国盟信息安全通报

2021 年 04 月 11 日第 237 期

全国售后服务中心

国盟信息安全通报

（第 237 期）

国际信息安全学习联盟

2021 年 4 月 11 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 700 个，其中高危漏洞 141 个、中危漏洞 406 个、低危漏洞 153 个。漏洞平均分值为 5.08。本周收录的漏洞中，涉及 0day 漏洞 497 个（占 71%），其中互联网上出现“Wordpress 插件 Duplicator 任意文件读取漏洞、Agentejo Cockpit 跨站脚本漏洞（CNVD-2021-24260）”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 3125 个，与上周（3128 个）环比减少 0.09% 。

主要内容

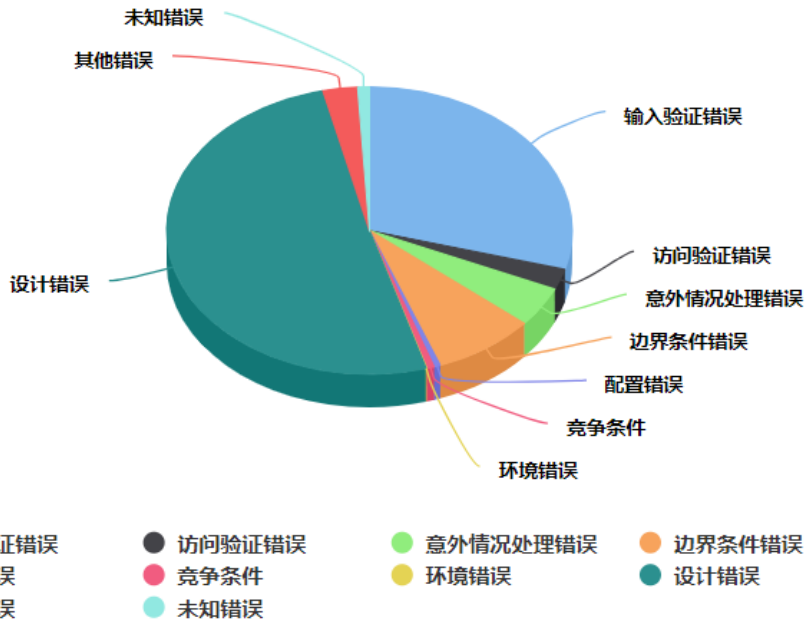
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

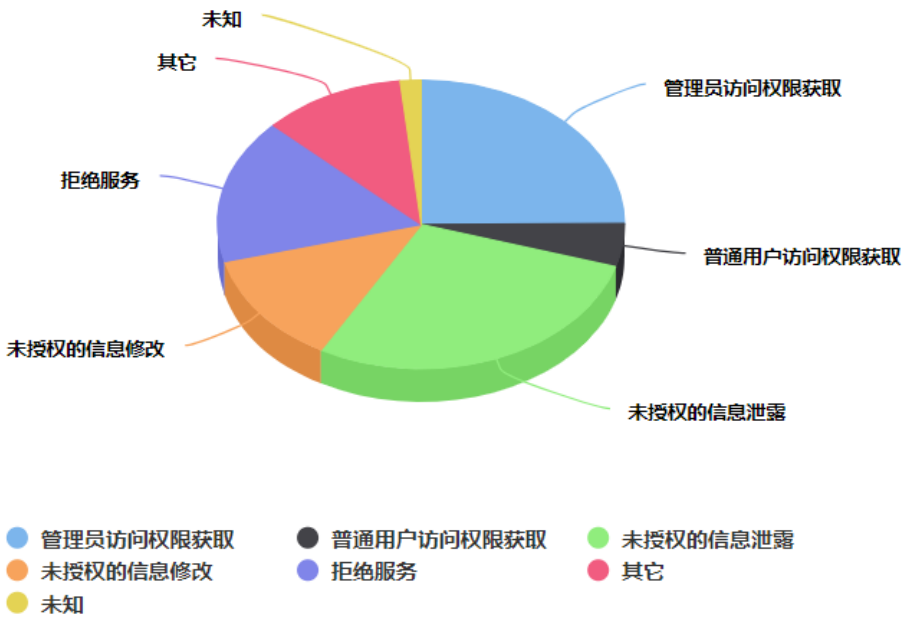
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 700 个，其中高危漏洞 141 个、中危漏洞 406 个、低危漏洞 153 个。漏洞平均分值为 5.08。本周收录的漏洞中，涉及 0day 漏洞 497 个（占 71%），其中互联网上出现“Wordpress 插件 Duplicator 任意文件读取漏洞、Agentejo Cockpit 跨站脚本漏洞（CNVD-2021-24260）”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 3125 个，与上周（3128 个）环比减少 0.09%。

二、安全漏洞增长数量及种类分布情况

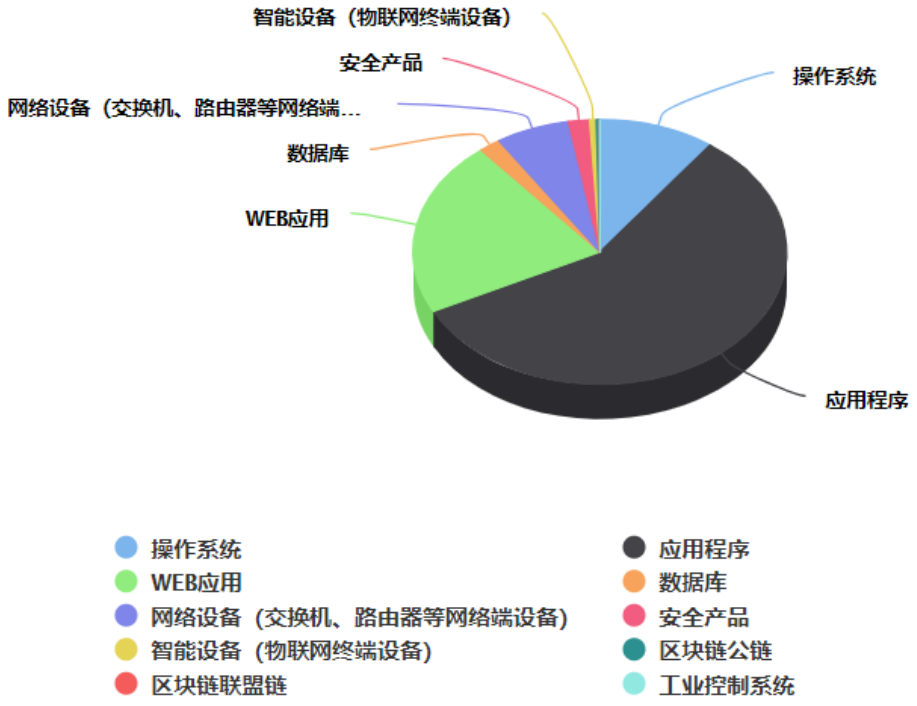
➢ **漏洞产生原因（2021 年 3 月 28 日—2021 年 4 月 11）**



➢ 漏洞引发的威胁（2021 年 3 月 28 日—2021 年 4 月 11）



➢ 漏洞影响对象类型（2021 年 3 月 28 日—2021 年 4 月 11）



三、安全产业动态

➢ 坚决遏制电信网络诈骗犯罪多发高发态势

近日，**中共中央总书记、国家主席、中央军委主席习近平近日对打击治理电信网络诈骗犯罪工作作出重要指示强调**，近年来，各地区各部门贯彻党中央决策部署，持续开展电信网络诈骗犯罪打击治理，取得了初步成效。要坚持以人民为中心，统筹发展和安全，强化系统观念、法治思维，注重源头治理、综合治理，坚持齐抓共管、群防群治，全面落实打防管控各项措施和金融、通信、互联网等行业监管主体责任，加强法律制度建设，加强社会宣传教育防范，推进国际执法合作，坚决遏制此类犯罪多发高发态势，为建设更高水平的平安中国、法治中国作出新的更大的贡献。

中共中央政治局常委、国务院总理李克强作出批示指出，依法打击电信网络诈骗犯罪的成效要继续巩固并深化，更好维护人民群众财产安全与合法权益。

全国打击治理电信网络新型违法犯罪工作电视电话会议 8 日在京召开。会上传达了习近平重要指示和李克强批示。国务委员、国务院打击治理电信网络新型违法犯罪工作部际联席会议总召集人赵克志在会上讲话，他指出，习近平总书记的重要指示为做好当前和今后一个时期的打击治理电信网络诈骗犯罪工作指明了前进方向、提供了根本遵循。要深入学习贯彻习近平总书记重要指示，增强“四个意识”、坚定“四个自信”、做到“两个维护”，切实

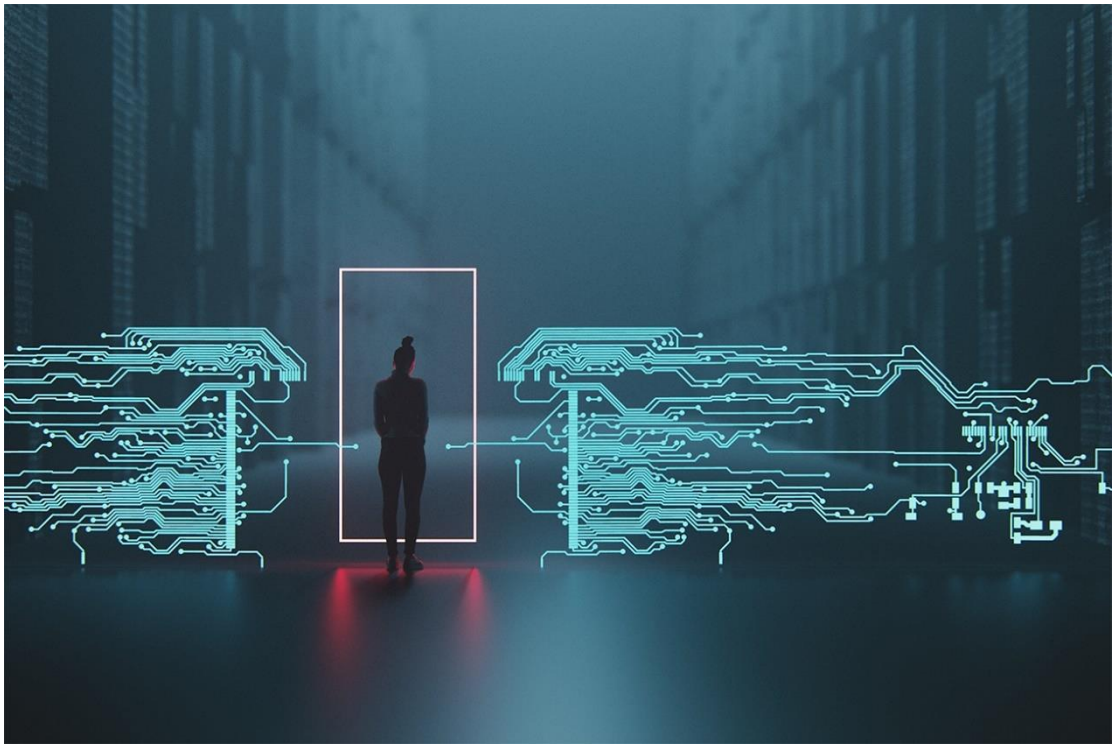
把打防管控各项措施抓细抓实抓落地，坚决遏制电信网络诈骗犯罪多发高发态势，以优异成绩庆祝建党 100 周年。

中央网信办、工业和信息化部、中国人民银行、最高人民法院、最高人民检察院有关负责同志在会上作了发言。会议通报了全国打击治理电信网络新型违法犯罪工作有关情况。

国务院打击治理电信网络新型违法犯罪工作部际联席会议召集人、25 个成员单位负责同志等在主会场参加会议，省市县三级打击治理电信网络新型违法犯罪工作联席会议召集人、成员单位负责同志在各地分会场参加会议。（来源：新华社）

➢ 立规铸范 重手严打 紧盯人民揪心事 破解网络诚信题

互联网时代，网络不仅是人们的生活方式，而且成为社会的运作方式和经济的运行方式。网络诚信，从一域变全局，成为社会诚信的载体和表现。今年 315 晚会曝光的多个案例涉及网络诚信，网上讨论至今余热未消，说明网络失信行为已经成为人民痛点和发展阻碍。人无信不立，业无信不兴，国无信不强。网络诚信建设必须成为社会诚信建设的基础性工程，需要一砖一瓦，立规铸范。近日，国家互联网信息办公室、工业和信息化部、公安部、国家市场监督管理总局联合印发《常见类型移动互联网应用程序必要个人信息范围规定》，涉及 39 类常见网络服务类型，针对的正是互联网领域的失信行为。



中国社会科学院大学新闻传播学院副院长、中国社会科学院新闻与传播研究所数字媒体研究室主任、研究员黄楚新认为：“全社会与互联网深度融合，网络诚信水平就是社会整体诚信水平的体现，会最大影响人们对社会整体诚信水平的感受、认知与满意度。”

隐私泄露：建议明确责任、顶格处罚

隐私泄露是央视 315 晚会后的热点话题之一。智联招聘、前程无忧、猎聘网等招聘平台均存在若干漏洞。大学生小傅告诉记者，自己去年暑假找兼职时在招聘 APP 上填报了个人信息，至今仍在收到很多精准拨打的骚扰电话，令人不胜其烦、不寒而栗。

新出台的《规定》已对求职招聘类 APP 作出规范，将“必要个人信息”限定为“注册用户移动电话号码”“求职者提供的简历”，当招聘 APP 索要其他个人信息时，求职者有权不予提供。此前中国青年网曾做调查，通过黑产 QQ 群购买一份简历只需 7 元，相关个人信息一览无余，求职者很容易落入诈骗陷阱。近年来，各地警方破获多起类似案件。

北京市京师（重庆）律师事务所律师韩世文在接受采访时说，近年来，个人信息泄露和买卖严重侵害公民合法权益，有些已经酿成了无可挽回的损失。网络安全法规定了加强网络安全保障，保护公民、法人和其他组织的合法权益。已经施行的《民法典》也作出规定，个人信息的收集、存储、使用、加工、传输、提供、公开等，应当遵循合法、正当、必要原则，不得过度处理。

“不只招聘类 APP，信息泄露在整个社会场域中都存在，网民几乎‘裸奔’，给犯罪行为提供便利，并产生连锁负面反应，比如有的年轻人因网贷致死。这不是个体问题，是结构性问题，不解决‘土壤’的问题，光对一棵树局部修枝剪叶，将来还会出问题。一旦出现问题，就应该排查系统性风险并进行顶格惩罚。”中国社会科学院大学新闻传播学院常务副院长漆亚林告诉中国青年网，有法律法规但执行不力、违法成本低、一人受罚但利益产业链条上更多人仍在获利，是这类问题屡禁不止的更深层次原因。被央视 315 晚会曝光后，属地有关部门约谈了智联招聘和猎聘网，并表示将加强监管，加大曝光和处置力度。

在漆亚林看来，除了重拳出击处置，还需要明确诚信链条上各方的责任，哪些是平台责任，哪些是个人责任，必须分明。“不能靠大学生自己去甄别真假。平台把关是前提，因为平台是获利方，负有监管责任，不能把责任推给消费者。立法中，责任要分明；执法中，处罚要到位。要系统分析，抓住要害。”

网络直播：亟需行业共识、技术控制

眼下，网络直播成为失信重灾区。去年 6 月，北京市消协发布报告指出，在 30 个直播带货体验样本中，竟有 9 个样本存在证件信息公示问题，3 个样本涉嫌虚假宣传问题。在创

造历史的“消费奇迹”背后，是刷单者疯狂的“引流集赞”。受访者小颖表示，自己在主播诱导下购买了一款“火遍全网”的运动鞋，到手后却发现是低劣仿货。此外，直播间大量存在的以抽奖和打赏为掩盖的涉嫌赌博行为，更是毒害万千青少年。

人民数据研究院副院长陈丽告诉记者，网络直播中的失信问题，多表现为商品质量低劣、夸大宣传、服务缺少监管、售后缺乏保障，问题的症结与行业和舆论都分不开。

首先是行业风控。直播带货往往依靠私域流量变现。私域流量强调主播自身进行营销和传播的自主控制权，播出过程中很少受到限制，风控意识不足，甄别不充分。其次是舆论氛围。“流量为王”，主播间的比拼大多数只看粉丝数量和售卖金额，很少对质量或信誉进行评估和评价。这种“只重量而不重质”的风气影响了对行业、对主播行为的评价。

找到问题症结，亟需对症下药。3 月 15 日，国家市场监督管理总局制定出台《网络交易监督管理方法》，对社交电商、直播带货等领域出现的新问题，明确了网络服务提供者的角色定位，明确了网络交易经营者、网络交易平台经营者、市场监管部门等主体的责任与义务，对虚假交易、伪造流量、误导性展示、混淆视听等网络不正当竞争行为进行了明文规制。

有专家担心，这些规范和办法仅作为行业自律性文件存在，对直播带货中的违法犯罪活动无法起到强制性的震慑作用，只能起到督促和劝诫作用。但陈丽认为，这种正在形成的行业共识，恰恰代表着网络直播行业的蜕变和趋势。

“去年 6 月，人民数据研究院和中国经济体制改革研究会互联网与新经济专业委员会做了一项关于数据安全的研究，发布了大数据风控与权益保护研究报告，着眼于行业共识的形成，提出‘行业自律十二原则’：合法原则、授权原则、必要原则、最小范围原则、明示原则、比例原则、封存销毁原则、可追溯原则、被遗忘原则、整体性安全原则、保护开发者原则、数据合规原则。”陈丽说。

除了这些由内而外的约束，下一步，直播带货中的网络失信行为，还有望通过新技术力量得到控制。

“5G 的发展，AR/VR 设备的普及，会从技术层面给直播带货行业带来巨大的想象空间。”陈丽告诉中国青年网，5G 环境下，直播视频的速度和清晰度会有大幅度提升，电商直播制造的临场感也会愈发生动鲜活。VR 直播营造虚拟的购物环境，使观众“身临其境”，商品细节一览无遗，这种沉浸式体验有助于消费者了解真实情况，有利于改进现有的直播带货中的失信问题。

对于新技术助力解决网络失信问题，黄楚新的判断更加乐观。“未来，前沿技术将为我国网络诚信建设提供更大的想象空间。人工智能技术将通过机器学习不断完善信息监管与筛

查机制，保障网络诚信建设的程序化与规范化。区块链技术以其去中心化与安全可靠的特点搭建网络诚信体系，激活行业发展的内生动力。今后随着量子通信技术的进一步发展，网络诚信建设必将借助系统化、底层化的科技力量，迈向量子加密传输的新阶段，助力我国数字经济行稳致远。”

公益诉讼：检察机关根治网络失信新尝试

最近几年，检察机关的公益诉讼新尝试，正在为根治网络失信行为探索司法路径。网络预付卡存入高额款项，但一朝商家跑路，款项立刻打水漂。最高人民检察院检察长张军、黑龙江省人民检察院检察长高继明都是全国人大代表，2020 年全国两会期间，他们与其他三位全国人大代表一起就探索预付卡消费领域检察公益诉讼、推动相关法律完善提出建议。最高检还曾专门组织全国人大代表赴上海和黑龙江两地实地调研。

在上海的调研中，代表们发现，预付卡消费这种网络失信行为和“九龙治水”的痼疾有关。根据上海市商务委市场秩序处处长刘炜的调查，单用途预付卡实行备案制，虽然法律上要求发卡企业必须把信息系统跟监管平台进行连接，但大量企业并没有按照地方人大要求联网、上报，商务部门也没有比较有力的手段强制所有的企业实现报备，只能先行把头部的大企业管住。“单用途预付卡消费领域的有效监管是一个系统性工程，光靠一个部门是不行的，必须形成合力。”他说。

检察机关的介入，成为撬动多部门联动、推动社会共治的关键一环。

上海市松江区市场监管局副局长宗晔发现，落实层面监管主体不明，权责不清，程序过于复杂，监管责任与执法权之间有错位现象。按照商务部的规定，商务部门有监管责任，也有权处罚，但由于商务部门没有执法力量，也无法做到日常巡查，所以处罚最终是由市场监管执法部门执行。

“关于是否有必要由最高人民检察院向有关行政主管部门制发检察建议，调研中许多地方和部门提出，应当顺应互联网时代新业态的发展，搞准单用途商业预付卡的新属性，主要是消费方式还是融资手段，再确定主管部门，规范监管措施。”最高人民检察院第八检察厅主办检察官、二级高级检察官邱景辉认为，鉴于这是一项复杂的系统工程，有必要明确牵头部门，统筹协调相关职能部门，发动行业协会、经营者、消费者积极参与、共享共治。

“最高人民检察院工作报告指出，紧盯人民群众的操心事、烦心事、揪心事，自觉在保障人民权益中担当作为。我们将抓紧研究论证，坚持问题导向、目标导向、效果导向，坚持法治思维和法治方式，以公益诉讼检察为抓手，协同刑事检察、民事检察、行政检察综合发力，争取从国家层面推动单用途商业预付卡监管资源整合、力量融合、手段综合，创新系统

集成、协同高效的源头治理，形成源头治理、预防为主的整体效应。”邱景辉说。（来源：中国青年报）

➢ 深度解读密评新国标 GB/T 39786-2021

2021 年 3 月，国家市场监督管理总局、国家标准化管理委员会发布中华人民共和国国家标准公告（2021 年第 3 号），国家密码应用与安全性评估的关键标准 GB/T 39786—2021《信息安全技术信息系统密码应用基本要求》（以下简称 GB/T 39786）正式发布，将于 2021 年 10 月 1 日正式实施。

GB/T 39786 是贯彻落实《中华人民共和国密码法》、指导我国商用密码应用与安全性评估工作开展的纲领性、框架性标准。该标准分五个级别，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个方面提出了密码应用技术要求，从管理制度、人员管理、建设运行和应急处置四个方面提出了密码应用管理要求，对于规范引导信息系统密码合规、正确、有效应用具有重要意义。

作为标准，GB/T 39786 没有也不适合在正文中做过多解释说明。为促进 GB/T 39786 的宣贯落实，作为标准的起草组成员，我们特撰写此文，对 GB/T 39786 的若干全局性要点进行解析。出于以上目的，同时限于篇幅，本文并不逐条描述标准内容，而是围绕标准的定位、使用等若干广为关心的要点问题展开，希望能够增进信息系统责任单位、商用密码应用安全性评估机构（以下简称“密评机构”）等对标准的理解，促进本标准在密码应用和安全性评估活动中发挥应有的作用。

一、GB/T 39786 的制订过程

GB/T 39786 是首次制订，但并非从零开始。2018 年，为指导当时即将启动的商用密码应用安全性评估试点工作，国家密码管理局发布了密码行业标准 GM/T 0054—2018《信息系统密码应用基本要求》（以下简称 GM/T 0054）。2018 年以来，基于 GM/T 0054 开展的密码应用和安全性评估工作，充分验证了 GM/T 0054 的科学性和可行性，也为 GB/T 39786 的制订带来了丰富的实践经验。此次 GB/T 39786 在 GM/T 0054 基础上进一步修改完善，制订发布为国家标准，其完备性、合理性、可操作性都得到进一步提升。

GB/T 39786 是在国家密码管理部门的全程指导下制订的。相关领导同志站在法律遵循、政策衔接、管理对接等角度，对标准提出了诸多指导意见；国家密码管理部门多次组织围绕本标准的专题研讨，从密码应用推进与安全性评估体系建设的全局，对本标准提出要求，并对编制组提出的跨部门联络等需求予以积极响应和协助。

GB/T 39786 是在各行业领域国家主管部门、商用密码业界同行的悉心帮助下制订完成的。标准起草单位涵盖 9 家密评试点机构、5 家商用密码产业单位、2 所大学，具有广泛的代表性。在标准起草阶段，首批密评试点机构、全体信安标委 WG3 工作组成员单位以及全体密标委应用组成员单位给予了倾心帮助。2019 年 6 月 25 日至 8 月 8 日，信安标委秘书处向工业和信息化部科技司、公安部十一局、国家保密局、国家密码管理局、国家认证认可监督管理委员会、中央网信办网络安全协调局等上级主管部门发函征求意见，并在信安标委官网面向社会公开征求意见。共收到国内外反馈意见 67 条，标准起草组均进行了认真的处理。

标准于 2019 年 10 月经信安标委 WG3 工作组投票通过，形成送审稿；2019 年 12 月通过信安标委审查，形成报批稿。在报批待发布阶段，国标委对标准行文、用语、格式给予了细致指导，使得标准文字质量日臻完善，为标准的最终发布奠定了良好基础。

二、GB/T 39786 内容概要及相较 GM/T 0054 的变化

GB/T 39786 整体上按照不同的密码应用级别，针对每个级别分别提出技术要求和管理要求，随着级别的提升，对密码应用的要求程度越来越强。其中对于不同级别的技术要求，又从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个层面分别提出，而各个级别、各个层面均需要共同遵循标准第 5 章所提出的通用要求。

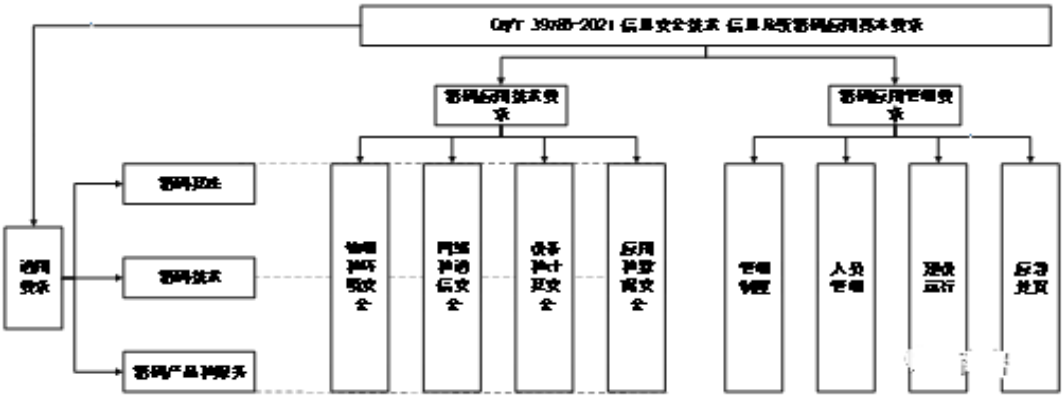


图 1 GB/T 39786 内容框架

与 GM/T 0054 相比，GB/T 39786 加强了与国家标准 GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》（以下简称 GB/T 22239）的衔接，明确了不同等级信息系统所使用的密码产品的安全级别要求，并结合密评工作实践对内容进行了优化，使之更为科学合理。其中主要的变化有四个方面。

1.行文结构的变化

GM/T 0054 采用了“先分层，后分级”的行文结构，按照物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个技术层面，以及单独的管理层面，分别描述每层中第一级到第四级信息系统的密码应用要求。

GB/T 39786 则改为了“先分级，后分层”的行文结构，按照信息系统密码应用第一级到第五级，分别描述每级的密码应用技术要求和管理要求，其中第五级为“略”。这种变化使得相应级别信息系统的责任单位，能够更为直观的查阅标准。

2.完整性要求的变化

GB/T 39786 总体上将 GM/T 0054 第三级对完整性要求的约束程度由“应”调整为“宜”，第四级维持“应”。这项调整的主要原因是与 GB/T 22239 形成更好的衔接。

在 GB/T 22239 中，对于网络安全等级保护第三级的数据完整性要求是“应采用校验技术或密码技术”进行完整性保护，见 GB/T 22239—2019 的 8.1.2.2 和 8.1.4.7；对于网络安全等级保护第四级提出“应采用密码技术”进行完整性保护，见 GB/T 22239—2019 的 9.1.2.2。为与上述网络安全等级保护要求相衔接，特在 GB/T 39786 中做出本调整。

需要说明的是，信息系统责任单位对于约束程度为“宜”的条款要求，并非可以随意选择不遵循该条款（即“不适用”），相关细节将在本文第四章描述。

3.对密码产品安全性级别要求的变化

GM/T 0054 对于第三级信息系统，对密码产品的配用采用了“宜采用符合 GM/T 0028 的

三级及以上”的描述。在工作实践中发现这种描述使得三级系统对于“宜”的解释空间较大，甚至会出现采用一级产品是否符合要求的争议。

为明确对密码产品安全性的门槛，GB/T 39786 对第三级信息系统的密码产品配用要求更改为“应达到 GB/T 37092—2018《信息安全技术密码模块安全要求》（以下简称 GB/T 37092）二级及以上”，仍维持第四级信息系统的密码产品“应达到 GB/T 37092 三级及以上”的要求。这样既降低了主观解释的不确定性，使得密码应用和安全性评估的客观依据更为明确，也使得第三级和第四级系统有了显著区分。

需要说明的是，信息系统所使用密码产品的安全级别遵循 GB/T 37092，经商用密码产品认证后确定，在产品认证证书上标明。商用密码应用安全性评估活动中，不对具体密码产品做考察，而是在确保实际使用的密码产品与产品认证证书的一致性后，直接采信产品检测认证的结果。对于应取得而未取得认证证书的商用密码产品，《信息系统密码应用高风险判定指引》将其视作高风险项之一。

4.密钥管理要求的变化

相比于 GM/T 0054 在正文中对不同等级信息系统提出环节逐渐增多的密钥管理要求的做法，GB/T 39786 在正文中重点对密钥管理与使用提出管理性质的要求，将密钥管理生命周期所涉及技术环节内容移至资料性附录 A。

这项调整是从标准衔接和可操作性角度考虑的。GM/T 0054 对密钥生命周期各环节的要求，本质上是对实现密钥产生、存储、分发、使用等功能的密码产品的技术要求，这些密钥管理的能力基本上是由密码产品来实现的。如前所述，密码应用安全性评估并不对密码产品进行重复检测，而是直接采信密码产品检测认证的结果。从与 GB/T 37092 衔接的角度，GB/T 39786 就不宜再重复规定密码产品的密钥管理安全能力。故此，GB/T 39786 一方面在通用要求部分对密钥管理所依托的密码产品和密码服务进行约束，另一方面从 GB/T 37092 不涉及的管理角度对密钥管理提出要求，如 8.5“管理制度”中要求密码应用安全管理制度包含密钥管理的制度、8.6“人员管理”中要求设置密钥管理员等。而将原 0054 中对密钥管理的技术要求修改后移入资料性附录。

需要注意的是，这并不意味着密钥管理不重要。事实上，密钥生命周期管理对信息系统密码应用安全来说是至为关键的，密码应用方案中应以独立的密钥管理章节详细说明信息系统涉及的密钥，包括其用途、生命周期涉及的环节，以及每个环节上使用了何种密码产品进行了何种保护。在密钥管理制度中，也应清晰说明密钥管理的相关方及其职责，在密钥各生命周期环节的操作规程，以及违反操作规程的惩处措施。在测评时，密评机构应审查密码应

用方案的密钥管理部分是否涵盖了各个层面所有的密钥、是否每个密钥的生命周期环节保护描述清晰，以及其保护措施是否能够保障密钥的安全。对于密钥管理的测评，在《信息系统密码应用测评要求》中进行了明确；而在关于密钥管理不当造成的高风险项，在《信息系统密码应用高风险判定指引》中做了清晰规定。

三、GB/T 39786 定位及其配套文件

在密码标准体系之中，GB/T 39786 位于“密码应用”大类的“应用要求”子类。

GB/T 39786 是信息系统密码应用的纲领性、框架性标准，但并非唯一标准。事实上，由于各行业、各领域信息系统的复杂性，很难用一个统一的标准去精确刻画所有的信息系统密码应用。在 GB/T 39786 的总框架下，相关标准化组织陆续制订发布了一些针对特定信息系统的密码应用技术要求和指南；密评联委会从测评的角度，也发布了进行密码应用安全性评估活动的一些指导性文件。

1.GB/T 39786 框架下的系列密码应用标准

在 2018 年 GM/T 0054 发布后，密码行业标准化委员会陆续制订发布了一批针对具体应用场景的密码应用技术要求和指南。这些标准聚焦电子保单、远程移动支付、电子招投标等不同的应用场景，就 GM/T 0054 的要求在特定信息系统中进行了进一步的具象化，供各行业领域信息系统责任单位参考。随着 GB/T 39786 的发布，这些标准在将来可能要做少许适应性修订。

表 1 GB/T 39786 框架下的系列密码应用标准列表

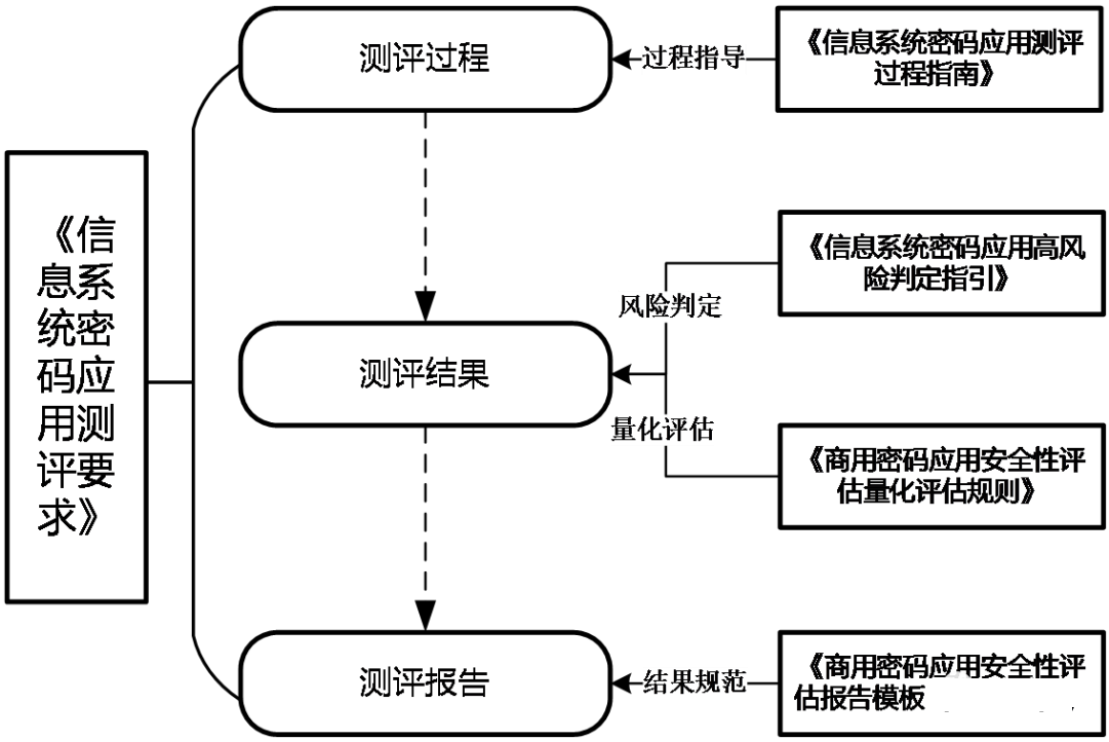
标准大类	标准子类	标准名称
密码应用	应用要求	GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求
		GM/T 0070—2019 电子保单密码应用技术要求
		GM/T 0072—2019 远程移动支付密码应用技术要求
		GM/T 0073—2019 手机银行信息系统密码应用技术要求
		GM/T 0074—2019 网上银行密码应用技术要求
		GM/T 0075—2019 银行信贷信息系统密码应用技术要求
		GM/T 0076—2019 银行卡信息系统密码应用技术要求
		GM/T 0077—2019 银行核心信息系统密码应用技术要求
		GM/T 0095—2020 电子招投标密码应用技术要求
		GM/T 0100—2020 人工确权型数字签名密码应用技术要求
	应用指南	GB/T 38541—2020 信息安全技术 电子文件密码应用指南
		GM/T 0096—2020 射频识别防伪系统密码应用指南

表 1 GB/T 39786 框架下的系列密码应用标准列表

此外，一些相关的密码应用标准正在制订过程中，包括《信息系统密码应用设计指南》和《信息系统密码应用实施指南》等。随着标准化的逐步完善，可为信息系统责任单位提供更多、更有针对性、更细粒度的密码应用指导。

2.基于 GB/T 39786 的配套测评文件

为了配合 GB/T 39786 的实施，更好地指导和规范密评活动，中国密码学会密评联委会组织制定了《信息系统密码应用测评要求》、《信息系统密码应用测评过程指南》、《信息系统密码应用高风险判定指引》、《商用密码应用安全性评估量化评估规则》、《商用密码应用安全性评估报告模板（2020 版）》五个测评类指导性文件，并于 2020 年 12 月在国家密码管理局官方网站发布，标准化工作也在有序推进。这五个文件是基本与 GB/T 39786 同步制订的，都是依据 GB/T 39786 的最新指标要求展开，内部关系如下图所示。



《信息系统密码应用测评要求》依照 GB/T 39786，规定了信息系统不同等级密码应用的测评要求；

《信息系统密码应用测评过程指南》指导了信息系统密码应用的测评过程，包括测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动，规范了各项测评活动及其工作任务；

《商用密码应用安全性评估量化评估规则》《信息系统密码应用高风险判定指引》是《信息系统密码应用测评要求》的有力补充，充分体现了密评的“综合判定、保住底线”的思路。

《商用密码应用安全性评估报告模板（2020 版）》从结果规范角度给出了密评报告的模板，囊括了《信息系统密码应用测评要求》《商用密码应用安全性评估量化评估规则》《信息系统密码应用高风险判定指引》的相关内容。

3.GB/T 39786 与网络安全等级保护的关系

《密码法》第二十七条规定：“商用密码应用安全性评估应当与关键信息基础设施安全检测评估、网络安全等级测评制度相衔接，避免重复评估、测评”。这项规定决定了密码应用安全性评估与等级保护测评的衔接性。对于 GB/T 22239 中规定的安全要求，GB/T 39786 不再重复规定，而是聚焦在 GB/T 22239 未细致规定的密码应用方面，形成二者既相互补充，又可相互独立实施的格局。对于同时具备等级保护测评、密码应用测评资质的机构，可以充分协调两类评估活动，做到一次现场完成两类评估。

信息系统所应遵循的密码应用等级，目前是参照等保定级的。信息系统根据 GB/T 22240—2020《信息安全技术网络安全等级保护定级指南》[10]完成定级备案后，其密码应用等级也相应确定，即等保定级为第一级的对应第一级密码应用基本要求，等保定级为第二级的对应第二级密码应用基本要求，以此类推。从密评机构的视角来看，信息系统完成等保定级是启动密评的基础，密评对象的范围最好也与等保定级范围保持一致，以减少密评对象包含不同等级所带来的复杂性。

需注意的是，GB/T 22239 将等级保护要求进一步细分为信息安全类要求（S）、服务保证类要求（A）、其他安全保护类要求（G），等保定级对象可能出现不同类不同级的情况，例如 S2A3。整体的等保定级结果，是“就高不就低”的，例如对于 S2A3、S3A2，其整体网络安全保护等级都定为三级。目前，密评所参照的是整体网络安全保护等级，不去区分 S 和 A。

四、关于“应”“宜”“可”和不适用项的理解

GB/T 39786—2021 对于每一个密码应用要求项，采用“应”“宜”或“可”来表达不同的约束程度。国家标准 GB 1.1—2020《标准化工作导则第 1 部分：标准化文件的结构和起草规则》（以下简称 GB 1.1）[11]的附录 C 对“应”“宜”或“可”给出了解释：“应”表示应该、只准许，“宜”表示推荐、建议，“可”表示可以、允许。但对于信息系统责任单位而言，在制定密码应用方案时，如何综合考量“应”“宜”或“可”的要求项哪些需要响应，仅就 GB 1.1 的这个定义是难以明确的。

为此，《信息系统密码应用测评要求》从测评的角度出发，对测评实践中如何把握“应”“宜”或“可”进行了进一步解释：

——对于“可”的条款，由信息系统责任单位自行决定是否纳入标准符合性测评范围。

若纳入测评范围，则密评人员应按照第 6 章相应的测评指标要求进行测评和结果判定；否则，该测评指标为“不适用”。

——对于“宜”的条款，密评人员根据信息系统的密码应用方案和方案评审意见决定是否纳入标准符合性测评范围；若信息系统没有通过评估的密码应用方案或密码应用方案未做明确说明，则“宜”的条款默认纳入标准符合性测评范围。若纳入测评范围，则密评人员应按照第 6 章相应的测评指标要求进行测评和结果判定。否则，密评人员应根据信息系统的密码应用方案和方案评审意见，在测评中进一步核实密码应用方案中所描述的风险控制措施使用条件在实际的信息系统中是否被满足，且信息系统的实施情况与所描述的风险控制措施是否一致，若满足使用条件，该测评指标为“不适用”，并在密码应用安全性评估报告中体现核实过程和结果；若不满足使用条件，则应按照第 6 章相应的测评指标要求进行测评和结果判定。

——对于“应”的条款，密评人员应按照第 5 章和第 6 章相应的测评指标要求进行测评和结果判定；若根据信息系统的密码应用方案和方案评审意见，判定信息系统确无与某项或某些项测评指标相关的密码应用需求，则相应测评指标为“不适用”。

从上述文字可以看出，测评指标为“不适用”可能有以下 3 种情况：

（1）条款所对应的保护对象或安全需求不存在。例如对于“应采用密码技术保证设备中的重要信息资源安全标记的完整性”，如果不对信息资源设定安全标记，则本项的保护对象不存在，在测评时相应指标设定为“不适用”。

（2）根据信息系统的密码应用方案和方案评审意见确定是否作为“不适用”项。需要注意的是，这种“不适用”的情况仅针对“宜”的条款。当然，在这种情况下认定为“不适用”项，密评机构仍有责任进一步核实，若评估认为所描述的风险控制措施无效或不足以控制风险，则仍需将其纳入测评范围；

（3）由信息系统责任单位自行决定是否作为“不适用”项。需要注意的是，这种“不适用”的情况仅针对“可”的条款。信息系统责任单位具有自主选择权，鼓励但不强制采用密码技术满足对应要求。

五、GB/T 39786 的使用

GB/T 39786 既是密码应用的纲领性、框架性标准，也是安全性评估的顶层准则。本章站在应用单位和测评机构两个视角，来分别描述 GB/T 39786 的用途和用法，供各相关方在工作中参考。

1.信息系统责任单位如何使用 GB/T 39786

对于信息系统责任单位来说，GB/T 39786 是制订密码应用方案的直接依据。信息系统责任单位在充分明确自身信息系统业务需求、安全需求的基础上，制定采用密码技术满足安全需求的密码应用方案。对于方案，信息系统责任单位应进行标准符合性自查，结合等保定级情况，逐条对照 GB/T 39786 相应级别的要求，自查是符合、部分符合、不符合还是不适用。制定密码应用方案时要重点考虑以下几方面情况：

（1）等保定级的范围是什么。对于密码应用方案所涵盖的范围，应与等保定级范围一致，以便于等保测评与密评的协调开展。

（2）对于“宜”项，建议慎重考虑选择“不适用”。除非有非常过硬或不可抗力的理由外，一般建议遵循“宜”项，以避免信息系统安全的“木桶效应”。确需选择“不适用”，则应详细描述理由和替代性风险控制措施，供方案评估时参考。一般来讲，“宜”的条款“不适用”的理由可以是：

保护对象不存在或安全需求不存在。例如信息系统不对信息资源设定安全标记，则自然不需要遵循“应采用密码技术保证设备中的重要信息资源安全标记的完整性”。

限于技术、管理、业务、环境上的条件约束，难以甚至无法采用密码技术。对于这类情况，要详细说明客观原因和密码技术以外的风险控制措施。

（3）不要忽视管理要求。从长期看，信息安全保障是管理因素大于技术因素的，要从信息系统风险控制的角度，结合业务过程充分、周全考虑并切实落实 GB/T 39786 所规定的管理制度、人员管理、建设运行、应急处置四个方面的管理要求。如果在组织管理、操作规程、人事管理、信息安全管理等制度中已经涉及到所要求的方面，则不必刻意单独为密码管理制定制度文件，而在相应的制度文件中补充体现密码管理的要求即可。

（4）务必重视密钥管理。如前所述，密钥安全是密码应用安全的重中之重，要在密码应用方案中以单独章节描述各个层面密码应用所涉及的密钥，明确其种类和生命周期过程保护措施，以及所涉及的密码设备。系统建设过程中，要制定密钥管理制度，清晰说明密钥管理的规则、相关方及其职责，在密钥各生命周期环节的操作规程，以及违反操作规程的惩处措施等。

2.密评机构如何使用 GB/T 39786

对于密码应用安全性评估机构来说，GB/T 39786 的直接作用是在“规划”阶段用来评估密码应用方案的合规性，以及指标条款的适用性，《信息系统密码应用测评要求》也是基于 GB/T 39786 的指标给出测评实施和结果判定等要求。因此 GB/T 39786 是密评机构开展密评工作的基础性标准。

根据信息系统的密码应用方案和方案评审意见，若通过评估的密码应用方案中的要求，高于信息系统相对应的密码应用基本要求等级的指标要求，则应按照密码应用方案中的要求进行测评。例如，根据密码应用需求，对网络安全保护等级第三级的信息系统，选取了网络安全保护等级第四级信息系统的相关指标要求。对上述特殊情况进行测评实施的结论应体现在密码应用安全性评估报告中。

信息系统的商用密码应用测评的最终输出是密码应用安全性评估报告，在报告中应给出各个测评单元（见《测评要求》第 6 章）的测评结果、整体测评结果（见《测评要求》第 7 章），以及在进行风险分析和评价（见《测评要求》第 8 章）后给出的测评结论（见《测评要求》第 9 章）。其中，整体测评结果是以测评单元的判定结果为基础，经单元间、层面间测评相互弥补后得出的纠正结果；风险分析和评价是对整体测评结果中的不符合项和部分符合项，判断信息系统密码应用在合规性、正确性和有效性方面的不符合所产生的安全问题被威胁利用后对信息系统造成影响的程度；测评结论是由综合得分以及风险分析和评价共同决定，表示信息系统达到相应密码等级保护要求的程度。（作者：商密君）

➢ 依法治理 APP 过度索权是强化个人信息安全的基础

近日，国家四部委联合下发了《常见类型移动互联网应用程序必要个人信息范围的规定》，对 39 款常见 App 在使用过程中，对必要个人信息采集类型做出了具体规定。

当前，我国以《网络安全法》《民法典》《刑法》及其司法解释为核心的个人信息保护体系已经建立，《个人信息保护法（草案）》也开始向社会公开征求意见。不过，立法条文的相对抽象，距具体落实在特定 APP 应用尚存一定距离，新规通过类型化的方式，将具体应用与抽象规定相结合，对未来个人信息保护将起到重要抓手作用。

互联网实践中，利用 APP 对消费者个人信息过度索权的情况非常普遍，主要包括三个方面：一是，通过网民协议格式条款，甚至具有市场支配地位的平台通过霸王条款，强制消费者“同意”对自己个人信息的无限制索取。二是，通过技术手段、技术迭代、大数据幌子等方式，掩盖过度获取个人信息目的，消费者维权成本很高，违法成本较低。三是，大量不法 APP 通过过度索权，形成了个人信息黑产，导致个人信息被不法分子利用，精准诈骗、撞库窃取、人肉搜索等互联网犯罪行为屡见不鲜。

此外，个别 APP 平台忽视承担起主体责任，“谁采集，谁负责”的法律责任体系没有被好好落实，个人信息在采集层面、使用层面、保护层面和处分层面都存在巨大安全隐患。以往执法实践更重视个人信息的使用、保护、处分和事后处罚，忽视了个人信息违法采集的前期责任。其实，从治理成本、执法效率角度看，在个人信息采集层面治理下的功夫越大，后续风险就会变得越小。因此，新规将执法层面前移，从采集个人信息范围角度加大治理力度，保护个人信息。

个人信息安全的治理工作不能过度依靠企业自律和事后执法处罚。平台自律应有法律法规作为基础，只有在足够具体、有效和针对性的规则面前，自律才会在个人信息保护中起到应有的效果。新规把实践中 39 款 APP 对个人信息索权类别，以非常简练、具体、明确的方式作出了规定，旨在督促平台尽到依法、依约采集个人信息的责任，目的在于强化平台作为信息采集者的主体责任，切实保护消费者个人信息的安全。

各部门在对个人信息保护监管工作中，很难判断某款 APP 采集个人信息范围的必要性、正当性和合法性具体边界。执法和司法都面临对个人信息采集类型、范围、边界判断困难的情况，这就导致对个人信息保护工作多集中在事后追责，缺乏技术监管的预判。

新规出台目的就是要进行“穿透式”监管，从个人信息采集源头抓起。这就需要 APP 设计者、开发者、经营者、所有者与使用者都必须严格按照规定，落实采集类型和范围责任，明确采集的必要性、正当性，只有达到新规具体标准，才能符合合法性基本原则。换言之，如果平台没有履行新规相关标准，即便采集的信息事先“获取”了消费者同意，或没有对采集的个人信息进行滥用，也不能以此进行抗辩。

值得注意的是，新规不仅列明了各款 APP 个人信息采集类别，而且还明确规定，任何组织和个人都有权利向相关部门进行举报，这就畅通了公众对个人信息安全监督的权利，也拓展了相关部门对保障个人信息安全的治理渠道，反过来，也更加夯实了互联网平台积极履行主体责任的必要性。（来源：光明日报）

四、政府之声

➢ 中阿发布数据安全合作倡议

2021 年 3 月 29 日，中华人民共和国外交部与阿拉伯国家联盟秘书处共同主持召开中阿数据安全视频会议。双方及阿盟成员国负责网络和数字事务官员出席对话。阿方欢迎中方提出《全球数据安全倡议》，支持秉持多边主义、兼顾安全发展、坚守公平正义的原则，共同应对数据安全风险挑战。**双方一致认为:**


English Français Español Русский عربي

外交部

首页 外交部长 外交部 外交动态 政府信息公开 驻外机构 国家和组织 资料 服务 移动客户端

首页 > 资料 > 声明公报

中阿数据安全合作倡议

2021-03-29

[字体: 大 中 小] 打印本页

2021年3月29日，中华人民共和国外交部与阿拉伯国家联盟秘书处共同主持召开中阿数据安全视频会议。双方及阿盟成员国负责网络和数字事务官员出席对话。阿方欢迎中方提出《全球数据安全倡议》，支持秉持多边主义、兼顾安全发展、坚守公平正义的原则，共同应对数据安全风险挑战。双方一致认为:

信息技术革命日新月异，数字经济蓬勃发展，深刻改变着人类生产生活方式，对各国经济社会发展、全球治理体系、人类文明进程影响深远。

信息技术革命日新月异，数字经济蓬勃发展，深刻改变着人类生产生活方式，对各国经济社会发展、全球治理体系、人类文明进程影响深远。

作为数字技术的关键要素，全球数据爆发增长，海量集聚，成为实现创新发展、重塑人们生活的重要力量，事关各国安全与经济社会发展。

在全球分工合作日益密切的背景下，确保信息技术产品和服务的供应安全对于提升用户信心、保护数据安全、促进数字经济发展至关重要。

呼吁各国秉持发展和安全并重的原则，平衡处理技术进步、经济发展与保护国家安全和社会公共利益的关系。

重申各国应致力于维护开放、公正、非歧视性的营商环境，推动实现互利共赢、共同发展。与此同时，各国有责任和权利保护涉及本国国家安全、公共安全、经济安全和社会稳定的重要数据及个人信息安全。

欢迎政府、国际组织、信息技术企业、技术社群、民间机构和公民个人等各主体秉持共

商共建共享理念，齐心协力促进数据安全。

强调各方应在相互尊重基础上，加强沟通交流，深化对话与合作，共同构建和平、安全、开放、合作、有序的网络空间命运共同体。

为此，双方倡议：

——各国应以事实为依据全面客观看待数据安全问题，积极维护全球信息技术产品和服务的供应开放、安全、稳定。

——各国反对利用信息技术破坏他国关键基础设施或窃取重要数据，以及利用其从事危害他国国家安全和社会公共利益的行为。

——各国承诺采取措施防范、制止利用网络侵害个人信息的行为，反对滥用信息技术非法采集他国公民个人信息。

——各国应要求企业严格遵守所在国法律。各国应尊重他国主权、司法管辖权和对数据的安全管理权，未经他国法律允许不得直接向企业或个人调取位于他国的数据。

——各国如因打击犯罪等执法需要跨境调取数据，应通过司法协助渠道或其他相关多双边协议解决。国家间缔结跨境调取数据双边协议，不得侵犯第三国司法主权和数据安全。

——信息技术产品和服务供应企业不得利用其产品和服务非法获取用户数据、控制或操纵用户系统和设备。

——信息技术企业不得利用用户对产品依赖性谋取不正当利益，强迫用户升级系统或更新换代。产品供应方承诺及时向合作伙伴及用户告知产品的安全缺陷或漏洞，并提出补救措施。

双方呼吁各国支持并通过双边或地区协议等形式确认上述承诺，呼吁国际社会在普遍参与的基础上就此达成国际协议。欢迎全球信息技术企业支持本倡议。（来源：中华人民共和国外交部）

➢ 工信部发文：智能网联汽车不得泄露敏感信息

2021 年 4 月 7 日，为加强道路机动车辆生产企业及产品准入管理，推动智能网联汽车产业健康有序发展，工信部装备工业一司组织编制了《智能网联汽车生产企业及产品准入管理指南(试行)》(征求意见稿)(以下简称《意见稿》)。

意见提到，智能网联汽车生产企业应依法收集、使用和保护个人信息，实施数据分类分

级管理，制定重要数据目录，不得泄露涉及国家安全的敏感信息。在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当按照有关规定在境内存储。因业务需要，确需向境外提供的，应向行业主管部门报备。

此外，智能网联汽车产品应明确驾驶自动化功能及其设计运行条件。设计运行条件应包括设计运行范围、车辆状态、驾乘人员状态及其他必要条件;设计运行范围应包括但不限于道路、交通、电磁环境、天气、光照等。

值得注意的是，特斯拉近日因“车内摄像头”登上微博热搜，该视频是黑客提取到的特斯拉车内摄像头拍摄的白天画面。据了解，该视频画面引起了网友广泛的讨论，但特斯拉官方表示：目前该驾驶室摄像头在北美以外的市场并没有激活。此外，新华社对特斯拉车内摄像头事件也做出回应：“车内隐私不是你想采就采。”（来源：工信部）

- **《智能网联汽车生产企业及产品准入管理指南（试行）》（征求意见稿）全文：**
- https://www.miit.gov.cn/jgsj/zbys/qcgy/art/2021/art_67412baef004441a9cafe0a440a928a2.html

➢ 《系统重要性银行附加监管规定（试行）（征求意见稿）》公开征求意见

2021 年 4 月 2 日，为完善我国系统重要性金融机构监管框架，加强宏观审慎管理，中国人民银行、银保监会日前公布了《系统重要性银行附加监管规定（试行）（征求意见稿）》（以下简称《附加监管规定》），通过明确相关要求，鼓励银行降低系统性风险，提高自救能力，防范“大而不能倒”风险。

2020 年 12 月，人民银行、银保监会联合发布了《系统重要性银行评估办法》。为平稳启动系统重要性银行名单评估与后续监管工作，两部门拟出台附加监管规定，建立附加资本、附加杠杆率、流动性、大额风险暴露等附加监管指标体系，明确审慎监管要求等，并向社会公开征求意见。

《附加监管规定》分为总则、附加监管要求、恢复与处置计划、审慎监管、附则等五章，共二十二条。

《附加监管规定》借鉴国际经验，建立附加资本、附加杠杆率、流动性、大额风险暴露等附加监管指标体系。为鼓励银行降低系统性风险，避免引发道德风险，系统重要性银行第一组到第五组的银行分别适用 0.25%、0.5%、0.75%、1%和 1.5%的附加资本要求。系统重要性银行需在进入名单或者得分变化导致组别上升后，经过一个完整自然年度后的 1 月 1 日满足要求。除第五组外，第一组到第四组组间的附加资本要求仅差 0.25%，组内暂不设置差异化的附加资本要求。人民银行、银保监会后续可以根据实际情况对附加资本要求进行调整，报国务院金融稳定发展委员会审议后实施。需要说明的是，本规定中系统重要性银行的附加资本要求与宏观审慎评估（MPA）中的附加资本要求不互相替代。

此外，《附加监管规定》将恢复计划与处置计划（又称“生前遗嘱”）作为系统重要性银行附加监管的一项重要工具。恢复计划需详细说明银行如何从早期危机中恢复，确保能在满足事先设定的触发条件后启动和执行。处置计划需详细说明银行如何在无法持续经营时安全、快速、有效处置，保障关键业务和服务不中断，避免引发系统性风险。在制定计划时，系统重要性银行要全面梳理重要实体、关键业务和自救资源，增加总损失吸收能力的要求，保障机构拥有充足的自救资源。通过恢复与处置计划的制定和审查，系统重要性银行要全面梳理风险领域和薄弱环节，提高透明度、降低复杂性，提高自救能力，防范“大而不能倒”

风险。（来源：金融时报）

- **关于《系统重要性银行附加监管规定（试行）（征求意见稿）》公开征求意见的通知**
- **全文：**http://www.pbc.gov.cn/rmyh/105208/4222909/index.html

➢ 最高检：2020 年检察机关起诉涉嫌网络犯罪人数上升近五成

2021 年 4 月 7 日，中华人民共和国最高人民检察院发布当前，电信网络诈骗案件高位运行，网络赌博犯罪案件上升明显，网络犯罪黑灰产业生态圈逐步形成并发展。来自最高检统计数据显示，2020 年，全国检察机关起诉涉嫌网络犯罪（含利用网络和利用电信实施的犯罪及其上下游关联犯罪）14.2 万人，同比上升 47.9%。当前，传统犯罪加速向网络空间蔓延，特别是利用网络实施的诈骗和赌博犯罪持续高发，2020 年已占网络犯罪总数的 64.4%。随机诈骗与精准诈骗相互交织，冒充公检法人员诈骗、交友诈骗、退款诈骗、信用卡贷款提额诈骗、刷单诈骗等较为突出。为赌博网站“洗白”资金的“跑分平台”、非法收集公民个人信息的“流氓软件”、扰乱网络市场秩序的“恶意刷单”等案件层出不穷。

最高检披露，规模庞大的地下黑灰产业密切配合，为网络犯罪持续“输血供粮”，成为该类犯罪多发高发的重要原因。网络犯罪往往形成较为固定的犯罪利益链条：上游为犯罪团伙提供技术工具、收集个人信息等；中游实施诈骗或开设赌场等网络犯罪；下游利用支付通

道“洗白”资金。数据显示，有近四分之一的网络诈骗是在获取公民个人信息后“精准出手”，有针对性实施犯罪，侵犯公民个人信息已成为网络犯罪黑灰产业的关键环节。

另外，网络犯罪集团化、跨境化特征凸显，犯罪主体呈现低年龄、低学历、低收入的“三低”趋势，老年人与年轻人更易成为受害对象。

2020 年，最高检成立惩治网络犯罪、维护网络安全研究指导组，统筹协调做好深化打击治理网络犯罪各项工作，全面加强惩治网络犯罪的研究和指导。最高检还向工业和信息化部发出第六号检察建议，围绕网络黑灰产业链条整治、APP 违法违规收集个人信息、未成年人网络保护等问题，提出治理建议等。

各地检察机关对严重影响人民群众安全感的网络犯罪保持严惩态势。针对电信网络诈骗、网络赌博等持续多发高发态势，积极参与打击整治非法开办贩卖电话卡、银行卡的“断卡”专项行动，打击治理跨境赌博专项行动等；针对假借“创新”名义在网络上实施的金融犯罪，穿透网络技术表象，实施精准打击，防范金融风险；针对网络诽谤等严重扰乱网络社会公共秩序行为，建议公安机关对“杭州女子取快递被造谣案”立案侦查，自诉转公诉；针对网络黑灰产业链条长、分工细等特征，突出打击重点，深挖上下游关联犯罪，有力斩断犯罪利益链条。

信息网络技术的高速发展深刻影响着社会发展，与此同时，犯罪活动日益向网络空间滋生蔓延，国家安全、经济发展和社会稳定面临新的挑战。2020 年，全国检察机关起诉涉嫌网络犯罪（含利用网络和利用电信实施的犯罪及其上下游关联犯罪）14.2 万人，同比上升 47.9%，有力维护了网络秩序。（来源：中华人民共和国最高人民检察院）

- **2020 年检察机关起诉涉嫌网络犯罪人数上升近五成**
- **全文：**https://www.spp.gov.cn/spp/xwfbh/wsfbt/202104/t20210407_514984.shtml#1

五、本期重要漏洞实例

➢ Google Android Framework 权限提升漏洞

发布日期：2021-3-29
更新日期：2021-3-29
受影响系统：
Google Android 8.1
Google Android 9
Google Android 10
描述：

CVE(CAN) ID: CVE-2021-0302
Android 是美国 Google 公司和开放手持设备联盟（简称 OHA）共同开发的一套以 Linux 为基础的开源操作系统。Google Android 8.1、9、10 中的 Framework 组件存在权限提升漏洞。攻击者可利用该漏洞会导致本地特权升级
建议：

厂商已发布了漏洞修复程序，请及时关注更新：

https://source.android.com/security/bulletin/2021-02-01

➢ Microsoft Internet Explorer VBScript Engine 远程代码执行漏洞

发布日期：2021-3-31
更新日期：2021-3-31
受影响系统：
Microsoft Internet Explorer 9
Microsoft Internet Explorer 11
描述：

CVE(CAN) ID: CVE-2020-1214
Microsoft Internet Explorer（IE）是美国微软（Microsoft）公司的一款 Windows 操作系统附带的 Web 浏览器。VBScript Engine 是其中的一个 VBScript 脚本语言引擎。Microsoft Internet Explorer 9 版本和 11 版本的 VBScript Engine 中处理内存对象的方式存在远程代码执行漏洞，攻击者可借助特制网站利用该漏洞在当前用户的上下文中执行任意代码，导致内存损坏。
建议：

厂商已发布了漏洞修复程序，请及时关注更新：

https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1214

➢ Cisco Jabber 代码执行漏洞

发布日期：2021-04-2
更新日期：2021-04-2
受影响系统：
Cisco Jabber for Windows <12.1.5
Cisco Jabber for Windows >=12.5.0，<12.5.4
Cisco Jabber for Windows >=12.6.0，<12.6.5
Cisco Jabber for Windows >=12.7.0，<12.7.4
Cisco Jabber for Windows >=12.8.0，<12.8.5
Cisco Jabber for Windows >=12.9.0，<12.9.5
描述：

CVE(CAN) ID: CVE-2021-1411
Cisco Jabber 是一个网络会议和即时消息传递应用程序，允许用户通过可扩展消息传递和状态协议（XMPP）发送消息。Cisco Jabber 存在代码执行漏洞，该漏洞源于邮件内容验证错误引起的。攻击者可以利用该漏洞通过向受影响的软件发送特制的 XMPP 消息，在目标系统上执行任意程序。
建议：

厂商已发布了漏洞修复程序，请及时关注更新：
https://www.webex.com/downloads/jabber.html

➢ Invigo Automatic Device Management SQL 注入漏洞

发布日期：2021-03-29
更新日期：2021-03-29
受影响系统：
Invigo Automatic Device Management <=5.0
描述：

CVE(CAN) ID: CVE-2020-10582
Invigo Automatic Device Management (ADM)是一款供手机运营商使用的本地管理工具，使运营商能够以低成本和高度的可靠性检测、维护和管理数百万台设备。Invigo Automatic Device Management 5.0 及更早版本中的/admin/display_errors.php 存在 SQL 注入漏洞。远程攻击者可利用该漏洞在数据库中执行任意 SQL 查询。
建议：

厂商已发布了漏洞修复程序，请及时关注更新：
https://www.on-x.com/sites/default/files/security_advisory_-_multiple_vulnerabilities_-_invigo_adm.pdf

六、本期网络安全事件

➢ 黄牛外挂软件侵入上海交警 APP：为约考试场次

2021 年 3 月 27 日，一早黄牛外挂软件侵入上海交警 APP 冲上微博热搜，黄牛胆大包天的操作引发网友围观。上海的老司机们都知道，如果在上一年度因为违章被扣满了 12 分，按照规定，在进行重新学习并在现场教育点进行业务受理后，只要通过“上海交警 APP”线上预约驾驶员满分考试并合格，便能重新取得驾照了。但如果考试场次都约满了怎么办？有人竟动起了歪脑筋！近期，有驾驶员在网上搜到一家网店，网店称只要花 900 元就能约到已经约满的考试场次。

开发外挂软件，黄牛“偷梁换柱”

网店的店家刘某是一名从事非法代办车驾管等业务的黄牛。一次，客户提出预约满分考试需求，他想到曾在黄牛群里看到可以用外挂软件抢名额，便想着开发一个自动抢名额的软件赚钱。他在微信好友里找了一个开发软件的人进行研发，两三天后，一款名为“抢课”APP 的软件就诞生了。在刘某的要求下，该好友不断对抢号软件进行技术升级，加入“换号”功能使成功率大幅提高。什么是“换号”功能呢？顾名思义，就是把已经预约成功的人的号换掉。

“这款 APP 可以绕过验证过程，直接跳到预约的最后一步。也就是说，可以先写入虚假

身份信息占用预约位置，然后再替换上真实的客户信息。”刘某说，用来占位的虚假身份证号都是他随便编的。

中介提供客源，两人联手牟利

有了软件，刘某在一个驾驶业务微信群里发布广告寻找客源，闵某很快找上了门。闵某也在做帮人预约满分考试的生意，但他的外挂软件成功率不高，也没法预约到 7 天内的考试。看到刘某的广告，闵某就把自己搞不定的十几单业务给了刘某，从中收取中介费，这些生意刘某都做成了。之后，只要碰到自己搞不定的客户，闵某就会介绍给刘某。两人熟悉后，刘某告诉闵某，自己之所以成功率高，都是因为有一款神器 APP 相助，他同时表示可以把该款 APP 有偿提供给闵某，大家有钱一起赚。为了表示诚意，刘某还把 APP 的初代版本给了闵某。虽然最后没谈妥，但闵某自己用刘某提供的 APP 也做了十几单生意。

疯狂“占坑”后事发，已被批捕

有了软件和客源，刘某使用“抢课”APP 一口气占用了同一天考试里两个考场约 90 个位子，做成了约 40 单。过了几天后，刘某发现剩下的坑已被后台清除掉了，猜测可能事情败露了。今年 1 月 15 日，民警在日常维护中发现，“上海交警”APP 遭人非法入侵，驾驶证满分考试模块中有大量异常数据，导致正常用户无法使用，造成经济损失 1.2 万余元。立案侦查后，公安机关先后抓获了刘某、闵某。

浦东检察院经审查后认为，刘某、闵某违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，涉嫌破坏计算机信息系统罪，于近日对刘某、闵某作出批准逮捕决定。（来源：澎湃新闻）

➢ 美国脸书公司 5.33 亿用户数据遭泄露

2021 年 4 月 4 日，近日，美国社交媒体脸书(Facebook)超 5 亿用户的个人数据遭到泄露，包括电话号码、电子邮件等信息。俄媒称，脸书创始人扎克伯格的电话号码也遭泄露。据新闻网站商业内幕(Business Insider)报道，一个低级别的黑客论坛 3 日曝光了 5.33 亿脸书用户的个人数据，这些用户涉及 106 个国家，泄露的信息包括脸书 ID、用户全名、位置、生日、个人简介以及电子邮件地址。

令大众吃惊的是，公布的这些个人隐私信息数据涉及来自 106 个国家的 5.33 亿 Facebook 用户，其中包括 3200 万美国用户，1100 万英国用户，600 万印度用户。俄罗斯

卫星通信社 4 日报道，遭泄露的 5.33 亿脸书用户数据中包含一些名人的信息，扎克伯格的电话号码也在其中。有消息称，遭泄露的电话号码与扎克伯格的真实号码是一致的。网络犯罪情报公司 Hudson Rock 的首席技术官加尔首先发现了脸书用户数据泄露，通过比对他所认识的人的信息，证实至少有一部分内容是真实的。事发后，脸书公司在 4 月 3 日的一份声明中称，上述数据来自 2019 年发生的信息泄露事件，当年 8 月已经进行修复。

脸书已经不止一次发生用户信息泄露事件

此前，Facebook 曾将 8000 万用户数据与剑桥分析公司(Cambridge Analytica)进行分享，而后者则将这些数据用于 2016 年美国大选政治广告，这严重违反了 Facebook 的服务条款。扎克伯格承认对此事负有责任并道歉。随后，美国联邦贸易委员会对此事展开调查，并对脸书开出 50 亿美元罚单。

国际上也有应对此事的相关法律条令和组织，例如 GDPR 通用数据保护条例，是欧盟议会和欧盟理事会在 2016 年 4 月通过，在 2018 年 5 月开始强制实施的规定。

GDPR 版强制执行隐私条例，规定了企业了在对用户的数据收集、存储、保护和使用时新的标准;另一方面，对于自身的数据，也给予了用户更大处理权。GDPR 虽然保护范围只在于欧洲生活的人民，但因为考虑到「全球性」是写入互联网基因内的属性，几乎所有的服务都会受到影响，所以生活在欧洲之外的人其实也会从此条例中获益。据公开信息纰漏，如果 2018 年脸书的“剑桥分析事件”发生在了 GDPR 的管辖范围之内，则其可能被处罚 1700 万英镑或全球营业额 4%的巨额罚款。（来源：参考消息）

➢ 澳洲联邦银行发生大规模技术故障 有人被二次收费有人却被清空房贷

2021 年 4 月 1 日报道，联邦银行(Commonwealth bank)出现了大规模的技术故障，致使许多用户受到了不同程度的影响。

据第七新闻 1 日报道，悉尼、墨尔本、布里斯班和珀斯等主要城市都因此受到了影响。从 2 日下午 4 时开始，银行就受到了各种各样的投诉，据悉，当时有超过 3000 次的服务中断。为此，联邦银行在社交媒体平台推特(Twitter)上发表声明称：“我们知道一些客户在访问我们的服务时遇到了困难，我们正在进行紧急调查和处理。我们为此感到十分抱歉，感谢您的耐心等待，我们会很快提供最新消息。”

联邦银行表示：此次技术故障问题主要集中在使用 NetBank 服务的客户，即该公司的网上银行。其中一位顾客表示，由于该故障的出现，他在购物时被收取了两次费用。联邦银行则向用户保证：“如果您因为这个技术问题而产生了费用，请您在设备恢复后或您方便的时候拨打 132221 电话，我们会为您解决问题。”而另一名用户表示，他当时的网络银行账户已经完全消失，这让他们感到“不安和不便”。另外由于目前的故障，一些联邦银行客户担心无法在商场的收银台处支付费用，尤其是在复活节期间。还有一名客户表示，在该技术故障下，他的房屋款消失了。他指出，这或许对他而言并不是一个坏结果。（来源：第七新闻）

➢ 全国最大销售外挂“海贼王”软件案宣判，主犯获刑 10 年！

2021 年 3 月 31 日，广州市南沙区人民法院公开宣判了一起销售微信外挂软件“海贼

王”的违法案件。据法院调查，2018 年 3 月，陈某展让陈某巍和王某帮他开发微信外挂软件，王某在陈某巍提供的微信底层接口协议基础上，编写了“黑客数据助手”、“黑客检测助手”、“黑客销售助手”等系列软件。2019 年春节后，其为了扩大犯罪规模，对上述软件进行包装并更名为“海贼王”，并形成了一条该软件销售黑产业链。

该产业链分为三层，上层为陈某展等 3 人，负责软件开发并把软件放到网站供下载。该软件使用需要授权码，该团伙通过售卖授权码和收取销售代理费盈利。中层是软件代理商梁某等 10 人，向上层获取代理资格，低价批量购买授权码然后卖给微信号商。下层为微信号商龚某等 31 人，主要向中层购买授权码，利用该软件进行“养号”和“卖号”业务。据悉，团队核心陈某展在此案中获利高达 427940 元。

“海贼王”外挂软件能够代替人工对微信界面进行操作，不法分子利用该软件侵入和控制微信计算机信息系统，批量登入登出微信账号，修改密码，窃取账号信息数据，完成“养号”和“卖号” 等行为。

本案中，被告梁某伦、陈某展判处有期徒刑十年、八年六个月，并处罚金人民币十一万六千元、十三万二千元，其他 36 名被告人分别被判处有期徒刑八年至六个月不等，并分处 149000 元至 2000 元的罚金。

南沙法院审理认为，根据审理查明的事实和证据，被告人陈某展、梁某伦等人无视国家法律，违反国家规定，提供专门用于侵入、非法控制计算机信息系统的程序、工具;侵入深圳腾讯计算机信息系统，获取计算机信息系统中的数据、且对腾讯计算机信息系统进行

非法控制;向他人出售或非法获取公民个人信息，其行为均已触犯刑律。犯提供侵入、非法控制计算机信息系统程序、工具罪，非法获取计算机信息系统数据、非法控制计算机信息系统罪，侵犯公民个人信息罪，遂依法作出上述判决。经办法官表示，这些外挂软件的出现，对正常微信用户会造成骚扰和恶意影响。法院对于开发、销售此类非法软件的行为将依法予以惩处。（来源：中国法院网）

➢ 内鬼、外鬼相互勾结非法获取某集团计算机业务数据获刑

2021 年 4 月 10 日据梅州蕉岭公安报道，近日，蕉岭公安在“净网”行动中闪电出击，快速打掉一个“黑客”作案团伙，侦破内鬼、外鬼相互勾结非法获取梅州某集团公司计算机业务系统数据而获取利益的案件，抓获作案团伙成员徐某、田某、詹某、彭某等多名犯罪嫌疑人，扣留作案工具一批。

“黑客”攻击公司经济声誉双受损

2020 年 12 月 24 日，梅州市某集团公司向蕉岭县公安局报警，称其公司互联网计算机物资招采平台被人非法侵入获取、修改数据，作案时间长达三年，对公司造成经济、名誉和

信誉上的巨大损失。接报后，办案部门立即对该公司信息中心机房进行调查取证。但由于该公司的物资招采平台存在较大漏洞，操作日志数据留存不够完善，不能从相关台账找寻到黑客的踪迹，侦破一时陷入困境。

数据技术支撑细致侦查露端倪

办案民警并没有因此气馁，“如果此案是内外勾结作案，那么内部人员与外界肯定有频繁联系并留下痕迹。”于是决定从该公司业务系统和相关内部人员展开侦查。通过大数据智能化技术对可疑人员进行排查时，办案民警发现徐某的日常活动比较可疑，经常出入与其收入水平严重不符的高级酒店。警方循线深入侦查发现，徐某与该集团公司已离职信息化工程师田某交往密切，且两人在警方介入侦查后更为反常，另用其他电话号码进行联系。

通过侦查，办案民警又发现，居住在广州市增城区的田某具备作案条件，很可能就是网上远程操作的“黑客”。紧接着，民警顺藤摸瓜，发现田某与梅州本地某公司供应商彭某联系比较密切，综合分析整个案情，初步判断徐某、田某、彭某等人为该案犯罪嫌疑人，是“内鬼”“外鬼”相互勾结，协同作案的团伙。

结伙营私事发“内鬼”“外鬼”同落网

在蕉岭警方进入该公司侦查此案的消息传开后，为防止犯罪嫌疑人销毁证据、逃跑藏匿，办案部门兵分三路，迅速对嫌疑人实施抓捕和搜索固定证据行动。在广州增城警方支持下，2 月 5 日，在田某住处顺利抓获嫌疑人田某、詹某（田某前妻）。同时，通过技术侦查，发现另外两名犯罪嫌疑人徐某和彭某分别居住在蕉岭长潭镇和梅县区华侨城，警方快速出击，同步实施抓捕，顺利地将嫌疑人徐某、彭某（供应商）抓捕归案。

经审讯，徐某、田某、彭某等犯罪嫌疑人供认，自 2018 年 11 月至 2020 年 12 月份以来，结成团伙、内外勾结，协同作案，由田某、詹某夫妻在家里通过远程控制手段，打开预留好的该集团公司业务系统的“后门”，侵入到该公司计算机业务系统，非法获取供应商招投标报价数据后提供给多个供应商，从中牟取利益的犯罪事实。由于田某的“协助”，多家供应商利用报价数据调整自家公司在该集团公司物资招采平台中的报价为最低价，中标后获取利益。另查明，犯罪嫌疑人徐某利用其在该公司物资供应部员工的身份，在合同签订、发票开具及货款结算时为物资供应商提供便利，向安徽省某输送设备有限公司、梅州市某节能环保技术服务有限公司及惠州市某贸易有限公司等多家供应商索取好处费人民币近 7 万元，涉嫌非国家工作人员受贿罪。

违规开“后门”为己开“狱门”

“黑客”田某是怎么做到的呢？原来，田某在该集团公司上班时，为方便自己在家里加

班做事，在公司计算机业务系统开了个“后门”。2016 年辞职后，想不到这个“后门”为其充当“黑客”赚钱提供了条件，通过这个“后门”为其搜集公司招投标数据和更改数据提供了便利。尽管田某技术再高明，也逃不过蕉岭网警智慧的眼睛，陷入法网囹圄。

犯罪嫌疑人徐某与田某、詹某约定，事成后从供应商处获得的好处费五五分成，徐某通过从田某、詹某处获取的该上市公司物资招采平台中数据，提供给供应商获利 5 万多元好处费，按约定支付给犯罪嫌疑人田某及詹某好处费人民币近 3 万元。田某、詹某夫妻又将商业情报卖给供应商彭某。犯罪嫌疑人彭某通过田某、詹某处获取该集团物资招采平台供应商数据，从而调整其经营的梅县区某公司报价中标获利金额人民币近 10 万元，支付给犯罪嫌疑人田某及詹某好处费约人民币 6 万多元。

犯罪嫌疑人徐某、田某、彭某、詹某等的违法行为，严重扰乱了正常的市场经济秩序，违背了该公司“公平、公正、公开”阳光采购制度，给该公司造成声誉上损害及经济上损失。

（来源：梅州公安）

➢ 5 亿 LinkedIn 用户倒霉 个人信息泄露

2021 年 4 月 9 日，据 Cyber News 报道，LinkedIn 信息大规模泄露，影响 5 亿用户，目前信息已经被攻击者拿到网上出售。

LinkedIn 新闻发言人证实，出售的信息的确来自 LinkedIn。LinkedIn 新闻发言人在声明中表示：“我们正在调查，网上发布的数据集看起来包含 LinkedIn 公开可浏览信息，还包括来自其它网站或者企业的聚合信息。从 LinkedIn 收集会员数据违反我们的服务条款，我们

一直在努力，希望保护好会员和会员数据。”

目前 LinkedIn 约有用户 7.4 亿，也就是说受影响的用户约占总用户数的三分之二。泄露的信息包括用户 ID、名称、邮件地址、手机号码、工作信息、性别、其它社交媒体账户。

攻击者在黑客论坛出售数据，他提供 200 万条记录作为样本。Cyber News 研究人员证实数据的确来自 LinkedIn 用户，但他们提醒说信息可能来自旧档案，并非最近的资料。

安全情报公司 IntSights 的分析师保罗·普鲁德霍姆（Paul Prudhomme）指出，泄露的数据影响巨大，因为作恶者可以利用员工信息攻击企业。普鲁德霍姆说：“大流行期间，越来越多的员工远程办公，家庭、个人设备使用频率增加，类似的攻击可能性提升。通过员工个人账户和设备攻击企业，这是攻击者绕开企业网络安全防御屏障的一种方式。”就在几天前 Facebook 刚刚证实泄露大量数据，影响 5.3 亿用户。（来源：新浪科技）