国盟信息安全通报

2019 年 9 月 02 日第 200 期

国盟信息安全通报

（第 200 期）

国际信息安全学习联盟

2019 年 9 月 02 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 383 个，其中高危漏洞 104 个、中危漏洞 264 个、低危漏洞 15 个。漏洞平均分值为 5.93。本周收录的漏洞中，涉及 0day 漏洞 89 个（占 23%），其中互联网上出现“Bento4 越界读取漏洞、Bento4 空指针解引用漏洞（CNVD-2019-28477）”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 1865 个，与上周（1469 个）环比增长 27%。

主要内容

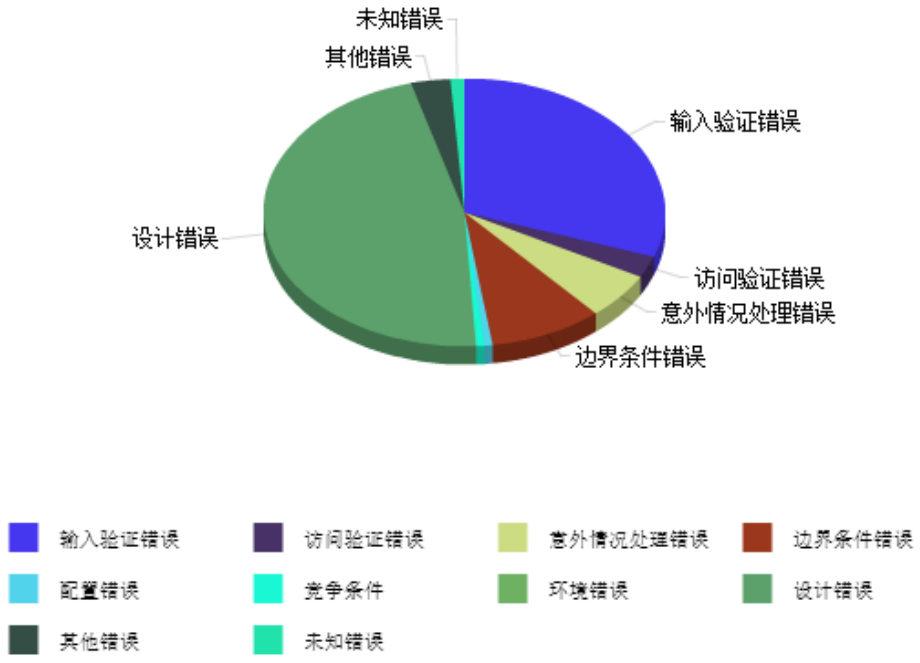
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

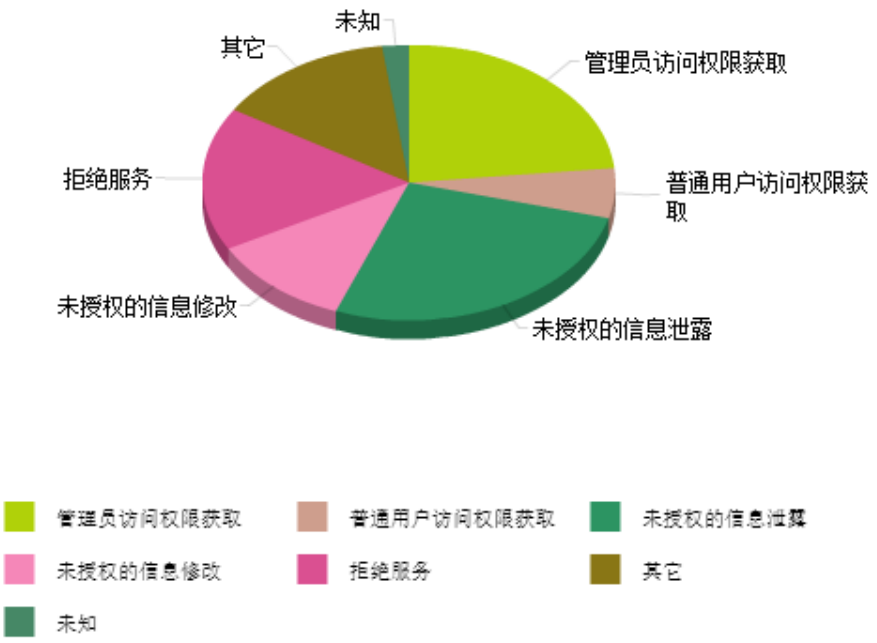
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 383 个，其中高危漏洞 104 个、中危漏洞 264 个、低危漏洞 15 个。漏洞平均分值为 5.93。本周收录的漏洞中，涉及 0day 漏洞 89 个（占 23%），其中互联网上出现“Bento4 越界读取漏洞、Bento4 空指针解引用漏洞（CNVD-2019-28477）”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 1865 个，与上周（1469 个）环比增长 27%。

二、安全漏洞增长数量及种类分布情况

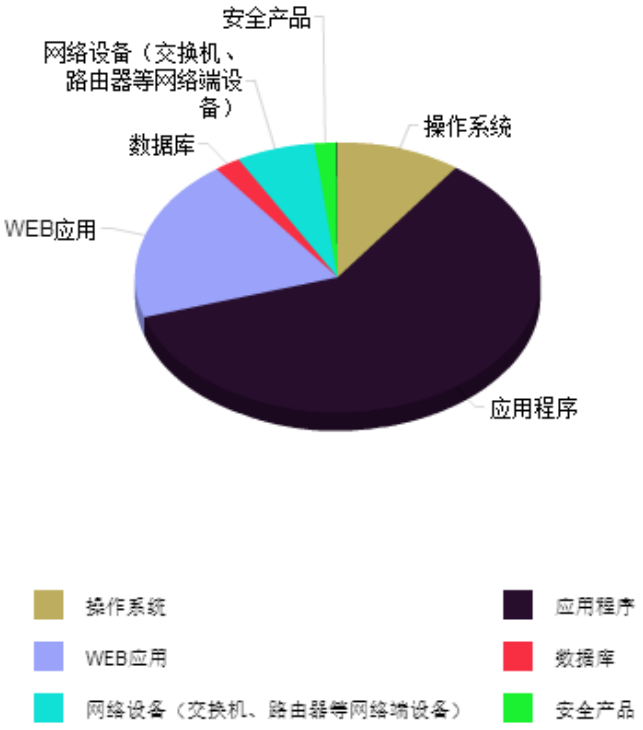
➢ 漏洞产生原因（2019 年 8 月 19 日—2019 年 9 月 02）



➢ 漏洞引发的威胁（2019 年 8 月 19 日—2019 年 9 月 02）



➢ 漏洞影响对象类型（2019 年 8 月 19 日—2019 年 9 月 02）



三、安全产业动态

➢ 刘烈宏：新时代的网络安全工作重点从五个方面着手

2019 年 8 月 25 日，随着网络信息技术的持续演进，互联网对整个经济社会发展的渗透、驱动作用越来越明显，带来的风险挑战也在不断扩大。“中央网信办副主任、国家网信办副主任刘烈宏在今日下午举行的国新办发布会上表示，网络安全威胁和风险日益增多，地下黑产、电信网络诈骗等各类违法犯罪活动时有发生，数据安全和侵犯个人隐私问题日益凸显。”

刘烈宏强调，针对关键信息基础设施的有组织高强度网络攻击愈加明显，特别是网络空间与现实世界安全问题不断交织，网络安全问题向现实世界传导，现实世界的安全问题也不断向网络空间蔓延，网络安全问题日益成为影响国家安全、社会稳定和人民群众切身利益的重大战略问题。

没有网络安全就没有国家安全。刘烈宏指出，做好新时代的网络安全工作，重点做好以下几方面的工作：

一是加强数据安全管理和个人信息保护。加快出台数据安全管理办法、个人信息出境安全评估办法等相关法规制度和标准规范。深入开展 APP 违法违规收集使用个人信息专项治理，依法严厉打击针对和利用国家大数据资源和个人信息的违法犯罪活动。

二是强化关键信息基础设施的保护。加快出台关键信息基础设施安全保护条例，落实运

营单位主体责任和保护部门的监管责任，统筹开展网络安全检查，强化网络安全态势感知，监测预警和应急处置能力建设。

三是培育扶持网络安全技术产业做大做强。我们正在加强网络安全技术产业的规划和整体布局，完善支持网络安全技术产业发展的政策措施，培育一批具有国际竞争力的网络安全企业。

四是持之以恒抓好网络安全人才培养。加强网络空间安全学科专业建设，实施好一流网络安全学院建设示范项目，加快建设国家网络安全人才与创新基地，形成人才培养、技术创新、产业发展的良好生态。

五是积极推动网络空间国际治理。在全球互联网治理体系变革“四项原则”、构建网络空间命运共同体“五点主张”指引下，深化与各国和相关国际组织的务实合作，深入开展网络安全的对话互动，共同应对网络安全的威胁与挑战，携手构建网络空间命运共同体。（来源：人民日报）

➢ 侵犯个人信息的刑事法律责任综述：量刑标准与案例分析

随着信息社会的到来，特别是大数据的迅猛发展，个人信息的性质与意义均发生了巨大变化，具有以前任何时代所不能具备的价值。侵犯公民个人信息的行为也因此愈演愈烈。无论是出于经济目的还是其他非法目的，非法获取、非法提供和非法利用个人信息的行为层出不穷，危害巨大。对此，《刑法》也在不断新增和完善打击侵犯公民个人信息犯罪的条款。

2009 年，全国人大常委会通过《刑法修正案（七）》，在《刑法》253 条之一增设了出售、非法提供公民个人信息罪和非法获取公民个人信息罪。2015 年《刑法修正案（九）》，将“出售、非法提供公民个人信息罪”“非法获取公民个人信息罪”调整为“侵犯公民个人信息罪”，同时对于特殊主体予以加重处罚，明确了单位构成该罪应并罚，并提高了刑罚处罚区间。2017 年 3 月，最高人民法院、最高人民检察院发布的《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》（以下简称“《解释》”）明确了公民信息和情节严重的认定标准，此外，《解释》还协调了侵犯公民个人信息罪与非法利用信息网络罪、拒不履行信息网络安全管理义务罪等关联罪名的关系，这些修改及时适应了该类犯罪的发展变化趋势，有利于实现《刑法》对个人信息的全面、有效保护。

而在司法实践中，侵犯公民个人信息罪的案件数量也呈逐年递增趋势。根据公开渠道检索得知，在 2015 年《刑法修正案(九)》颁布之后，案由为侵犯公民个人信息罪的案件共有 2286 起，其中 2018 年全年共审理 1129 件。而截至 2019 年 8 月，2019 年也已审理 333 起。

侵犯公民个人信息罪要求“情节严重或特别严重”

根据《刑法修正案(九)》的最新规定，侵犯公民个人信息罪是指以窃取或者其他方法非法获取公民个人信息，出售或者非法提供公民个人信息，情节严重的行为。根据刑法规定，犯本罪的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金；罚金数额一般在违法所得的一倍以上五倍以下。

值得注意的是，侵犯公民个人信息罪作为情节犯，有明确的情节严重程度的要求，区分为两档“情节严重”与“情节特别严重”，并规定了不同的刑罚。《解释》第五条、第六条以列举的方式规定了“情节严重”及“情节特别严重”的情形。第一，在认罪标准上根据个人信息性质和内容的不同，分别以“五十条以上”“五百条以上”“五千条以上”和“按相应比例合计达到有关数量标准的”为“情节严重”；第二，“将在履行职责或者提供服务过程中获得的公民个人信息出售或者提供给他人”达到前述标准一半以上的为“情节严重”；第三，数量达到前两项标准十倍以上的为“情节特别严重”（具体情形见文末表格）。以上标准的出台，对于指导侵犯公民个人信息罪的司法适用具有重要的作用。

此外，《刑法修正案(九)》还专门针对“将在履行职责或者提供服务中获得的公民个人信息出售或者提供给他人”做了从重处罚的规定。根据《刑法》第二百五十三条之一第二款规定，违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者

提供给他人的，应从重处罚。如前所述，将履行职责过程或提供服务过程中获得的公民个人信息出售，数量达到一般主体立案追诉标准一半以上的，便达到“情节严重”的要求，依法追究刑事责任。例如，在籍栋良、李志强侵犯公民个人信息案（2017）[1]中，被告人籍栋良利用在派出所工作的职务之便，使用前所长的数字证书查询公安系统内公民个人信息 3670 余条，并通过微信出售公民个人信息非法获利。

侵犯公民个人信息罪“情节严重”与“情节特别严重”具体情形一览表[7]

序号	情节严重情形		情节特别严重情形[8]
1	非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息五十条以上的		造成被害人死亡、重伤、精神失常或者被绑架等严重后果的
2	非法获取、出售或者提供住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息五百条以上的		造成重大经济损失或者恶劣社会影响的
3	出售或者提供行踪轨迹信息，被他人用于犯罪的	为合法经营活动而非法购买、收受公民个人信息，具有下列情形之一的： （一）利用非法购买、收受的公民个人信息获利五万元以上的； （二）曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚，又非法购买、收受公民个人信息的； （三）其他情节严重的情形。	数量或者数额达到情节严重情形第 1 项、第 2 项、第 5 项至第 8 项规定标准十倍以上的
4	知道或者应当知道他人利用公民个人信息实施犯罪，向其出售或者提供的		其他情节特别严重的情形
5	非法获取、出售或者提供第 1 项、第 2 项规定以外的公民个人信息五千条以上的		——
6	数量未达到第 1 项、第 2 项、第 5 项规定标准，但是按相应比例合计达到有关数量标准的		
7	违法所得五千元以上的		
8	将在履行职责或者提供服务过程中获得的公民个人信息出售或者提供给他人，数量或者数额达到第 1 项、第 2 项、第 5 项至第 7 项规定标准一半以上的		
9	曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚，又非法获取、出售或者提供公民个人信息的		
10	其他情节严重的情形		

[7]根据《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》法释〔2017〕10 号第五条及第六条进行整理。

[8]实施非法获取、出售或者提供公民个人信息行为，且具有以下情节之一的，认定为“情节特别严重”。

单位侵犯公民个人信息：单位及直接责任人员均须担责

为切实加大对单位侵犯公民个人信息犯罪的惩治力度，《刑法》第二百五十三条之一第四款规定，单位实施侵犯公民个人信息犯罪的，依法追究单位和相关责任人员的刑事责任。对于单位，可以处以罚金。而对于直接负责的主管人员和其他直接责任人员视具体情节，判处有期徒刑或者拘役，并处或单处罚金。例如在南京乔治尼亚家居有限公司、梁某等人侵犯公民个人信息罪一案（2018）[2]中，南京乔治尼亚家居有限公司采用购买公民个人信息后进行电话推销等经营模式，销售该公司家具产品。梁某作为该公司法定代表人安排市场部人员从家装建材、楼盘销售从业人员处非法购买大量公民个人信息名单，后进行电话推销。法院经查明，判处单位罚金，判处梁某及直接责任人员有期徒刑并处罚金。

尽管从法条的字面规定来看，单位构成侵犯公民个人信息犯罪，单位仅会受到罚金的处罚。但是实践中，一旦企业被认定为构成单位犯罪，遭受的绝非仅是罚金损失，而是可能丧失一些领域的投标资质和市场准入的条件，直接影响到业绩指标考核，股价表现。而且侵犯公民个人信息行为往往是舆论媒体和社会大众关注的新闻焦点，若被以侵犯公民个人信息为由提起刑事诉讼，无论最终判决结果如何，都将对企业自身的社会形象造成难以挽回的影响。

侵犯公民个人信息可能触犯的其他罪名

首先，以设立钓鱼网站等方式，非法利用信息网络以获取公民个人信息的，属于牵连犯，以侵犯公民个人信息罪定罪处罚。根据《解释》第八条规定，设立用于实施非法获取、出售或者提供公民个人信息违法犯罪活动的网站、通讯群组，情节严重的，应以非法利用信息网络罪定罪处罚；同时构成侵犯公民个人信息罪的，依照侵犯公民个人信息罪定罪处罚。例如在查正中、王卫海帮助信息网络犯案（2017）[3]中，被告设立用于非法获取公民个人信息的钓鱼网站，并将钓鱼网站存放在其租赁远程服务器上，后出租给他人用于实施网络犯罪活动，从中非法谋利。法院经审理认定被告同时触犯了非法利用信息网络罪和侵犯公民个人信息罪，并援引《解释》第八条的规定，最终以侵犯公民个人信息罪定罪处罚。

其次，在大数据的时代背景下，公民的个人信息常以电子数据形式存储于计算机信息系统中，而不少案例中行为人通过黑客手段入侵计算机信息系统获取公民个人信息。针对这一行为，目前司法实践中主流做法是认定行为人构成非法获取计算机信息系统数据罪与侵犯公民个人信息罪的想象竞合犯，从一重罪处罚。例如，在王东兴、李朝丹非法获取计算机信息

系统数据、非法控制计算机信息系统案（2018）[4]中，二审法院认为上诉人通过破解、修复的软件侵入快递公司计算机信息系统下载等方式非法获取并向他人出售公民个人信息的行为，既构成侵犯公民个人信息罪，又构成非法获取计算机信息系统数据罪。一审法院择一重罪即按侵犯公民个人信息罪处罚，符合法律规定，故驳回上诉。

再次，大量非法获取公民个人信息并诈骗应数罪并罚。2013 年最高院、最高检与公安部联合发布的《关于依法惩处侵害公民个人信息犯罪活动的通知》明确规定，对使用非法获取的个人信息实施其他犯罪行为，构成数罪的，应当依法予以并罚。例如杨某、黄某犯侵犯公民个人信息案（2016）[5]中，法院认定被告人非法获取公民个人信息后拨打相应手机号码骗取被害人财物的行为，虽然存在手段行为和目的行为的关系，但不具有密切关联性，不成立牵连犯，又缺乏法律明文规定按一罪论处，应当实行数罪并罚，故最终判决被告同时构成非法获取公民个人信息罪和诈骗罪。

最后，根据《解释》第九条规定，网络服务提供者拒不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，致使用户的公民个人信息泄露，造成严重后果的，应以拒不履行信息网络安全管理义务罪定罪处罚。但通过公开渠道检索案例，以拒不履行信息网络安全管理义务罪定罪处罚的仅有一起，即胡某拒不履行信息网络安全管理义务案（2018）[6]，被告人胡某为非法牟利，租用国内、国外服务器，自行制作并出租“土行孙”、“四十二”翻墙软件，为境内 2000 余名网络用户非法提供境外互联网接入服务。但法院判决中并未说明是否造成用户个人信息泄露。因此，目前该条规定还没有相

关司法实践。（来源：个人信息与数据保护实务）

➢ 报告显示：我国网民规模 8.54 亿 互联网普及率 61.2%

2019 年 8 月 30 日，中国互联网络信息中心（CNNIC）在京发布第 44 次《中国互联网络发展状况统计报告》（以下简称:《报告》）。《报告》从互联网基础建设、网民规模及结构、互联网应用发展、互联网政务应用发展和互联网安全等多个方面展示了 2019 年上半年我国互联网发展状况。

党的十九大以来，在以习近平同志为核心的党中央坚强领导下，各地区、各部门深入贯彻落实全国网络安全和信息化工作会议精神，网络强国建设整体推进，网络安全保障能力稳步提升，互联网在经济社会发展中的重要作用更加凸显。2019 年上半年，中国互联网发展呈现出六个特点。

一、IPv6 地址数量全球第一，“.CN”域名数量持续增长。

截至 2019 年 6 月，我国 IPv6 地址数量为 50286 块/32，较 2018 年底增长 14.3%，已跃居全球第一位。我国 IPv6 规模部署不断加速，IPv6 活跃用户数达 1.3 亿，基础电信企业已分配 IPv6 地址用户数 12.07 亿；域名总数为 4800 万个，其中“.CN”域名总数为 2185 万个，

较 2018 年底增长 2.9%，占我国域名总数的 45.5%。2019 年 6 月，首届“中国互联网基础资源大会 2019”在京召开，大会围绕网络强国战略大局，回顾中国互联网二十五周年发展历程，聚焦互联网基础资源行业发展，展示前沿创新技术，搭建行业交流平台，推动行业规范有序发展。

二、互联网普及率超过六成，移动互联网使用持续深化。

截至 2019 年 6 月，我国网民规模达 8.54 亿，较 2018 年底增长 2598 万，互联网普及率达 61.2%，较 2018 年底提升 1.6 个百分点；我国手机网民规模达 8.47 亿，较 2018 年底增长 2984 万，网民使用手机上网的比例达 99.1%，较 2018 年底提升 0.5 个百分点。与五年前相比，移动宽带平均下载速率提升约 6 倍，手机上网流量资费水平降幅超 90%。“提速降费”推动移动互联网流量大幅增长，用户月均使用移动流量达 7.2GB，为全球平均水平的 1.2 倍；移动互联网接入流量消费达 553.9 亿 GB，同比增长 107.3%。

三、下沉市场释放消费动能，跨境电商等领域持续发展。

截至 2019 年 6 月，我国网络购物用户规模达 6.39 亿，较 2018 年底增长 2871 万，占网民整体的 74.8%。网络购物市场保持较快发展，下沉市场、跨境电商、模式创新为网络购物市场提供了新的增长动能：在地域方面，以中小城市及农村地区为代表的下沉市场拓展了网络消费增长空间，电商平台加速渠道下沉；在业态方面，跨境电商零售进口额持续增长，利好政策进一步推动行业发展；在模式方面，直播带货、工厂电商、社区零售等新模式蓬勃发展，成为网络消费增长新亮点。

四、网络视频运营更加专业，娱乐内容生态逐步构建。

截至 2019 年 6 月，我国网络视频用户规模达 7.59 亿，较 2018 年底增长 3391 万，占网民整体的 88.8%。各大视频平台进一步细分内容品类，并对其进行专业化生产和运营，行业的娱乐内容生态逐渐形成；各平台以电视剧、电影、综艺、动漫等核心产品类型为基础，不断向游戏、电竞、音乐等新兴产品类型拓展，以 IP（Intellectual Property，知识产权）为中心，通过整合平台内外资源实现联动，形成视频内容与音乐、文学、游戏、电商等领域协同的娱乐内容生态。

五、在线教育应用稳中有进，弥补乡村教育短板。

截至 2019 年 6 月，我国在线教育用户规模达 2.32 亿，较 2018 年底增长 3122 万，占网民整体的 27.2%。2019 年《政府工作报告》明确提出发展“互联网+教育”，促进优质资源共享。随着在线教育的发展，部分乡村地区视频会议室、直播录像室、多媒体教室等硬件设施不断完善，名校名师课堂下乡、家长课堂等形式逐渐普及，为乡村教育发展提供了新的解决

方案。通过互联网手段弥补乡村教育短板，为偏远地区青少年通过教育改变命运提供了可能，为我国各地区教育均衡发展提供了条件。

六、在线政务普及率近六成，服务水平持续向好。

截至 2019 年 6 月，我国在线政务服务用户规模达 5.09 亿，占网民整体的 59.6%。在政务公开方面，2019 年上半年，各级政府着力提升政务公开质量，深化重点领域信息公开；在政务新媒体发展方面，我国 297 个地级行政区政府已开通了“两微一端”等新媒体传播渠道，总体覆盖率达 88.9%；在一体化在线政务服务平台建设方面，各级政府加快办事大厅线上线下融合发展，“一网通办”“一站对外”等逐步实现；在新技术应用方面，各级政府以数据开放为支撑、新技术应用为手段，服务模式不断创新；在县级融媒体发展方面，各级政府坚持移动化、智能化、服务化的建设原则，积极开展县级融媒体中心建设工作，成效初显。（来源：中国网信网）

- **第 44 次中国互联网络发展状况统计报告**
- **全文：**http://www.cac.gov.cn/2019-08/30/c_1124938750.htm

➢ 关于人工智能安全问题政策应对的思考

在科技发展史上，技术的进步和变革都会带来“双刃剑”效应。从人工智能概念的提出，到人工智能应用的落地，已经影响到社会发展的诸多方面，而人工智能技术本身的安全问题和与此相关的安全威胁，同样不容忽视。在各国出台国家战略、政策法规、制度措施等助力人工智能发展的同时，人工智能的安全、风险、法律与伦理等问题，值得关注。

一、人工智能面临的安全挑战

人类智能的模拟延伸以及结果的不确定性，决定了人工智能的安全问题不容忽视。不同领域对其的理解和着眼点不同，综合来看，大致可以将人工智能的安全问题按照诱因分为两类：一类是人工智能技术客观因素导致的安全问题，另一类则是人为主观因素导致的安全问题。

因人工智能技术客观原因导致的安全问题主要源于三点：一是源于 AI 技术的不成熟，例如，Uber 无人车决策失误撞死行人；二是源于 AI 技术的不确定性，例如，算法“黑箱”缺乏透明度和可解释性；三是源于 AI 新技术引发的社会变革，例如，AI 对人类就业的冲击以及对伦理、法律制度的挑战。技术客观原因产生的安全问题并非当下弱人工智能时代 AI

安全问题真正的痛点，因为当 AI 技术没有按照预期轨道和人们要求发展时，人类可以直接进行人为的干预和控制。

从当下暴露出来、难以治理的人工智能安全问题看，大部分还是由人为主观因素导致的。尤其当 AI 技术被不法分子所利用，AI 就可以替代、辅助不法分子实施不法行为，谋取暴利。此时的 AI 即可以被用来进行网络系统攻击，窃取重要数据和个人信息，控制各类系统；也可以被用来进行 AI 换脸、AI 洗稿等谋取不正当利益。即使不法分子没有利用 AI 技术，他们也还可以通过注入大量“有毒”数据进行数据投毒，利用现在人工智能系统对数据极大的依赖性，干扰甚至控制 AI 最后决策。

人工智能本身带来的安全挑战并不可怕，可怕的是人心难测，当人工智能这一技术出现时，在人们面临科技带来的巨大便利时，人类能否守住正义的底线，不被利益冲昏头脑，才是当下人工智能安全所要面临的最大挑战。

二、各国政策对人工智能安全问题的关注点

受各国人工智能产业现状及背后基本国情的影响，不同国家对人工智能安全领域相关政策的关注点也不尽相同。

作为人工智能技术最发达的国家之一，美国相关政策体系的构建比较丰富，不仅从战略、法律到原则倡议、标准制定进行了由上到下的规范，对于自动驾驶、算法等具体的应用场景和技术也进行了规范。从目前美国已经颁布的政策法规看，美国政府从战略层面对人工智能的关注点已经从 2016 年《国家人工智能研究和发展战略计划》(National Artificial Intelligence Research and Development Strategic Plan)中的“确保安全”向 2019 年《人工智能倡议》

（American AI Initiative）“提升国际竞争力、确保美国领先地位”的国际博弈转变，尤其是《2018 年国防部人工智能战略摘要 利用人工智能促进安全与繁荣》（Summary of The 2018 Department of Defense Artificial Intelligence Strategy Harnessing AI to Advance Our Security and Prosperity）这一政策，充分体现了美国对人工智能技术在国家安全事业的应用给予重点关注。对于人工智能的安全问题则更多聚焦在具体应用场景和技术的规定当中，如《2019 算法问责案》（Algorithmic Accountability Act of 2019）和《自动驾驶法案》（Self Drive Act）等。

对欧盟而言，如何继续保持在新兴产业领域的话语权成为其重点关注的内容。在欧盟委员会发布的《欧盟人工智能》（Artificial Intelligence for Europe）战略规划中，明确指出要确保欧盟具有与人工智能发展和应用相适应的伦理和法律框架，最大化欧盟整体在人工智能领域的国际竞争力。另外，从欧盟目前颁布的政策法规来看，尽管欧盟在人工智能产业领域存在缺失，但是，仍然通过制度创新以及对安全问题的细致规定抢占政策主导地位。

日本、韩国、新加坡等亚洲国家，更多是将人工智能安全的战略重点放在促进产业健康发展以及公共安全、国家安全的应用上，并对人工智能的一些安全问题、伦理问题做出原则性规定。日本于 2017 年发布的《人工智能技术战略》（Artificial Intelligence Technology Strategy）、韩国于 2018 年发布的《人工智能研发战略》（Artificial Intelligence R&D Strategy）以及新加坡于 2019 年发布的《人工智能治理框架》（Artificial Intelligence Governance Framework）等，均有所体现。

大部分国家对人工智能安全领域的关注点基本都在于如何促进产业发展以及如何利用人工智能保障国家、公共安全，提高竞争力方面；关于人工智能安全问题的规定也大多停留在原则、倡议层面；对具体的应用场景和技术的安全规定也仅限在自动驾驶、算法以及智能机器人等领域。总而言之，各国在人工智能安全问题的政策制定上还处于探索阶段，所制定的政策法规也带有浓厚的国家色彩和战略考量。如何在安全可控的基础上利用人工智能在国际舞台上占据有利地位，已成为每个国家必做的功课。

三、关于如何进行政策应对的思考

从各国对人工智能安全问题的政策关注点看，关于人工智能安全问题的政策治理，已经上升到国际竞争层面：一方面，人工智能相关技术的应用是现在及未来国际竞争必争的战略高地；另一方面，人工智能在国防等国家安全层面的作用也是将来国际博弈的重要筹码。因此，有关人工智能安全问题的政策应对并非单纯的政策制定那么简单，需要从全局出发，慎重考量。

首先，要加强在国际领域的话语权，保护中国人工智能企业在全球的产业发展。在加强

政策国际话语权方面，欧盟一直都做得非常出色。最典型的例子就是 2018 年正式生效的《通用数据保护条例》（GDPR），可谓在全球掀起数据保护“狂潮”，不仅众多国家纷纷出台了自己的数据保护法案，对数据保护的严格要求也对全球企业产生了影响，尤其对美国的大型互联网跨国公司产生重击。欧盟在人工智能方面也采取了同样的策略。对中国而言，继续保持人工智能在全球的优势地位，政策是必不可少的一环，如何在政策领域主动先发制人而非被动的受他国挟制，需要依靠国家力量，引领提升产业国际影响力。

其次，对人工智能的安全问题要理性对待，分而治之：对因技术客观因素导致的安全问题要适度宽容；对因人为主观因素导致的安全问题要坚决抵制。之所以要对因技术客观因素导致的安全问题适度宽容，是因为但凡一个新事物的产生都不是绝对安全可靠的，人工智能也不例外。新技术的产生既会带来机遇，也会带来风险，尤其是对人工智能这一数字时代被重新激活生命的“新生儿”。对于技术还不够成熟的人工智能技术和应用，可以像对待“未成年人”一样对待并保护它，给它安排“监护人”，监护它的“行为”并承担责任；对于一些重大的“刑事”问题给予适当的宽容。至于那些因人为主观因素导致的诸如利用人工智能系统攻击、数据窃取等安全问题，在人工智能并未出现之时就已存在，只是人工智能的出现加剧了危害后果，根本问题还是人的问题。对于这类问题和行为，政策上亟需坚决抵制，而且抵制的重点需放在人的不正当行为而非人工智能技术上。一方面，技术是在不断变革和进步的，政策的制定永远赶不上技术的发展，此类安全问题的根本原因在于人的不法行为而非人工智能，治病需治根；另一方面，“甲之砒霜，乙之蜜糖”，人工智能技术也可极大的助力安全事业。

最后，发挥政策相较法律更加灵活的特性，审时度势，保障人工智能安全可控发展。在符合中国国情和产业发展规律的基础上，守住人工智能发展的原则底线，在安全与发展的平衡点间左右调节。当人工智能产业还不够成熟时，对人工智能产生的安全问题的政策引导要大于政策限制；当人工智能产能过剩时，转而依靠安全标准的提高促进产业质量的升级。

总而言之，政策的适当与否决定了产业发展的好坏，过松或过严的政策都不利于产业得发展。无论如何，政策的制定都不应当是在办公室里拍脑袋想出的一纸空文，应尽可能多地倾听各方意见虽然会影响政策的制定效率，却一定会使出台的政策更加科学，真正发挥政策的治理作用。（来源:《中国信息安全》杂志 2019 年第 7 期）

四、政府之声

➢ 国家网信办发布《儿童个人信息网络保护规定》10 月 1 日实施

2019 年 8 月 22 日，《儿童个人信息网络保护规定》（以下简称《规定》）公布，自 10 月 1 日起正式施行，针对中华人民共和国境内通过网络收集、存储、使用、转移、披露不满十四周岁的儿童个人信息进行了规范。**《规定》的主要内容包括四个方面：**

一是针对儿童个人信息的全生命周期提出更为严格审慎的规范原则，并落实在具体规则中。明确儿童个人信息的收集、存储、使用、转移行为应当遵循正当必要、知情同意、目的明确、安全保障、依法利用的原则。

二是进一步明确儿童及其监护人针对儿童个人信息享有的各项权能。包括：在收集、使用、转移、披露环节，儿童监护人的知情权、同意权，及上述环节中相关要素发生实质性变更时的再次授权；儿童及其监护人发现儿童个人信息存在误差时的信息更正权；发现网络运营者违法、违规收集、存储、使用、转移、披露，或撤回同意、停止服务时的信息删除权。

三是明确网络运营者针对儿童个人信息的专门性、特设性保护义务。包括：专条、专员——设置专门的儿童个人信息保护规则和用户协议，指定儿童个人信息保护专员；知情同意——提供更加详细、灵活的用户协议（隐私条款）并以显著、清晰的方式告知监护人并征得监护人同意，且发生实质性变化时需再次征得同意；最小存储——存储儿童个人信息不得超

过实现其收集、使用目的所必须的期限，停止运营产品或者服务时应当立即停止收集并删除其持有的儿童个人信息；最小访问——内部工作人员严格按照权限、经过审批访问数据，严控知悉范围、记录访问情况、防止非法获取；泄露及停业通知——儿童个人信息发生泄露、毁损、丢失，造成或者可能造成严重后果的，应当报告主管部门，并逐一告知儿童及其监护人或发布公告，停止服务的应当告知监护人；安全存储——存储儿童个人信息应当采取加密等措施；共享、披露限制——涉及向第三方转移儿童个人信息的，需经安全评估，涉及委托第三方处理儿童个人信息的，签署委托协议，规范双方权利义务。

四是自动例外。即通过计算机信息系统自动留存处理信息且无法识别所留存处理的信息属于儿童个人信息的，不需按照本规定操作。（来源：中国网信网）

- **《儿童个人信息网络保护规定》**
- **全文：**http://www.cac.gov.cn/2019-08/23/c_1124913903.htm

➢ 十部门联合印发《加强工业互联网安全工作的指导意见》（解读）

2019 年 8 月 28 日，工业和信息化部、教育部、人力资源和社会保障部、生态环境部、国家卫生健康委员会、应急管理部、国务院国有资产监督管理委员会、国家市场监督管理总局、国家能源局、国家国防科技工业局联合印发了《加强工业互联网安全工作的指导意见》（工信部联网安〔2019〕168 号）（以下简称《安全指导意见》）。**现就《安全指导意见》有关内容解读如下。**

问：《安全指导意见》出台的背景和意义是什么？

答：党中央国务院高度重视工业互联网发展，习近平总书记明确提出，要深入实施工业互联网创新发展战略。《国务院关于深化“互联网+先进制造业”发展工业互联网的指导意见》将安全保障与网络、平台建设并列为工业互联网三大体系之一。出台实施《安全指导意见》，一是落实党中央国务院工作部署，加快制造强国和网络强国建设，强化工业互联网安全体系化布局；二是有助于提升工业互联网安全保障水平，应对工业互联网发展面临的网络安全新风险、新挑战；三是有利于凝聚各方共识，构建协同推进、各司其责的安全工作体系，形成工业互联网安全保障合力。

为做好《安全指导意见》编制工作，工业和信息化部会同教育部、人力资源和社会保障部、应急管理部、国务院国有资产监督管理委员会、国家能源局等相关部门系统调研相关企

业，广泛征集产业各方意见，厘清工业互联网安全职责界面，明确重点任务。《安全指导意见》出台后，将为地方主管部门和相关企事业单位开展工业互联网安全工作提供依据和指导。

问：《安全指导意见》的总体要求是什么？

答：《安全指导意见》坚持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、三中全会精神，围绕制造强国和网络强国建设，聚焦设备、控制、网络、平台、数据安全，落实企业主体责任、政府监管责任，健全制度机制、建设技术手段、加强公共服务能力、促进产业发展、强化人才培育，构建责任清晰、制度健全、技术先进的工业互联网安全保障体系，全面提升工业互联网创新发展安全保障能力和服务水平。

《安全指导意见》提出了四条基本原则：一是筑牢安全，保障发展。坚持安全与发展并重，确保工业互联网安全和发展同步规划、同步建设、同步运行；二是统筹指导，协同推进。强化统筹协调和系统谋划，推动产学研用各方形成发展合力，打造国家、地方、行业企业协同联动的工作格局；三是分类施策，分级管理。坚持分类分级管理的基本思路，强化重点领域、关键环节的管理和防护，提升企业综合防护水平；四是融合创新，重点突破。创新安全管理机制和技术手段，强化工业互联网安全关键核心技术研究，提升产业供给能力。

问：《安全指导意见》提出的主要目标是什么？

答：《安全指导意见》提出了两个阶段发展目标。到 2020 年底，建立监督检查、信息共享、应急处置等安全管理制度；制定设备、平台、数据等至少 20 项亟需的安全标准；基本建成国家工业互联网安全技术保障平台、基础资源库和安全测试验证环境；在电子信息、航空航天等重点领域形成至少 20 个创新实用的安全产品、解决方案的试点示范，培育若干具有核心竞争力的工业互联网安全企业。到 2025 年，建立起较为完备可靠的工业互联网安全

保障体系。

问：《安全指导意见》提出了哪些重点任务？

答：为全面提升工业互联网创新发展安全保障能力和服务水平，《安全指导意见》提出了 7 个方面 17 项重点任务。

一是推动安全责任落实。企业依法落实主体责任，政府履行监督管理责任，相关行业主管部门开展本行业领域工业互联网安全指导、监管工作。

二是构建安全管理体系。健全监督检查、信息通报、应急处置等安全管理制度，制定工业互联网行业企业分类分级指南，不断完善工业互联网安全标准体系。

三是提升企业安全防护水平。督促相关企业部署针对性防护措施，不断夯实设备和控制、网络、平台等安全。加强对标识解析系统的安全评估，强化平台安全，加强工业 APP 安全管理。

四是强化工业互联网数据安全保护能力。指导企业完善数据安全防护措施，建立工业互联网数据分类分级管理制度，构建工业互联网全产业链数据安全管理体系。

五是建设国家工业互联网安全技术手段。打造国家、省、企业三级协同的安全技术保障平台。建立基础资源库和安全测试验证环境，提升识别隐患、抵御威胁、化解风险的能力。

六是加强工业互联网安全公共服务能力。开展安全评估认证，推动测评机构的审核认定。鼓励和支持专业机构、安全企业等提升安全服务水平，增强安全产品及解决方案供给能力。

七是推动科技创新与产业发展。加大技术研发和成果转化支持力度，培育安全企业，开展试点示范，遴选优秀安全解决方案和最佳实践，加强应用推广。

问：《安全指导意见》实施的保障措施是什么？

答：为了保障工业互联网安全有关工作任务有效落实，推动安全工作有序高效开展，《安全指导意见》提出了四个方面的保障措施：一是加强组织领导，强化统筹协调，构建各负其责、紧密结合、运转高效的工作机制，形成合力。二是优化创新环境，加大支持力度，鼓励企业技术创新和技术应用，推动安全产业集聚发展。三是发挥市场作用，汇聚产学研用多方力量，形成市场需求牵引、政府支持推动的发展局面。四是加强宣传教育，提升企业和相关从业人员安全意识，深入推进产教融合、校企合作，加快人才培养。（来源：中华人民共和国工业和信息化部）

- **《关于印发加强工业互联网安全工作的指导意见的通知》全文：**
- http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757020/c7288758/content.html

➢ 科技部等六部门印发《关于促进文化和科技深度融合的指导意见》的通知

2019 年 8 月 28 日，为促进文化和科技深度融合，全面提升文化科技创新能力，转变文化发展方式，推动文化事业和文化产业更好更快发展，更好满足人民精神文化生活新期待，增强人民群众的获得感和幸福感，科技部、中央宣传部、中央网信办、财政部、文化和旅游部、国家广播电视总局共同研究制定了《关于促进文化和科技深度融合的指导意见》，并于近日正式印发。

意见指出，目前，国家对网络强国建设作出总体部署，对数字经济发展提出明确要求，有关互联网发展及数字化、网络化、智能化建设正在积极有序推进。同时要看到，文化和科技深度融合仍面临许多新的挑战，科技对文化建设支撑作用的潜力还没有充分释放，相关部门和地方对文化和科技融合的重要性和紧迫性的认识尚需进一步提高。

意见明确，面向文化建设重大需求，把握文化科技发展趋势，瞄准国际科技前沿，选准主攻方向和突破口，打通文化和科技融合的“最后一公里”，激发各类主体创新活力，创造更多文化和科技融合创新性成果，为高质量文化供给提供强有力的支撑。坚持需求导向、问题导向、统筹融合。

意见提出，到 2025 年，基本形成覆盖重点领域和关键环节的文化和科技融合创新体系，实现文化和科技深度融合。按照国家科技创新基地优化整合总体部署，建成若干目标明确、重点突出、协同攻关的文化科技领域国家科技创新基地，建成 100 家左右特色鲜明、示范性强、管理规范、配套完善的国家文化和科技融合示范基地，200 家左右拥有知名品牌、引领行业发展、竞争力强的文化和科技融合领军企业，使文化和科技融合成为文化高质量发展的重要引擎。

意见还明确了加强文化共性关键技术研发、完善文化科技创新体系建设、加快文化科技成果产业化推广、加强文化大数据体系建设、推动媒体融合向纵深发展、促进内容生产和传播手段现代化、提升文化装备技术水平、强化文化技术标准研制与推广 8 项重点任务。（来源：科技部网站）

- **《关于促进文化和科技深度融合的指导意见》的通知全文**
- http://www.most.gov.cn/mostinfo/xinxifenlei/fgzc/gfxwj/gfxwj2019/201908/t20190826_148424.htm

➢ 水利部印发水利网络安全管理办法（试行）

2019 年 8 月 19 日，为贯彻落实习近平总书记网络强国战略思想，依据《中华人民共和国网络安全法》，水利部网信办组织制定了《水利网络安全管理办法（试行）》（以下简称《办法》），并于近日通过审议印发。水利部部长鄂竟平高度重视《办法》制定工作，多次作出批示指示，提出要抓住用务实手段查找问题这一“关键”和处罚这一“要害”,突出问题导向，围绕“办什么—谁来办—怎么办—办得不好怎么处罚”这条主线制定《办法》。

《办法》包括总则、网络安全规划建设、网络运行安全、监测预警与应急处置、监督考核与责任追究、附则共六章。《办法》指出，水利网络安全遵循“积极利用、科学发展、依法管理、确保安全”的方针，建立及时发现漏洞、及时有效处置漏洞和严格责任追究三套机制，确保水利信息化规划建设同步落实网络安全等级保护制度，明确运行阶段网络安全责任

《办法》围绕查、改、罚等环节，强化利用攻防演练、渗透测试、在线监测等客观、有效方式去发现问题；深入评估、分析问题产生的原因，采取修补漏洞、系统升级、部署防护措施、完善管理制度等措施进行有效处置、整改；明确责任追究主体及原则，细化责令整改、警示约谈、通报批评以及建议行政处分和组织处理等追究方式，将水利网络安全保护对象重要程度与网络安全事件严重程度组合量化追究事项，对造成严重损失及危害的、屡教不改的，从严从重处罚，直至追究行政、法律责任。

《办法》突出问题导向，对于今年水利部攻防演练发现的 41.5%属于信息化项目规划建设阶段没有同步落实网络安全等级保护要求留下的问题，以及 58.5%属于运行阶段管理不到位造成的问题，明确了具有针对性、有效性的解决措施。

同时，《办法》通过“网络安全规划建设”“网络运行安全”两章，明确具体任务、责任单位，建立了信息系统全生命周期安全管控规范，有效解决上述问题，确保《办法》实用、管用。叶建春副部长强调要加大《办法》的执行力度，要求部网信办近期选择部分部直属单位开展网络安全渗透测试，对渗透测试发现的问题，在通报整改的基础上，结合网络安全现场检查，依据《办法》进行责任追究。

《办法》为水利行业网络安全强监管提供准则和依据，是健全水利网络安全保障体系、提升水利网络安全防护能力的重要举措。（来源：水利部官方网站）

五、本期重要漏洞实例

➢ Cisco Integrated Management Controller 命令注入漏洞

发布日期：2019-08-23
更新日期：2019-08-26
受影响系统：
Cisco IMC Software Release < 4.0
Cisco IMC Software Release < 3.0
Cisco IMC Software Release
描述：

CVE(CAN) ID: CVE-2019-1885
Cisco Integrated Management Controller（IMC）是一套用于对 UCS（统一计算系统）进行管理的软件。
Cisco Integrated Management Controller 的 Redfish 协议中存在安全漏洞，可使经身份验证的远程攻击者注入任意命令，从而获取 root 权限。此漏洞源于对用户输入验证不充分。

<*来源：Cisco
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-cmdinjec
*>
建议：

厂商补丁：
Cisco

Cisco 已经为此发布了一个安全公告（cisco-sa-20190821-ucs-cimc）以及相应补丁：
cisco-sa-20190821-ucs-cimc：Cisco Integrated Management Controller Command Injection Vulnerability
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-ucs-cimc

➢ D-Link DIR-823G 命令注入漏洞

发布日期：2019-08-23
更新日期：2019-08-27
受影响系统：
D-Link DIR-823G 1.0.2B05
描述：

CVE(CAN) ID: CVE-2019-15527

D-Link DIR-823G 是一款无线路由器。
D-Link DIR-823G 1.0.2B05 版本固件，HNAP1 存在命令注入漏洞。该漏洞位于 SetWanSettings 的 MaxIdTime 字段。攻击者可利用该漏洞执行安全攻击。

<*来源：vendor
*>

建议：

厂商补丁：
D-Link

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://www.dlink.com/
参考：
https://github.com/TeamSeri0us/pocs/blob/master/iot/dlink/823G-102B05-6.pdf

➢ Adobe Experience Manager 任意代码执行漏洞

发布日期：2019-08-13
更新日期：2019-08-19
受影响系统：
Adobe Experience Manager 6.5
Adobe Experience Manager 6.4
描述：

CVE(CAN) ID: CVE-2019-7964
Adobe Experience Manager（AEM）是一套可用于构建网站、移动应用程序和表单的内容管理解决方案。
Adobe Experience Manager 6.4 版本、6.5 版本在实现中存在身份验证绕过漏洞。攻击者可利用该漏洞导致远程代码执行。此漏洞仅影响使用 SAML 的 AEM。

<*来源：zb3 Robert Lowery
链接：https://helpx.adobe.com/security/products/experience-manager/apsb19-42.html
*>

建议：

厂商补丁：
Adobe

Adobe 已经为此发布了一个安全公告（APSB19-42）以及相应补丁:
APSB19-42：Security updates available for Adobe Experience Manager | APSB19-42
链接：https://helpx.adobe.com/security/products/experience-manager/apsb19-42.html

➢ IBM Cloud Automation Manager 安全漏洞

发布日期：2019-08-27
更新日期：2019-08-29
受影响系统：
IBM Cloud Automation Manager 3.1.2
描述：

CVE(CAN) ID: CVE-2019-4133
IBM Cloud Automation Manager 是 IBM Cloud Private 中的云管理解决方案，用于在多个云环境中部署云基础结构。
IBM Cloud Automation Manager 3.1.2 版本存在不安全的 Content-Security-Policy 标头漏洞，可使客户端用户运行自定义脚本。

<*来源：vendor
链接：http://www.ibm.com/support/docview.wss?uid=ibm10967359
*>

建议：

厂商补丁：
IBM

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.ibm.com/support/knowledgecenter/en/SS2L37_3.2.0.0/cam_upgrade_cam.html

六、本期网络安全事件

➢ 德国万事达信用卡信息泄露 近 9 万名用户受影响

2019 年 8 月 22 日，据欧联网援引欧联通讯社报道，近日，德国有近 9 万个万事达（Mastercard）信用卡用户的信息，一度出现在网络上。万事达公司对此已经做出反应。

据报道，德国一个网络论坛 19 日出现任何人都能打开的 Excel 表格，上面列出近 9 万名德国万事达信用卡用户的信息。

这些所泄露的资料全部都是来自参与了万事达信用卡奖励计划“Princeless Specials”用户的信息，其中包括姓名、邮箱地址、信用卡号码的前两位数及最后四位数，有的还包括用户住址和手机号码。此后网站迅速移除了表格，并提醒获得表格的论坛用户不要外传。

万事达公司随后宣布，暂时关闭对德国开放不到两年的“Princeless Specials”平台，并表示，公司对待个人隐私非常严肃，会全面调查泄密原因。万事达还强调，该事件与平台的支付系统没有关系。

报道称，从表格抽样核对的信息显示，所涉及的泄密资料是真实的，不过表格中也出现了一些重名现象。

万事达公司表示，如果客户想知道自己的电子邮箱是否被盗，可以通过公司公布的网站查询。若发现自己的邮箱地址被盗用，应该马上更改密码。（来源：欧联通讯社）

➢ 江苏丹阳半马报名首日遭黑客入侵 运营方：已报警

2019 年 8 月 23 日，江苏镇江丹阳市半程马拉松比赛报名通道正式开通。随后，有网友在丹阳当地论坛爆料称，自己在联系组委会公开邮箱进行咨询时，却被提醒“**所属域名不存在，邮件无法送达**”。对此，23 日当天，丹阳文体广电和旅游局通过该论坛进行回复称：“经查，有人入侵网站篡改规程信息，现已报警处理。”

2019 年 8 月 27 日，记者从赛事组委会了解到，网站被黑一事属实，具体报警及后续处理均由报名网站具体运营方负责。赛事运营单位相关负责人介绍，网站被黑出现在 23 日报名通道开放前时，“大概是报名前一两个小时，比赛规程信息被人篡改，但 8、9 点正式开放报名通道时，已经恢复正常”。他表示，公司目前已经加大了对报名网站的管理、保护，后续报名工作一切顺利，已成功报名 4000 余人。据该负责人介绍，目前警方对于网站被黑的调查尚无结果，组委会主要精力也都放在做好防范方面。（来源：北京青年报）

➢ 乌克兰核电站员工因偷核电进行数字货币挖矿被捕

2019 年 8 月 21 日，乌克兰安全局(SBU)，因在核电站现场发现了数字货币采矿设备，而发起逮捕行动。据报道，有数字货币矿工通过部署挖矿设备在核电站，而与互联网进行外联挖矿，导致破坏了核设施的安全，并最终泄露了核电站物理保护系统的机密信息。而数字货

币开采可能涉及乌克兰国民警卫队守卫核电站的员工。

2019 年 7 月 10 日，由于在南乌克兰核电厂 SE NAE Energoatom 的一个单独单位的中央控制面板行政大楼 104 号办公室进行了授权搜查，发现并没收了计算机设备和部件。计算机设备未在核电厂领土内获得授权，形成了一个可以访问互联网的单独的局域网，并用于接收加密货币。

在 104 号机柜中，SBU 查获了六个 Radeon RX 470 显卡，两个延长线，四个电源，三个系统单元（其中一个是自制的），一个带有电源的开关，带有三个显卡的金属支架，七个提升器和五个延长线，一个主板，一个 U 盘和一个硬盘。此外还有一套金属框架，其上安装了主板，三个冷却器，五个显卡，一个硬盘和两个电源。

同一天，搜查工作在军事单位 3044（乌克兰国民警卫队编辑）使用的场所进行，位于南乌克兰核电站的领土上。搜索结果发现并查获了 16 个显卡，一个具有军事单元库存号的 system unit，即台式计算机的组件，可见水深，背后是否还涉及军事单位的人参与挖矿呢？

当然，还有七个机械硬盘，两个固态硬盘，一个 U 盘和一个路由器，均用于数字货币挖矿。此外，SBU 员工在 SUE NPP 的其他场所发现并没收了 CTC 联合媒体转换器，光纤和网络电缆，理论上这些电缆不应该出现在这些场所内。

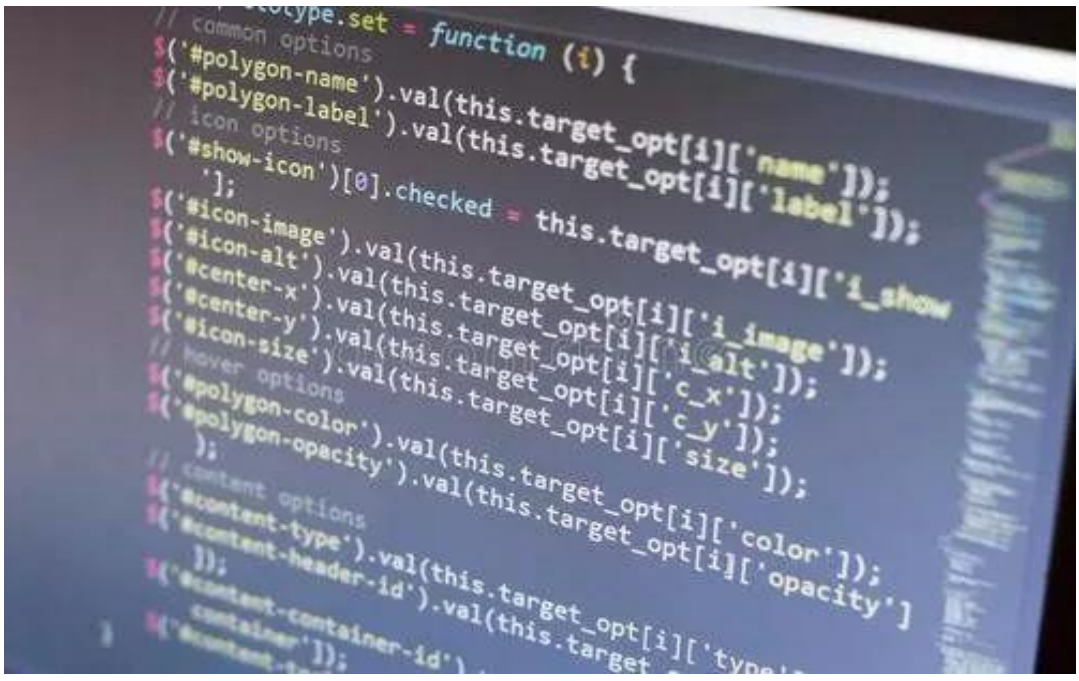
当然，这不是乌克兰第一次被偷电挖矿了，据此前报道，2018 年 2 月，俄罗斯联邦核

中心的多名工程师因试图使用乌克兰最大的超级计算机之一开采比特币(BTC)而被捕。而这台计算机每秒能够执行 1000 万亿次计算，为了安全起见，一直与互联网断开连接。（来源：中关村在线）

➢ “为了给家乡做点贡献” 男子入侵政府网站被捕

2019 年 8 月 16 日，记者从宁夏银川市公安局网安支队了解到，该支队主要侦办黑客攻击、组织考试作弊、侵犯公民个人信息等网络违法犯罪。今年以来，该队已成功侦办 8 起案件。近期，银川市公安局网安部门就成功侦办一起重大非法侵入计算机信息案。

2019 年 7 月 19 日，某政府网站管理员向网安支队报警，该政府网络内局长信箱模块有网民多次发送非正常留言，后模块运行不正常，疑遭黑客攻击。接警后，网安支队立即开展核查，发现有用户名为“ADMIN”、“ADMI”两个账号在该网站上进行注册后，表面上留言内容为“11111111”或者空白，但其实均隐藏着恶意代码。嫌疑人的行为已构成《刑法》二百八十五条非法侵入计算机信息系统罪。至此，网安支队确定该网站被黑客使用跨站脚本攻击(XSS)方式进行非法入侵。



办案民警介绍，该攻击方式可以秘密获取网站管理员使用电脑的浏览器权限，并绕过验证登陆后，可删改网站内容，并进行植入木马等后续提权操作等，进而可能造成非常严重后果。

2019 年 7 月 22 日，网安支队将此案立为“7.22 某政府门户网站被非法侵入计算机信息系统案”，市县两级网安部门抽调精干力量组成专案组开展联合侦查。

经查，嫌疑人真实身份为李培及其徒弟李木子，经过多方调查发现二人均在乌鲁木齐市。在掌握嫌疑人犯罪事实以及住址后，专案组于 7 月 25 日派出抓捕小组赴新疆乌鲁木齐市进行抓捕，经过当地警方大力配合，于 7 月 31 日将两名嫌疑人成功抓获归案。经审讯，李培供职于某网络科技公司，负责向运营商提供重要信息系统等级保护测评业务，工作中网络渗透测试的目标网站均获得官方授权，属于公司正常业务行为。

那么，李培为何会对银川市的政府网络实施黑客攻击呢?

原来，李培是银川人，最近，他利用休息时间，在未授权的情况下，对银川市的某政府网站进行渗透测试，他的目的就是为了找出网站漏洞并生成漏洞报告，然后上传 CNVD(国家信息安全漏洞共享平台，由国家计算机网络应急技术处理协调中心运营)，由 CNVD 下发各网站进行修补。

按照李培的说法，他这是为家乡做点贡献，在此之前，他还对包括石嘴山市多个政府网站及周边多个省、市政府网站进行攻击。可法律意识较为淡薄的李培并没有意识到自己的行为属于违法犯罪行为。最终，两名嫌疑人对犯罪事实供认不讳，目前羁押在银川市看守所。

（来源：中国长安网）

➢ 美德克萨斯州 23 个政府机构网络遭“协同勒索软件攻击”下线

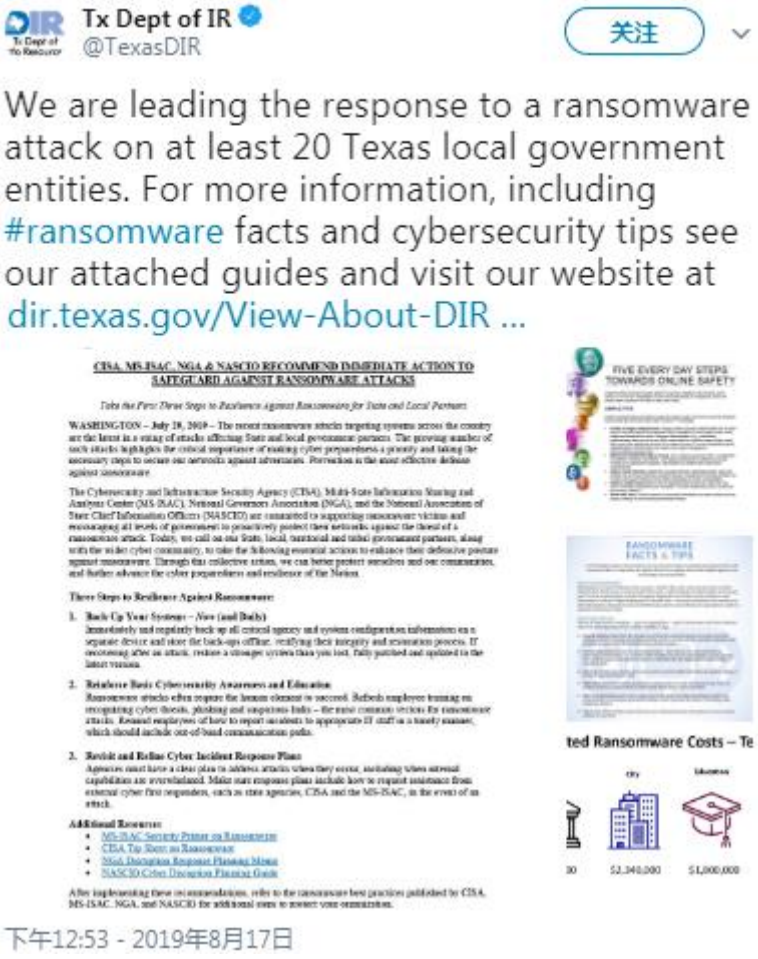
2019 年 8 月 21 日,据外媒 Gizmodo 报道，当地时间上周五早上，德克萨斯州的近 20 家州政府机构报告称存在重大计算机问题。该州现在认为，导致这次严重攻击事件的罪魁祸首是同一个黑客。德克萨斯州信息资源部(DIR)周五在一份新闻稿中说，其正在监督该州数个州政府机构对“协调勒索软件攻击”的反应。截至周六，DIR 知道有 23 个受攻击影响的机构，该部门认为这可能是由“单一威胁行为者”执行的。

DIR 表示正在与许多组织合作，将系统重新上线，包括州紧急事务管理部、军事部和公用事业委员会，以及联邦调查局的网络部门和联邦紧急事务管理部门。

“目前，DIR、德克萨斯军事部和德克萨斯 A&M 大学系统的网络响应和安全运营中心团队正在为受影响最严重的司法管辖区部署资源，”

DIR 在一份声明中说：DIR 并没有具体说明哪些机构在袭击中受到影响。“在这个时候，

我们尚未列出受影响的实体，以免使其成为其他潜在坏人的目标，”DIR 发言人在一封电子邮件中说。



这一事件只是最近针对美国市政当局和州政府机构的多起勒索软件攻击中的最新事件。今年 6 月，佛罗里达州里维埃拉海滩市议会投票决定支付超过 60 万美元给一个勒索软件团伙,以恢复被锁定和加密的数据。几天后，佛罗里达州的 Lake City 向袭击该城市网络的黑客支付了价值 46 万美元的比特币赎金。

今年 5 月，属于巴尔的摩市政府的大约 10000 台计算机感染了 RobbinHood 勒索软件，这次攻击预计将使该市损失数千万美元。去年，亚特兰大市遭受 SamSam 勒索软件攻击，两名伊朗黑客被起诉。

正如 Next Web 在报道德克萨斯州攻击事件时指出的那样，网络安全公司 Malwarebytes 最近的一份报告显示，该公司已经看到针对普通消费者的恶意软件攻击正在减少，而针对政府机构和企业的攻击却在增加。根据调查结果，2019 年第二季度针对企业的勒索软件检测增加了 363%。（来源：cnBeta）

➢ 高三学生自学编程研发“黑客软件” 盗取上亿条个人信息被公诉

2019 年 8 月 30 日，自学软件编程技术，研发黑客软件利用网站注册漏洞疯狂盗取公民个人信息上亿条，在境内外网络公开售卖……刚满 18 岁的在校学生，竟构想出一个非法“数据帝国”的梦！记者 8 月 29 日从无锡市惠山区人民检察院(下称：惠山检察院)获悉，该院近日依法以侵犯公民个人信息罪对犯罪嫌疑人刘某某提起公诉。

市民举报一名购买黑客软件的男子被抓

2018 年 9 月，无锡市惠山区警方接到网友的举报称，有人在论坛、贴吧等平台售卖公民个人信息以及盗窃信息所用的黑客软件，惠山区警方第一时间立案侦查，跨省抓捕了江西籍 26 岁犯罪嫌疑人付某。

付某交代，自己网名叫“清风”，对软件编程和黑客技术有着浓厚的兴趣，于 2018 年初在某网络交流论坛中向一个网友请教获取他人的个人信息的方法，并从对方那购买了一款黑客软件用于非法获取公民个人信息。

据查，2018 年 5 月至 8 月，付某利用购得的黑客软件攻击各网站系统漏洞，非法获取公民个人信息，并将该黑客软件升级并取名“清风安全网-手机号批量查姓名”，在网络论坛等渠道以 500 元/月的价格大肆售卖，累计侵犯公民个人信息 200 多万条，非法获利上千元。2019 年 4 月 3 日，犯罪嫌疑人付某被提起公诉，被判处有期徒刑三年六个月，并处罚金 3000 元。

顺藤摸瓜“黑客”竟是一名 18 岁高中生

而在办理此案的过程中，犯罪嫌疑人付某交代，出售给他黑客软件的网友叫“i 春秋”，这一信息引发了办案人员的“注意”。随后，惠山检察院与惠山区警方顺藤摸瓜，锁定到该网名的网络 IP 地址，确定“i 春秋”网名使用者为刘某某，其定位于广东省信宜市。同时，惠山区警方发现刘某某涉嫌盗取公民个人信息，在境内外网络渠道公开售卖，遂立案。

2019 年 4 月，惠山区警方赴广东省进行案件调查，犯罪嫌疑人刘某某竟是广东省信宜市某高级中学的一名刚年满 18 周岁高三在校学生。刘某某被警方带走后，该校教师和同学始终不敢相信，这样一个普普通通即将奔赴高考的高中生会是一个精通网络技术，盗窃公民个人信息的黑客。

据了解，犯罪嫌疑人刘某某是一名理科生，家境条件优越，从小就对计算机十分感兴趣，经常利用节假日操作电脑，自学计算机技术，还通过翻墙软件浏览境外网站“取经”，其父母因为工作繁忙，以为刘某某只是玩电脑，所以持放任态度。到高中阶段，刘某某已掌握独立编写软件程序的能力。

据犯罪嫌疑人刘某某交代，从 2017 年下半年开始，其在各大论坛、贴吧看到查询网络用户个人信息的方法，对此产生了兴趣，心想能通过自己学到的技术和本事应该可以获取他人的个人信息，于是刘某某不知不觉走上了不归路。

不出一月，刘某某成功编写出一款软件，该软件可通过内置接口，将其对接到各网站后，便轻松获取到网站用户账号和对应的手机号。但很快刘某某发现该软件操作繁复，且不能批量获取信息。于是，在 2018 年 6、7 月，刘某某在网络论坛中找到了解决方案，并计划构建属于自己的“信息数据库”。

“数据帝国”非法获取约亿条公民个人信息

刘某某受到启发，又编写出了一款能够批量获取信息的软件，将软件接口与某网站进行对接，成功获取了该网站的用户账号以及对应手机号码。为了建立自己的“数据帝国”，刘某某租用了网络数据对信息进行储存，并专门在境外租用十多台服务器支持操作。

一个月的时间，刘某某非法获取了约 1 亿条公民个人信息，全部存储于自己的数据库中。刘某某为了不让其他同行发现漏洞，于 2018 年 8 月向其盗取个人信息的网站反馈，将网站存在的漏洞进行封堵。此后，刘某某在境内网络建立起微信、QQ 群，在境外使用“telegram”等聊天工具，自助编写“信息查询”机器人，将数据库通过微信、QQ 等群聊以包月查询的形式向他人兜售，并且通过连接 VPN 翻墙在境外以比特币为交易货币贩卖数

据库长达两个月，共计获利约两万元。考虑到有风险，担心公安机关发现，刘某某将数据库封存不再售卖。

检察官： 暴露网络平台安全问题

按照犯罪嫌疑人刘某某的设想，他将会对数据库中上亿条个人信息进行整理，进而获取用户名、手机号码对应的真实姓名、家庭地址等公民个人信息，利用技术手段实现经纬度实时定位，从而建立起一个强大的“数据帝国”。

承办检察官指出，该案数据总量大，非法获取公民个人信息精准，暴露出了一些网络平台用户信息存在明显的安全问题。同时犯罪嫌疑人买卖个人信息均为线上交易，为逃避打击和监管，其依托 QQ 群、微信群，通过第三方支付平台进行交易，甚至通过翻墙登录一款境外聊天软件，以比特币为货币单位进行交易，境外 IP 地址难以追寻，交易平台不具备监管力度，信息交易情况极其隐蔽，危害公民个人信息安全甚至是国家数据信息安全。

近年来，网络犯罪案件上升趋势显著，并呈现出低龄化。针对类似案件暴露出的问题，惠山检察院将与知名互联网企业合作，及时调取相关数据信息，及时预警和取缔存在非法交易行为群体或个体账户，建立健全违法犯罪线索移交机制，并通过典型案例释法明理，提高公民对个人信息保护的重视程度。（来源：杨子晚报）