Business Suite 12.2.6
Oracle E-Business Suite 12.2.5
Oracle E-Business Suite 12.2.4
Oracle E-Business Suite 12.2.3
Oracle E-Business Suite 12.1.3
Oracle E-Business Suite 12.1.2
Oracle E-Business Suite 12.1.1
描述：

BUGTRAQ ID: 107938
CVE(CAN) ID: CVE-2019-2638/CVE-2019-2633

甲骨文公司的应用产品，全称是 Oracle 电子商务套件（E-Business Suit），是在原来 Application（ERP）基础上的扩展，包括 ERP（企业资源计划管理）、HR（人力资源管理）、CRM（客户关系管理）等等多种管理软件的集合，是无缝集成的一个管理套件。

CVE-2019-2633：Oracle E-Business Suite 的 Oracle Work in Process 组件中的漏洞（子组件：消息）。受影响的受支持版本为 12.1.1,12.1.2,12.1.3,12.2.3,12.2.4,12.2.5,12.2.6,12.2.7 和 12.2.8。易于利用的漏洞允许低权限攻击者通过 HTTP 进行网络访问，从而危及 Oracle Work in Process。成功攻击此漏洞可能导致对关键数据或所有 Oracle Work in Process 可访问数据的未授权创建，删除或修改访问，以及对关键数据的未授权访问或对所有 Oracle Work in Process 可访问数据的完全访问。

CVE-2019-2638：Oracle E-Business Suite 的 Oracle General Ledger 组件中的漏洞（子组件：Consolidation Hierarchy Viewer）。受影响的受支持版本为 12.1.1,12.1.2,12.1.3,12.2.3,12.2.4,12.2.5,12.2.6,12.2.7 和 12.2.8。易于利用的漏洞允许通过 HTTP 进行网络访问的低权限攻击者破坏 Oracle 总帐。成功攻击此漏洞可能导致对关键数据或所有 Oracle General Ledger 可访问数据的未授权创建，删除或修改访问，以及对关键数据的未授权访问或对所有 Oracle General Ledger 可访问数据的完全访问。

<*来源：Onapsis 的 Martin Doyhenard

链接：https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html

*>

建议：

厂商补丁：

Oracle

Oracle 已经为此发布了一个安全公告（CVE-2019-2638/CVE-2019-2633）以及相应补丁：

CVE-2019-2638/CVE-2019-2633：Oracle Critical Patch Update Advisory - April 2019

链接：https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html

➢ Apache UIMA DUCC Webserver 跨站脚本执行漏洞

发布日期：2019-06-06

更新日期：2019-06-06

受影响系统：

Apache Apache uimaDUCC 2.2.2

Apache Apache uimaDUCC 2.2

Apache Apache UIMA DUCC 2.2.1

Apache Apache UIMA DUCC 2.1

Apache Apache UIMA DUCC 2.0.1

Apache Apache UIMA DUCC 2.0

Apache Apache UIMA DUCC 1.1

Apache Apache UIMA DUCC 1.0

描述：

BUGTRAQ ID: 108195

CVE(CAN) ID: CVE-2018-8035

DUCC 是一个 Linux 集群控制器，旨在扩展任何 UIMA 管道，用于高吞吐量收集处理作业以及低延迟实时应用程序。在 UIMA-AS 的基础上，DUCC 特别适合在多个线程中运行大型内存 Java 分析，以便充分利用多核机器。DUCC 管理跨群集部署的所有进程的生命周期，包括非 UIMA 进程，如 tomcat 服务器或 VNC 会话。

此漏洞与用户对 DUCC 网页输入数据的浏览器处理有关。在用户浏览器中运行的包含 Apache UIMA DUCC(<= 2.2.2)的 javascript 无法充分过滤用户提供的输入，这可能导致用户提供的意外执行 javascript 代码。

<*来源：Marshall Schor

*>

建议：

厂商补丁：

Apache

目前厂商还没有提供补丁或者升级程序，我们建议使用此软件的用户随时关注厂商的主页以获取最新版本：

http://syncope.apache.org/security.html

➢ Microsoft SQL Server 信息泄露漏洞

发布日期：2019-06-04

更新日期：2019-06-04

受影响系统：

Microsoft SQL Server 2017 for x64-based Systems

描述：

BUGTRAQ ID: 108249

CVE(CAN) ID: CVE-2019-0819

SQL Server 是 Microsoft 公司推出的关系型数据库管理系统。具有使用方便可伸缩性好与相关软件集成程度高等优点，可跨越从运行 Microsoft Windows 98 的笔记本电脑到运行 Microsoft Windows 2012 的大型多处理器的服务器等多种平台使用。

Microsoft SQL Server Analysis Services 在不正确地强制执行元数据权限时，存在信息泄露漏洞。成功利用此漏洞的攻击者可以查询他们没有访问权限的表或列。

要利用此漏洞，经过身份验证的攻击者需要向受影响的 Analysis Services 数据库提交查询。

<*来源：Microsoft

链接：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0819

*>

建议：

厂商补丁：

Microsoft

Microsoft 已经为此发布了一个安全公告（CVE-2019-0819）以及相应补丁：

CVE-2019-0819：Microsoft SQL Server Analysis Services Information Disclosure Vulnerability

链接：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0819

六、本期网络安全事件

➢ 离职员工抄袭老东家软件获刑 2 年 4 个月

2019 年 6 月 3 日，广东省广州市天河区人民法院审理的一起侵犯商业秘密案件引起社会关注。经审理查明，北京麒麟合盛科技有限公司(以下简称麒麟科技)是麒麟合盛网络技术股份有限公司(以下简称麒麟网络)的全资子公司，两家公司主要从事提供海外移动互联网服务方面业务，其公司核心技术以及商业模式均应用在海外市场。

黄礼强、钱振鹏、李娴、裴智松 4 名被告人曾受雇于麒麟科技，双方签订的《劳动合同》中有保密和竞业禁止条款。在职期间，4 名被告人事先合谋，利用工作时掌握的产品源代码、商业运营资料等商业秘密，研发与公司类似的手机安卓系统清理软件产品营利，并在离职前将资料带走。

2016 年 10 月 26 日，4 名被告人筹备设立上海厚乘信息技术有限公司(以下简称厚乘公司)，公司营利性业务为手机安卓系统清理软件，包括 Color Booster 等产品，这些软件基本功能相同。经鉴定，Color Booster 软件源代码中，至少存在 67 个函数与麒麟科技两款软件源代码相同或实质相似，且这些都属于不为公众所熟知的技术信息。厚乘公司的 Color Booster 等软件由 4 名被告人上传至某国外应用市场供用户下载使用，并通过与多个网络平台合作的广告费用营利。

麒麟科技于 2017 年 1 月 6 日向广州市公安局进行控告。广州市公安局立案侦查后，认

为上述 4 人的行为已涉嫌侵犯商业秘密罪，并经进一步调查取证后由广州市天河区人民检察院依法对 4 人提起公诉。经查，自 2016 年 8 月 9 日起，厚乘公司账户实际获利共计 98975.3 美元(以当日汇率折算，约合人民币 680059.29 元)。5 月 16 日，广州市天河区人民法院认为黄礼强等 4 名被告人的行为已构成侵犯商业秘密罪。归案后均能供认主要犯罪事实，并自愿认罪认罚，可以从轻处罚。据此作出一审判决，判处黄礼强有期徒刑 2 年 4 个月 15 天，并处罚金 24 万元；对钱振鹏、李娴、裴智松分别判处有期徒刑 2 年 3 个月 15 日，并处罚金 15 万元；追缴 4 名被告人以及厚乘公司违法所得 680059.29 元，予以没收。同时，麒麟科技保留追究民事法律责任的权利。

对于本案所涉的焦点问题，《法制日报》记者与相关专家进行了对话。

对话人：中国人民大学法学院教授 刘俊海；中华全国律师协会信息网络与高新技术专业委员会副主任陈际红

记者：离职员工带走公司的商业秘密(软件源代码)并牟利。请简要分析一下这种行为。

陈际红：这是一起典型的侵犯商业秘密案件，在这起案件里受法律保护的标的是软件的源代码。软件源代码受双重保护，一方面，受著作权法保护；另一方面，如果源代码本身没有公开，那么也受反不当竞争法里面的商业秘密保护。此案中的违法行为属于在反不当竞争法中对商业秘密保护的一种违法形态：通过披露、使用、传播非法获取的商业秘密，侵犯商业秘密的表现形式。此外，离职员工还涉嫌触犯了刑法中关于商业秘密犯罪的条款。

刘俊海：这种行为涉嫌侵害原用人单位的商业秘密，违反了反不正当竞争法，也触犯了刑法。此行为侵害了商业秘密所有权企业的核心竞争力，也造成企业和企业之间的不公平竞争，恶化了诚实守信的商业生态环境，同时颠覆了雇主和雇员之间的劳资关系。

记者：商业秘密在法律上如何界定？

陈际红：商业秘密认定通常包含三性：秘密性，保密性和实用性。秘密性是指商业秘密的标的本身没有公开；保密性是指在公司里对于商业秘密本身要采取保密措施；实用性是指商业秘密本身能为权利人带来利益。三者皆具备，就构成了商业秘密。

刘俊海：商业秘密在反不正当竞争法里有界定，一是技术秘密，二是经营秘密。

记者：员工与公司签订保密协议，离职后还需要对相关内容保密吗？

陈际红：公司和员工签订保密协议的相应义务，不会因为员工的劳动合同关系终止而终止，即使劳动关系终止后，只要员工签订的保密协议还在有效期，那么离职员工仍要遵循保密协议规定。员工离职后，如果违反原来签署的保密协议，仍构成违法。（来源：法制日报）

➢ 美国汉堡连锁品牌 Checkers 遭黑客攻击 102 家门店 POS 机被感染

2019 年 5 月 31 日，美国快餐连锁品牌 Checkers & Rally's 遭遇恶意程序攻击，15%的美国门店 POS 机被感染，导致严重的数据泄露。Checkers 是美国境内最大的免下车汉堡连锁餐馆之一，总部位于佛罗里达州坦帕市，目前已经在美国 28 个州开拓业务。

黑客攻击了 Checkers 的支付系统，并且在 100 多家线下门店的 POS 系统中植入了恶意软件。这些恶意软件会收集支付卡磁条上的数据，包括持卡人姓名、支付卡号、卡验证码以及到期日期等等。

Checkers 在本周三的安全公告中表示：“近期我们发现部分 Checkers & Rally's 线下门店出现了恶意程序导致数据泄露问题。在发现这个问题之后，我们快速聘请了业内的数据安全专家进行广泛调查，并配合联邦执法机构协同受影响餐馆解决这个问题。”

目前 Checkers 没有回应外媒 Threatpost 的评论请求。 Checkers 表示，根据调查结果，没有证据表明持卡人信息以外的数据受到此问题的影响。

目前美国 20 个州的 102 家 Checkers 门店被发现存在恶意程序，其中最早一笔支付发生在 2015 年 12 月。Checkers 在其官方网站上罗列了本次受影响的所有门店信息。(来源:cnBeta)

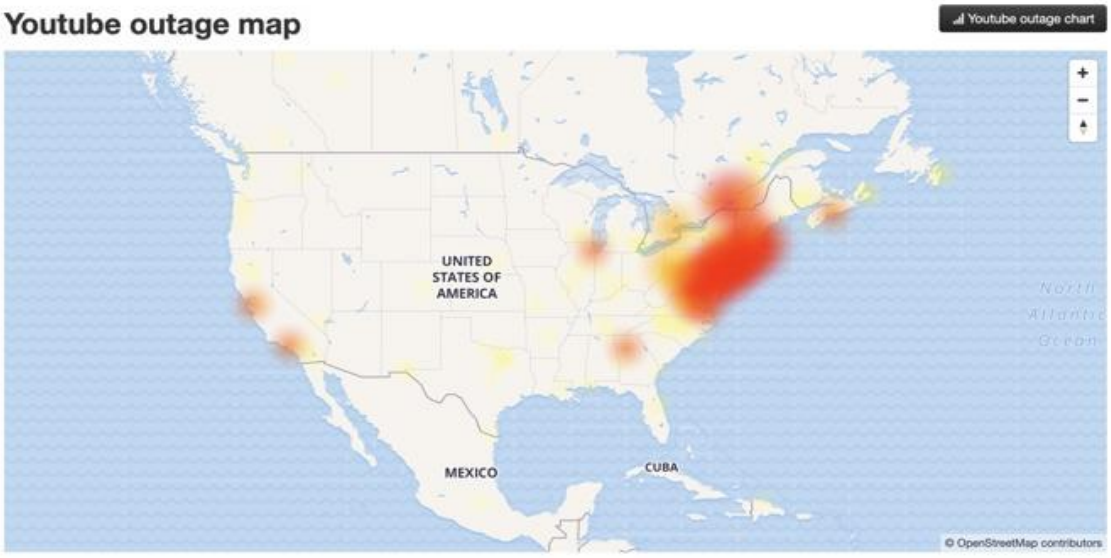
➢ 谷歌多项服务全球大规模宕机：涵盖 YouTube、Gmail 等

2019 年 6 月 3 日，本周日，谷歌在全球范围内遭遇了大规模中断，包括 Gmail、YouTube 和 Google Drive 在内基于谷歌云架构服务的诸多谷歌服务均受到影响。本次宕机于北京时间

6 月 3 日凌晨 2 点 58 分开始，用户访问谷歌服务出现各种错误提醒，并且阻止用户访问电子邮件、上传 YouTube 视频等等。

根据谷歌官方状态页面显示，包括 Gmail, Calendar, Drive, Docs, Sheets, Slides, Hangouts, Meet, Chat 和 Voice 在内的谷歌服务均无法使用。那些依赖于谷歌云架构的第三方服务同时也受到影响，目前谷歌官方并没有完全恢复的预估时间，也没有公布关于本次宕机事件的根本原因。

苹果的 iCloud 服务也受到轻微影响，苹果报告称有不到 1%的用户出现了响应时间低于正常值的情况。AppleInsider 也进行了测试，但是并没有出现任何中断或者卡顿的情况。



凌晨 4 点 45 分：谷歌报告称，由于网络比较拥挤“用户可能会看到性能下降或者间歇性错误”。谷歌表示已经确认了造成拥堵的根本原因，预计很快会恢复正常。

凌晨 6 点：在简讯中，谷歌承认这些问题， 并表示工程团队已经完成缓解工作的第一阶段，目前正在实施第二阶段，应该会尽快修复正常。（来源：cnBeta）

➢ 羊城通 APP 和乘车码遭恶意网络攻击，现已恢复服务

2019 年 5 月 29 日，羊城通乘车码竟然瘫痪了？昨夜，记者接到市民爆料，称乘坐公共交通时无法正常使用羊城通乘车码进行扫码付款。昨夜，羊城通公司表示已进行系统升级修复；今日，羊城通公司发布公告称，羊城通 APP 和羊城通乘车码已恢复正常服务，而此次异常则是由于网络遭到恶意攻击。这种尴尬 你遇到了吗？

出门不带钱包，手机一刷即可上车，这已然成为不少广州市民们的出行习惯。然而昨日晚高峰，不少市民在如常打开乘车码时却陷入了无法扫码的尴尬。“实在是太尴尬了，从上车开始站到司机旁边开始弄，到最后快到站了还没扫出来。”市民卢女士表示，她最后只能让朋友截图帮忙刷。市民艾女士也颇为窘迫：“我一直以为是自己的手机问题，站在司机旁边一直刷一直刷，真的很尴尬！羊城通忘记充钱，乘车码用不了，在包包里找了很久才找出两块钱！”

在社交媒体上，不少广州乘客都在吐槽自己的遭遇，有的果断选择放弃下车步行两公里回家，有的则是极为尴尬地问旁边的陌生人借零钱，还有的表示自己坐了“霸王车”，只能和司机师傅一直说抱歉。记者也在支付宝上搜索了羊城通乘车码，界面没有照常显示二维码，只有“正在加载”；在小程序中，界面则一直显示：“如刷码失败，请点击刷新乘车码”。

乘车码异常为遭到恶意攻击

28 日 19 时许，羊城通公司发布关于羊城通 APP 和羊城通乘车码系统升级修复的公告，称据运营监控，今天下午 17：00 发现羊城通 APP 和羊城通乘车码无法正常使用，目前公司

相关技术人员正在进行系统升级修复。市民张先生看到公告后质疑道：“升级修复不会提前发通知的吗？这样临时来一出，会造成多少人不方便？5 点出问题，一直到 7 点才出来发公告？”

29 日 7 时许，羊城通公司发布关于羊城通 APP 和羊城通乘车码恢复服务的公告，称：**“目前羊城通 APP 和羊城通乘车码已恢复正常服务。”以下为公告全文：**

关于羊城通APP和羊城通乘车码恢复服务的公告

羊城通 今天

尊敬的羊城通客户：

感谢您一直以来对羊城通服务的关注和支持！

据羊城通公司2019年5月28日下午17:00运营监控，发现羊城通APP和羊城通乘车码无法正常使用，已及时通过羊城通官网、羊城通新浪微博发布了公告；目前羊城通APP和羊城通乘车码已恢复正常服务。

本次异常情况是由于网络遭到了恶意攻击，羊城通公司已立即向公安机关报案，并启动应急预案。广东省网络安全应急响应中心、市网信办等单位派出多名专家协助羊城通公司技术人员对异常情况进行全面排查，迅速定位问题，并制定解决方案全力修复，羊城通APP和羊城通乘车码服务于当晚22:00逐步恢复。

羊城通提醒：部分用户如使用羊城通乘车码微信小程序无法显示或刷新的，可长按羊城通乘车码小程序，将其拖动到手机底部删除后，重新在微信搜索栏输入“羊城通乘车码”，即可重新获得羊城通乘车码小程序并使用；若仍无法使用，请关机重启。（来源：广州日报大洋网）

➢ 浙江首例:用户买房后信息被泄露检察机关启动公益诉讼

2019 年 6 月 2 日，买新房本是喜事，可却因为个人信息被泄露遭遇广告推销，电话不断。近日，浙江省诸暨市检察院提起公诉的陈某、杨某、骆某等人，因犯侵犯公民个人信息罪被判刑。同时，诸暨市检察院还启动公益诉讼，向诸暨市市场监督管理局发出诉前检察建

议书，向诸暨市建设局及装修装饰行业协会发出工作函，取得了良好的社会效果。

案情回顾

2017 年 12 月，小朱刚刚买了一套婚房，没多久，便开始接到各种各样的推销电话，一天少则一两个，多则五六个，从售楼商铺到装修设计，从家居建材到小额贷款，电话那头不但能准确地说出小朱的姓名，甚至连其购买的楼盘房号也一清二楚。忍无可忍的小朱向警方报案，警方展开调查后发现在诸暨某宾馆两个房间内有大量号码频繁拨打电话。

经搜查，房间里竟然是某家居公司雇来的十几个人拿着厚厚的电话材料逐一拨打电话进行推销。同时，警察在现场扣押的 u 盘中发现 85 个文档，每一个文档就是诸暨一个小区的业主信息，共计包含公民个人信息 2 万余条!

通过审查发现，泄露这些信息的“上家”是装饰公司的设计师骆某，其在工作之余还做着倒卖楼盘信息的小生意。而骆某获取房产信息的“上家”有两个：一个是诸暨某房产公司的内勤财务处，另一个则是某房产公司前员工杨某处。杨某曾经是一家房产公司的员工，离职后自己开了中介公司，从前同事、公司数据员陈某手上免费拿到了大量公民个人信息。经统计，陈某共计提供公民个人信息 8 万余条!陈某、杨某、骆某三人因犯侵犯公民个人信息罪，均被判处有期徒刑三年，缓刑四年，并处罚金 1 万元。（来源：浙江新闻）

➢ 缤客网订酒店被退单 信用卡遭多个国家国际盗刷

2019 年 5 月 30 日，赵女士在缤客网上订酒店，遭遇酒店退单之后，没有索回应退款项，且此后信用卡遭遇多个国家的国际盗刷。对此，缤客网公关回应称，接到投诉后，正在帮助游客赵女士处理此事。Booking 是总部位于荷兰的住宿预订平台，在国内被网友称作“缤客”。住在西安的赵女士说，她从 2014 年起就开始在缤客网上预订酒店。

并未输入密码信用卡却立即扣款

2019 年 3 月 23 日，赵女士准备出国旅游，于是通过缤客网(Booking 网)预订了 2019 年 7 月 23 日到 7 月 27 日位于法国巴黎一家酒店的住宿，共计 316 欧元。“在向缤客网提供了银行卡卡号、姓名、CVV 码等相关信息之后，3 月 23 日，我的信用卡被扣款 2756 元(到店前付款一部分，到店后支付剩余费用)。”赵女士说，一般酒店都是到店付款，但是自己的信用卡却立即扣款，而且自己并未输入密码。“因为我是真实入住酒店，早晚都要付款，所以对于提前扣款，我并没有太追究。”

收到“取消”邮件后信用卡被盗刷十余笔

没想到的是，4 月 26 日赵女士收到一封邮件。“缤客网给我发邮件说酒店方在我的预订期内无法提供服务，对此深表遗憾，并代表住宿方为我免费取消了住宿。”赵女士回忆

说，自从收到来自缤客网的取消服务邮件后，她当时在缤客网预订酒店住宿的信用卡莫名其妙被疯狂盗刷十余笔，这些消费分别来自德国、英国、意大利、西班牙、法国等国家。“庆幸我发现还算及时，事发后两天内及时阻止，才没有造成更大的损失。”

订单被取消后，预先支付的酒店房费没有退还，再加上银行卡被盗刷，赵女士联系缤客网的客服进行投诉。“我得到的答案竟然是，要求提供当时的付款信息及银行信息，并让银行出具一份拒绝追款或款项追不回来的证明，缤客网才会帮我处理。”

缤客网回应投诉正在处理之中

缤客网在酒店预订的过程中是不需要提供密码的，输入银行卡信息后，银行卡的相关信息会直接发给酒店，所以最后出现卡被盗刷的现象。赵女士说，她对缤客网目前的处理态度难以接受。“我把钱支付到你的账号里，现在酒店退单，理应先把我的钱退还给我。”

对于赵女士所说的情况，5 月 28 日下午，缤客网的公关人员回应称，对于订酒店的退款以及银行卡被人盗刷一事，接到赵女士的反馈之后，已经由缤客网负责客户服务的相关工作人员跟进处理此事，后续如有进展，会第一时间进行反馈。

记者调查：国际上很多消费只需要 CVV 码即可完成扣款

对于网上订房，仅仅关于缤客网的，在网络上就有大量网友发帖，讲述自己银行卡被盗刷的案例。甚至有网友撰写了“防范 booking 订房信用卡被盗刷的几点心得”，让其他网友降低被盗刷银行卡的风险。

记者查询了解到，CVV 即 Card Verification Value，又称“后三码”，是由卡号、有效期和服务约束代码生成的 3 位或 4 位数字，一般写在银行卡(信用卡)卡片磁条的 2 磁道用户(信用卡背后)自定义数据区里面。CVV 信息被存储在磁条银行卡的磁道中，根据卡号、磁道主账号、发卡银行标志代码等信息，通过各银行自定义的特殊加密算法进行加密，每步都采用 CVKA 技术加密，得到验证码。

一家银行的客服人员告诉记者，在国际上根据商家不同，有的需要提供密码，有的只需要银行卡号和 CVV 码就可完成支付，不需要提供密码。

CVV 算是信用卡的“第二密码”。在使用信用卡时，有两种交易方式，一个是“过卡交易”，另一个是“离线交易”。 特别需要注意的是“离线交易”，因为这种方式可以在持卡人预订酒店、机票，或者网上支付时，只提供信用卡账号和 CVV 码，不需要密码就能完成支付。现在一些不法分子就利用这一点，在获得持卡人信用卡号、后三码后，在国外网站疯狂网购。赵女士表示，如果在缤客网的投诉没有得到合理解决，她只能使用法律手段维权，现在正在联系相关律师。（来源：北京青年报）

信息安全意识产品免费大赠送

isa@spisec.com