国盟信息安全通报

2020 年 3 月 02 日第 210 期

全国售后服务中心

国盟信息安全通报

（第 210 期）

国际信息安全学习联盟

2020 年 03 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 514 个，其中高危漏洞 200 个、中危漏洞 271 个、低危漏洞 43 个。漏洞平均分值为 6.35。本周收录的漏洞中，涉及 0day 漏洞 233 个（占 45%），其中互联网上出现“Wordpress 插件 contact-form 远程文件上传漏洞、Kyrol Internet Security 无效指针漏洞”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 4336 个，与上周（4121 个）环比增加 5%。

主要内容

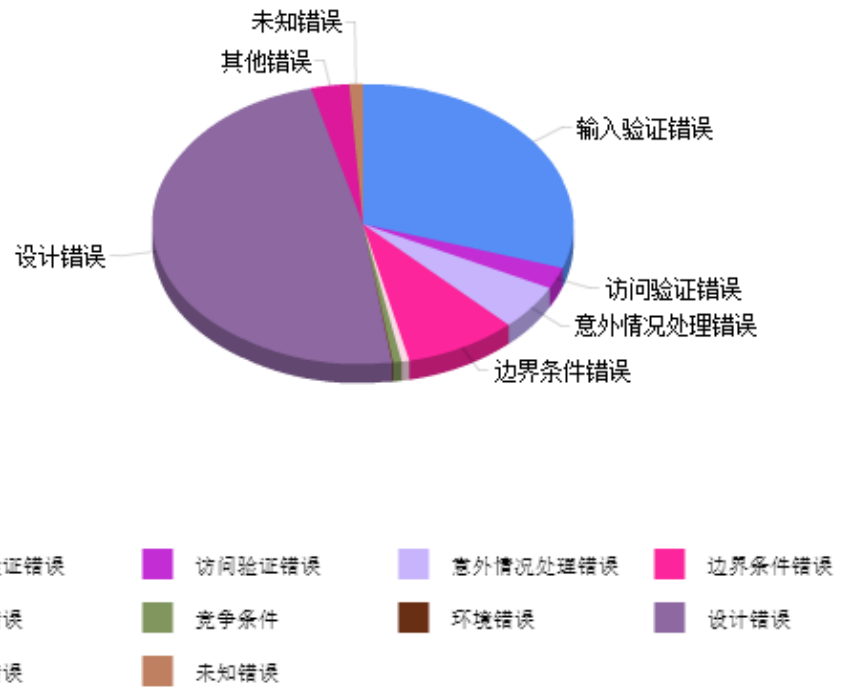
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

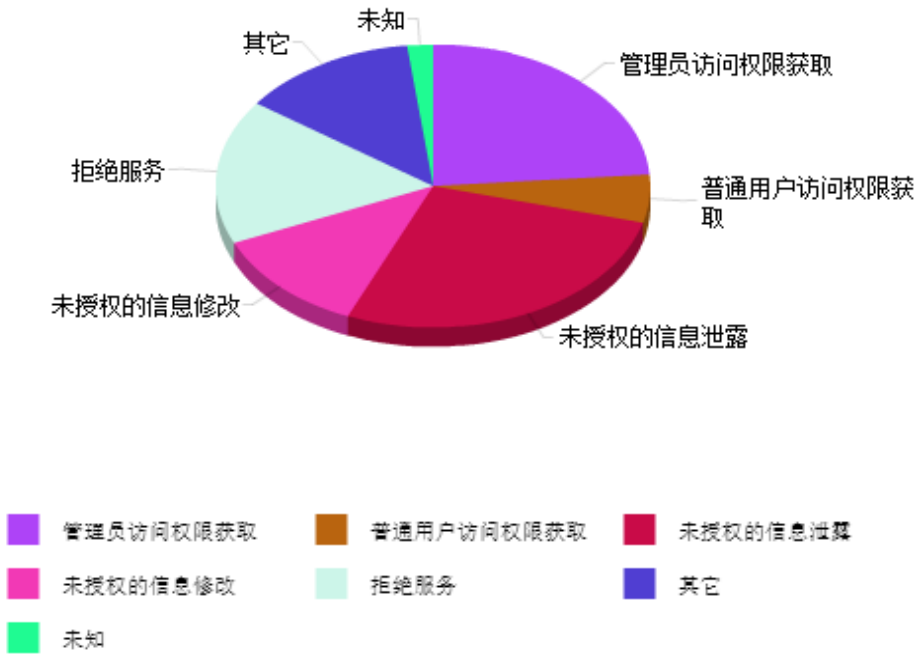
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 514 个，其中高危漏洞 200 个、中危漏洞 271 个、低危漏洞 43 个。漏洞平均分值为 6.35。本周收录的漏洞中，涉及 0day 漏洞 233 个（占 45%），其中互联网上出现“Wordpress 插件 contact-form 远程文件上传漏洞、Kyrol Internet Security 无效指针漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 4336 个，与上周（4121 个）环比增加 5%。

二、安全漏洞增长数量及种类分布情况

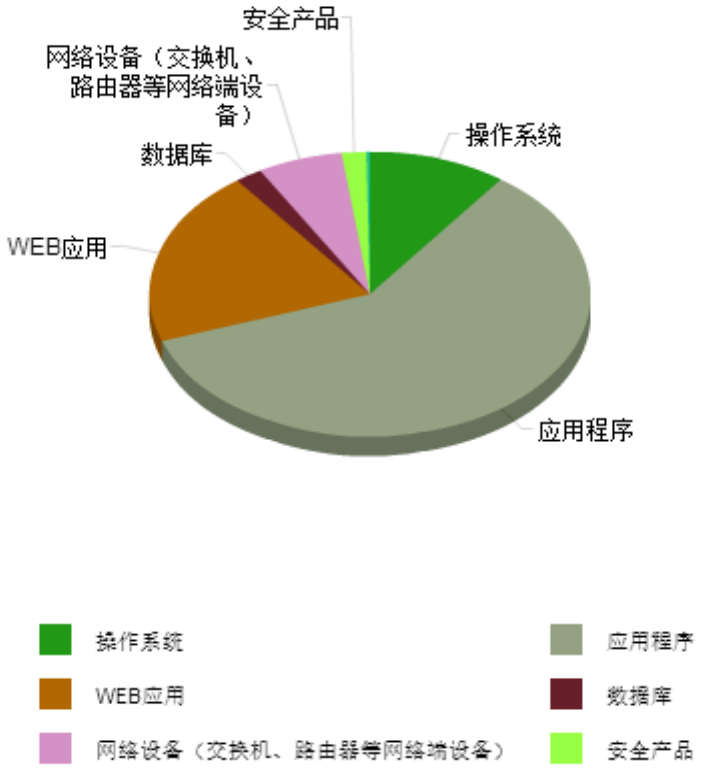
➢ 漏洞产生原因（2020 年 02 月 17 日—2020 年 03 月 02）



➢ 漏洞引发的威胁（2020 年 02 月 17 日—2020 年 03 月 02）



➢ 漏洞影响对象类型（2020 年 02 月 17 日—2020 年 03 月 02）



三、安全产业动态

➢ 用好大数据这把“双刃剑”

近日，中央网信办公开发布《关于做好个人信息保护利用大数据支撑联防联控工作的通知》（以下简称《通知》），明确为疫情防控、疾病防治收集的个人信息，不得用于其他用途。任何单位和个人未经被收集者同意，不得公开姓名、年龄、身份证号码等个人信息。

无疑，此举很有现实针对性。不久前，有网友反映武汉就读大学生个人信息泄露的问题。从武汉返乡大学生的身份证号、手机号码、家庭住址等信息被公然散布在私人微信群聊里，引发一些骚扰、恐吓行为，给当事人的生活造成极大困扰。对此，《通知》明确，收集或掌握个人信息的机构要对个人信息的安全保护负责，采取严格的管理和技术防护措施，防止被窃取、被泄露。

大数据是一把“双刃剑”。在疫情防控阻击战中，这种特征表现得更加明显。一方面，大数据技术深度挖掘交通数据、通信数据、电商消费数据等不同维度数据，为相关决策部门提供宝贵参考，助力科学防治、精准施策。另一方面，在公民个人信息的采集、汇总、共享、披露等多个环节，还存在数据泄露、丢失、滥用等情形，不仅损伤了有关部门的公信力，更让疫情防控工作的效果打了折扣。

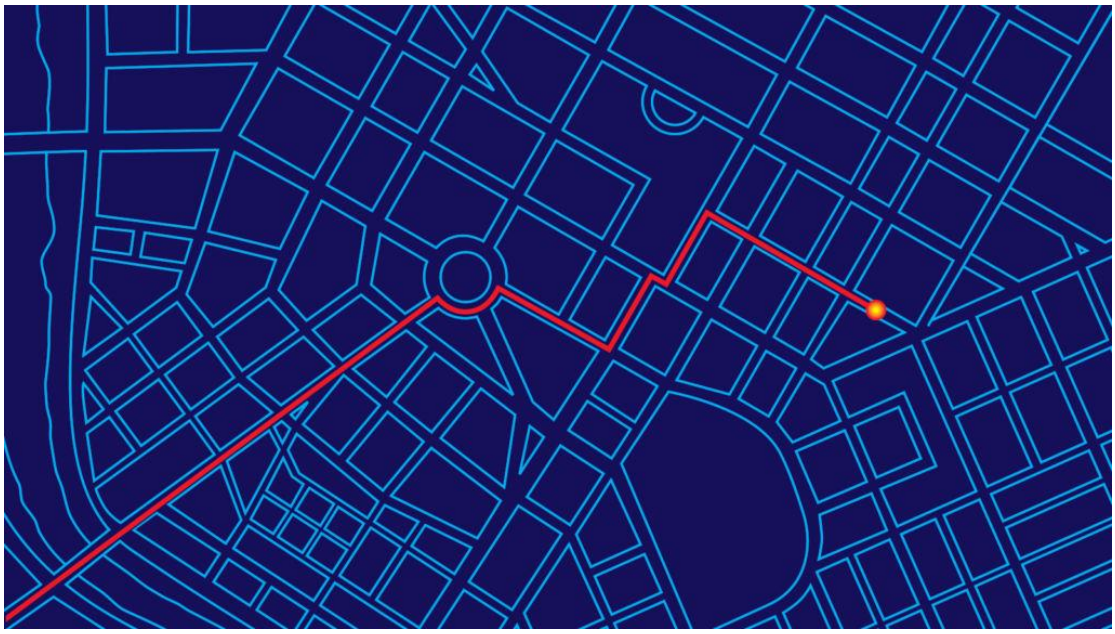
从标准层面看，无论是《网络安全法》《个人信息安全规范》，还是《传染病防治法》《突发公共卫生事件应急条例》等法律法规中的有关规定，都对信息收集的主体、标准、条件和范围有明确要求。然而，疫情来势汹汹，一些地方采取极端做法，过度收集大量敏感信息，同时“牛栏关猫”，对搜集来的信息没有做到妥善保管，导致个人信息泄露，给相关人员带来不必要的困扰乃至损失。

疫情防控工作到了最吃紧的关键阶段，做好有效防控和个人信息保护之间的平衡至关重要。在借助大数据精准防控的同时，也要在各个环节注意做好个人信息保护工作，防止出现数据泄露、丢失、滥用等情形。比如，在疫情报告、通报工作中，注意对个人特征的脱敏，以满足一般公众对疫情的知情权为限，减少个人敏感信息的披露；在数据管理过程中，注意对不同层级人员公开不同的数据粒度，避免个人信息滥用。

疫情面前没有旁观者，信息安全也没有局外人。在法律法规不断完善、行政体系高效落实、个人信息安全意识不断提升的过程中，大数据技术应扬长避短，为打赢疫情防控阻击战发挥更多作用。（来源：光明日报）

➢ 疫情下的数据利用和个人信息保护再权衡

全国范围的新冠肺炎疫情抗击工作开展以来，围绕“早发现、早隔离”的防治原则，人们利用包括大数据技术在内的多种手段，进行重点人群的监测预警、统计分析，以准确、及时、全面的信息为武器对抗疫情。相关的应用包括实时监测车辆、人口动态信息，或利用大数据开展人员流动监测，为研判疫情态势提供技术支持；包括面向公众的“同程排查”服务，用户输入行程日期、车次和地区，即可查询已被披露的新冠肺炎确诊患者同行的火车、飞机和地铁等等。北京、天津、江苏等地方主管部门公布“病例发病期间活动过的小区或场所”，帮助市民及时了解疾病线索，便于社区有针对性地开展疫情防控工作。



除此以外，社会上也出现过一些明显违法或失范的信息利用活动，比如在微信群中公开、

转发有武汉接触史人员的姓名、身份证号、行程、位置等个人信息。在种种信息利用活动面前，我们不禁要问：虽然数字时代的个人信息保护已成为广泛共识和基本准则，但面对公共卫生突发事件，如何权衡公共需要与个人权利，以划定合理的信息保护与利用的界限？

一、我国公共卫生突发事件下的信息利用和保护规则

信息的收集、利用对于传染病疫情防控的重要意义不言而喻，当前我国已基本建立起疫情下的个人信息收集与利用规则框架，通过《突发事件应对法》《传染病防治法》《突发公共卫生事件应急条例》，结合《网络安全法》的相关规定，从应急保障、信息公开、信息保护等角度，分别对政府部门、企业组织以及个人在传染病疫情防控场景下的责任义务进行了规定，为疫情下相关信息的合理利用提供了基本准则。

（一）政府部门按照法定职责收集、公布事件相关信息，对疫情开展监测

政府及有关部门、专业机构应当“通过多种途径收集突发事件信息”（《突发事件应对法》第三十八条）。政府应当主动公开“突发公共事件的应急预案、预警信息及应对情况”（《政府信息公开条例》第二十条）。卫生行政主管部门负责向社会发布突发公共卫生事件的信息（《突发公共卫生事件应急条例》第二十五条）。除了收集和发布疫情事件信息以外，卫生行政部门和相关政府部门还应当开展监测预警。有关部门、医疗卫生机构应当对传染病做到“早发现、早报告、早隔离”（《突发公共卫生事件应急条例》第四十二条）。各级人民政府应当开展“流动人口管理”，落实预防、控制措施，非事件发生地区也要开展“重点人群、重点场所和重点环节的监测和预防控制工作，防患于未然”（《国家突发公共卫生事件应急预案》，2006年实施）。

在传染病疫情防控中，“突发事件信息”、“预警信息”均可以理解为包括传染病人、疑似传染病人、密切接触者等重点人群的健康状况、行踪、位置、工作单位等个人信息。开展“流动人口管理”、“重点人群、重点场所和重点环节的监测和预防控制工作”也将不可避免地涉及大量个人信息收集、分析和利用活动。法律法规赋予政府及有关部门在疫情防控中对个人信息广泛的收集利用权力。底线是不得“故意泄露传染病病人、病原携带者、疑似传染病病人、密切接触者涉及个人隐私的有关信息、资料”（《传染病防治法》第六十八条）。“医疗卫生人员未经当事人同意，不得将传染病病人及其家属的姓名、住址和个人病史以任何形式向社会公开”（《突发公共卫生事件与传染病疫情监测信息报告管理办法》，卫疾控发[2006]332号，第十四条）。

（二）企业、组织和个人承担信息报告义务，并可利用所掌握的数据支持疫情防控

获悉突发事件信息的公民、法人或者其他组织，应当“立即向所在地人民政府、有关主

管部门或者指定的专业机构报告”（《突发事件应对法》第三十八条）。“任何单位和个人发现传染病病人或者疑似传染病病人时，应当及时向附近的疾病预防控制机构或者医疗机构报告”（《传染病防治法》第三十一条）。

《网络安全法》等法律法规对于网络运营者的个人信息保护义务进行了明确界定，包括信息收集的最小化和必要原则，用户知情权，用户同意权，以及对于与第三方（非主管部门）共享的限制等核心规则。

结合前述突发事件管理和传染病防治的有关规定，可以将企业、组织等主体在疫情中处理个人信息及相应的数据保护义务分为三种情况：一是直接发现和疫情相关的信息应当主动向主管部门报告，不受个人信息保护规则的限制。二是按照主管部门要求，或受其委托对用户数据开展分析、利用、研究，辅助疫情防控工作的，应当按照要求或委托的内容进行数据处理，不能超过主管部门的相关职责权限，同时不受常态下个人信息保护规则的限制。三是自主对用户数据进行分析、利用，用于开发疫情防控相关产品和服务的，应当履行常态下的个人信息保护义务。

状态		最小化和必要原则	用户知情同意	第三方共享限制
疫情	直接发现	×	×	×
	受委托的数据利用	×	×	×
	自主的数据利用	√	√	√
常态	自主的数据利用	√	√	√

表 1. 企业或组织在疫情与常态下的个人信息保护义务对比

二、域外公共卫生突发事件下的信息保护豁免

将视线投向域外，欧盟、美国等数据保护与利用规则较为发达的国家和地区，均在立法或判例中确立了公共事件中的个人信息处理规则，主要包括：

（一）为保护公共利益在一定程度上限制个人信息知情同意权

欧盟《一般数据保护条例》确立了一般情况下的数据主体知情同意原则，但同时也规定了 6 类无需获得数据主体同意即可处理个人信息的理由。具体包括为保护数据主体及其他自然人的重要利益而处理个人数据，为公共利益而执行任务，或数据控制者被赋予公共职能时必须处理个人数据等。美国《健康保险携带和责任法案》（简称 HIPAA）规定在 12 类涉及

“国家利益优先”的情形下，可以不经个人同意而披露及使用健康信息，其中包括公共卫生事件、卫生监管活动、降低卫生或安全风险、重要政府工作等。HIPAA 规制的“可识别个人健康信息”同时涵盖了个体信息和集合信息，既包括个人过去、现在和未来的身体和精神健康信息，相关支付信息，也包括人口学统计数据。

（二）运用“第三方准则”保护第三方机构向主管部门提供数据或数据分析结果

“第三方原则”是指第三方机构（如医院、电信运营商、保险公司等）应政府部门要求提供其掌握的个人信息，不受美国宪法第四修正案（公民免受无理由搜查和扣押）的限制。该原则是美国法院在处理数据协助义务案件中所应用的一项规则，也适用于强制上报健康数据等活动，数据收集方可以在不经用户同意的情况下变更收集时告知用户的使用目的，并将数据一次性或持续性披露给政府部门。

随着掌握海量用户数据的数字平台兴起，数据用于公益目的的场景将越来越丰富。以防治流感为例，目前美国已经有众多基于用户数据的平台正积极利用贫困、失业、低学历、住房不稳定以及粮食不安全等信息确定高风险人群，以这些数据为基础，帮助医疗行业更准确地预测流感的发病率和入院率，促进医疗资源的有效分配。第三方准则为海量数据用于执法和公益目的搭建了一种框架，值得重视。

（三）运用比例原则衡量特殊情况下信息利用与保护的合理界限

无论是公共利益优先还是“第三方准则”，都是在利益冲突场景下为权衡信息利用与保护而提出的法律原则，并未解决现实情况下如何划定具体边界的问题。如何在不同场景下在两者之间进行再权衡，很大程度上将取决于比例原则，即将公共需要或公共利益与个人信息受到克减的程度相比较，找到一个相对合理的平衡点。

大数据利用是利益冲突的典型场景，近年来受到各方关注。美国联邦法院大法官 Rubenstein 一针见血地指出，大数据给隐私保护法带来了挑战：一方面模糊了个人信息和非个人信息的边界，另一方面冲击了信息最小化原则和知情同意原则。健康或医疗大数据就是这样一个例子，健康信息普遍被认为是最具有个人和秘密特性的信息，但同时也是对识别犯罪嫌疑人、调查流行病、制定公共政策、开展生物医学和行为学研究等具有高度价值的信息。今后在健康大数据领域势必将产生更加多样的数据应用，个人信息利用与保护的界限划定将面临更多挑战。

三、启示与建议

疫情下的数据利用与个人信息保护实践为完善个人信息保护制度提供了新的观察视角，在数据管理制度不断健全完善的当下具有特别意义，建议政策制定者加强研究应对，将平衡

原则从抽象空洞的基本原则发展为鲜活具体的可操作规范。

（一）不断审视数据利用与个人信息保护的平衡

近年来，我国积极推进个人信息保护的立法和实践，个人信息保护制度不断完善，重点领域的执法力度明显加强。信息保护固然是数字经济时代的应有之义，数据利用则更是社会各领域发展前进的强劲动力，必须在其中维持微妙的平衡。相关部门在规范制定和执行中应开展“平衡性测试”，统筹考虑个人信息的敏感性、个人权益的可恢复性、公共需要的重要性紧迫性等因素，处理好数据管理的“宽”与“严”的关系。

（二）细化公共事件等特殊场景下的数据利用规则

加快以规则形式明确公共事件等特殊场景下的数据利用规则。可以考虑按照数据的不同识别程度，如匿名性、可关联性、可识别性，结合数据的敏感性、重要性，公共需求的迫切性等维度，分别规定不同的利用规则，认定标准，保护措施，管理体制，主体责任。政策制定者应持续发布指导事例，阐释具体个案中、不同行业背景下的国家利益、公共利益具体含义，明确个人信息权利与公共需求、执法协助、学术研究等法律保护事由的合理界限，为数据利用和保护的平衡提供清晰的指引和合理的预期。（来源：中国信通院）

➢ 拔除网络生态“杂草”

当我们借助互联网的便利自由浏览阅读免费、快捷、海量的网络信息时，网络暴力、人肉搜索、深度伪造、流量造假、操纵账号等行为也在污染着网络生态。针对这些问题，国家互联网信息办公室近日发布《网络信息内容生态治理规定》（以下简称《规定》），自 2020 年 3 月 1 日起施行，旨在营造良好网络生态，保障公民、法人和其他组织的合法权益，维护国家安全和公共利益。

网络暴力是“毒瘤”

中国社科院发布的《社会蓝皮书：2019 年中国社会形势分析与预测》显示，青少年在上网过程中遇到过暴力辱骂信息的比例为 28.89%。其中，暴力辱骂以“网络嘲笑和讽刺”及“辱骂或者用带有侮辱性的词汇”居多，分别为 74.71%和 77.01%；其次为“恶意图片或者动态图”（53.87%）和“语言或者文字上的恐吓”（45.49%）。

由于网络用户的匿名性与隐蔽性特征，网络暴力已成为威胁互联网环境的一大毒瘤。许多网民对未经证实或已经证实的网络事件，在网上发表具有伤害性、侮辱性和煽动性的失实

言论，对当事人的名誉权和隐私权造成严重损害。

人肉搜索更是网络暴力的升级版。四川德阳的安医生在泳池里与两个男孩发生争执，事后安医生在网络上遭到人肉搜索，给当事人生活造成严重影响。

从根本上说，互联网领域的种种乱象都是网络信息发布者责任意识缺乏的体现，此次网信办出台相关规定，对网络信息发布主体实行问责制，未来或对网络生态治理带来更积极影响。

给网络空间“洗洗澡”

国家网信办有关负责人表示，出台《规定》主要基于以下两个方面的考虑：一是建立健全网络综合治理体系的需要；二是维护广大网民切身利益的需要。而《规定》中的生态治理，是指政府、企业、社会、网民等主体，以培育和践行社会主义核心价值观为根本，以网络信息内容为主要治理对象，以建立健全网络综合治理体系、营造清朗的网络空间、建设良好的网络生态为目标，开展弘扬正能量、处置违法和不良信息等相关活动。

做好网络信息内容生态治理，网络信息内容生产者、网络信息内容服务平台需要率先承担责任，规范自身行为。网络内容生产者应当保证所发布网络信息的真实性，并且应该有积极的导向性；网络信息内容服务平台应当履行信息内容管理主体责任，建立网络信息内容生态治理机制。在网络出现“夸夸群”之后，“互怼群”“互喷群”也相继出现，群友之间毫无理性地谩骂指责，严重污染了互联网环境，也成为网络语言暴力滋生的土壤。

网民自律也必不可少。中国互联网络信息中心发布的数据显示，截至 2019 年 6 月，中国网民规模达 8.54 亿，其中大学学历以上占 9.9%，而初中学历以下网民占比 56.9%。数量

庞大的网民群体包括青少年网民，都应不断提高自身文化素质，做到文明上网。青少年在中国网民中占有很大比例，由于涉世未深、人生观价值观正在树立，在网上发表不当言论的行为屡见不鲜。要加强对青少年上网行为的引导，使其在法律和道德允许的范围内自由表达。同时，针对网络技术发展催生出的网络直播等媒介样态，用户在用弹幕、评论等多种形式参与网络互动时，应意识到这些网络空间也不是法外之地。

打好网络治理“攻坚战”

《规定》的出台，有利于建立健全网络综合治理体系，加强和创新互联网内容建设，落实互联网企业信息管理主体责任，全面提高网络治理能力，营造清朗的网络空间。

《规定》的出台对于新时代中国互联网生态治理是一个良好开端。南京大学法学院教授单勇在接受采访时表示：“有法可依、依法治理是实现互联网良性生态治理的根本举措。目前，《个人信息保护法》以及《数据安全法》两部关于完善互联网领域治理的法律也正在制定中。”

“网络信息内容服务平台要强化自身的责任意识，对于违法违规的帖子、评论、回复等内容要依法删除。”单勇认为，当前的互联网是一个以平台为基础的生态环境，我们要强调平台社会、平台治理。在未来的互联网生态治理中，要努力实现社会整体安全与个人权利保护之间的平衡，在为个人信息与数据权利提供法律保护的同时，实现网络总体安全的最大化。网络监管部门也要拓宽治理思维，在互联网生态领域实现治理能力的现代化。

网络生态治理是一场攻坚战，包括网络信息内容生产者、网络信息内容服务平台以及网络服务使用者等多个主体都应该参与其中，规范自己的行为、承担相应的责任，共同努力赢得这场战役的胜利。（来源：人民日报海外版）

➢ 没有了选择权和知情权，人脸识别还值得信任吗？

近期，曝光了一系列和人脸识别相关的新闻，引发了普遍关注。有某高校强制使用网课系统打开摄像头使用人脸监控，有犯罪分子通过人工软件制作的 3D 头像通过支付宝人脸识别认证，人脸识别技术应用的问题和风险可见一斑。当然，人脸识别技术非接触式的特点，使其应用优势也显而易见，在机场、车站，人脸识别提高了进出站效率，远程身份核验为在线服务提供保障，甚至最近有组织在防疫期间使用其进行身份核验来避免人员接触。

有人认为，人脸并不是什么“保密”的信息，人不可能把脸藏起来，平时就是公开的。

然而，这种说法并没有考虑当人脸和个人财产、行踪等产生绑定和关联时，还有谁会觉得人脸被随意收集使用没有风险？人脸识别的背后是对人脸特征个人信息的收集使用，自然需要遵守个人信息保护的原则。可是，以使用人脸识别功能的 App 为例，到底做的如何呢？

举报问题情况

截至目前，“App 个人信息举报”举报平台收到的超过 1 万条的有效举报信息中，与人脸识别相关举报信息有 500 余条，涉及 50 余款 App。包括了使用人脸进行身份核验、认证，或使用人工智能技术生成虚拟人脸、预测分析等场景。其中，大部分 App 使用人脸识别技术用于身份核验，确保必须是本人亲自参与完成某些业务功能，以此解决仅用姓名、手机号码、身份证号码等“实名制”信息核验带来的可信度不足等问题，典型的有金融账户开户、支付环节、司乘认证、会员身份核验等。随着人脸识别技术的日趋成熟，2019 年下半年开始，引入人脸识别技术的 App 逐渐增多，很多 App 都将其视为创新点。除了 App 以外，智能摄像头、支付终端等都开始逐步加载人脸识别功能，人脸识别的大范围应用迹象已现端倪。当下，很多网友对人脸识别应用过程中的个人信息保护问题的提出了疑问，可见，在逐步进入“刷脸”社会时，如何处理便利性和安全性的平衡关系成为当务之急。

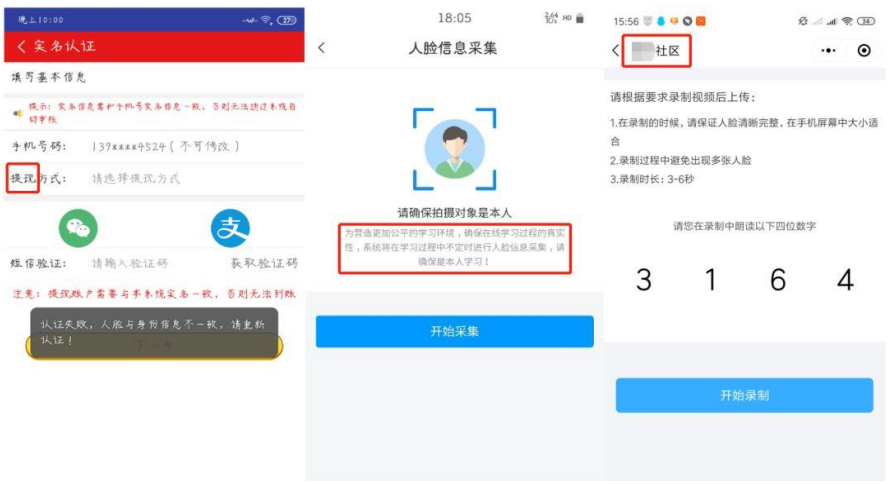
详情		12299	无法注销账号，解除绑定的银行卡强制采集人脸信息并且强制上传身份证正反面，版本v6.6.4
受理		12292	强制用户人脸识别认证，不完成人脸识别不能其使用基本功能
受理		12245	版本号8.0.5 该应用在用户换新手机首次登陆已经验证了银行卡预留手机号验证码、登录密码的情况下强行要证。目前已知的支付类app如、银行类app例如、等部分软件虽有人脸识别，但是也没有强制
详情		12171	1.收取押金后退还押金难。 2.强制要求用户人脸识别。
受理		12169	进入app需要填写身份证并进行人脸认证
详情		12150	版本号：2.2.0 应用市场：苹果应用市场、应用宝等 私营注册主体公司，非法收集公民隐私 1、收集身份证正反面照片拍照 3、收集手机通讯录 4、收集人脸信息 公司，背后股东是私人，非国家政府机构，谁给他们必须使用他们的APP，而且还收集我们的身份证信息、人脸信息、通讯录信息的，还在《用户协议》中不保证用户信息
受理		12146	由于大学课程学习需要，需要使用app进行线上课程学习。但是在学习过程中，平台以"确保学习真实性"为由无法继续学习。导致个人课程无法完成，无法获得学分，无法毕业。
受理		12026	App v5.1.0 收集个人，人脸信息。收集范围过大。个人信息收集提示中，最后一条霸王条款，收集的个人信息出现一切收集人。app没有注销账号功能。
受理		11952	升级为VIP后，新版本的app不实名认证和人脸识别就不能正常使用，其客服理由是：保障终身VIP账号安全，户安全是经营方的责任，可以通过技术手段实现，为什么要转嫁给消费者，要求消费者提供个人隐私呢？他这样的做法据。
受理		11899	我居住的地方不是小区 是属于城中村 此app被强行要求下载 否则无法进出这也就算了，各种隐私侵犯，需要拍身份证包括通讯录，甚至需要手持身份证录像上传？一个门禁软件需要那么多要求吗？如果是政府要求我无可厚非 问题是他们各种吐槽 请工作组麻烦如实调查

典型现象和问题分析

梳理上述被举报的 50 余款 App 在应用人脸识别技术时发现，大多数在处理人脸信息方面存在一些共性现象和问题，主要包括：

1. 强制要求用户提供人脸信息（占比约 60%）

比如，在提现时的身份核验环节要求刷脸，网友表示“当问及客服，强制收集人脸信息的理由，平台表示因涉及提现交易必须确保为本人操作，除非提供人脸信息，否则不能提取账户钱款”；而在社区门禁解锁、高校监督课堂行为等环节，要求必须使用 App 上线的人脸识别功能。这其中，有些 App 将采用人脸识别核验身份作为了可选的补充措施，但是大部分 App 将其列为“必选项”，但是，并没有给出充分的理由。这其中，常见的理由是为了满足法律法规或行业监管有关“实名制要求”、确保用户身份真实性、实现反欺诈等业务风险控制，需要收集用户真实身份信息，对此，我们曾经分析过“手持身份证照片”的必要性，其逻辑类似，文章见：收集“手持身份证照片”究竟为哪般？。而与收集的身份证照片相比，如果人脸识别过程对人脸各个角度原始照片均做保留，恐怕其一旦被滥用、泄露，后果更甚。



身份核验也好、安全风控也罢，其方式方法有多种多样，采取强制，或者以提升其它操作方式复杂度“变相”强制方式获取人脸信息，既没有足够充分的法律依据，也没有照顾用户的隐私体验。面对新兴的人脸识别技术，用户往往处于“到处在收，却没得选”的境地，怎能不让用户心存芥蒂，杭州动物园强制使用人脸识别被人起诉成为“中国人脸识别第一案”是最好的例证。

2. 未清晰说明收集使用人脸信息的规则（占比约 90%）

既然人脸信息的收集往往不可避免，那么如何处理、保护人脸信息自然成为网友们关心的问题。就从身份核验的目的出发，完全可以在提取人脸特征信息后，及时删除原始的人脸图像，以避免数据泄露造成影响，如果能够告知用户能及时删除人脸信息或直接核验不做保留，相信大家对其接受度会有提升。可见，清晰、合理的个人信息处理规则可以让用户了解原委，为使用人脸识别的功能建立信心。

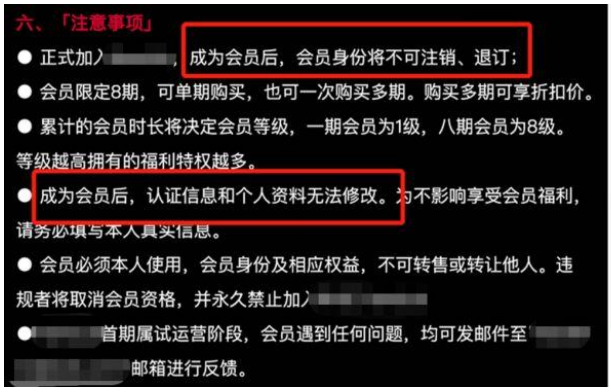
然而，核验发现，绝大部分相关 App 只在隐私政策中笼统提及“个人信息的保存将在法律法规要求的最短保存限期内，当超出上述保存期限，会对其进行匿名化处理”、“我们收集的个人信息，将在中国内地存储和使用”等，对于用户关心的人脸信息是否会留存原始图像信息，留存多长时间，使用范围如何，是否向第三方提供，采取了何种安全措施等均是只字不提。有网友问及 App 客服人脸信息是否会被保存时，却被告知“公司会使用加密方式保证客户信息安全，但因商业机密拒绝提供人脸信息识别出处、处理方式等”。一方面，面对完全“黑盒”的人脸识别功能，另一方面，面对时常曝光的人脸原始照片被贩卖的新闻，怎能不让用户心生戒备。

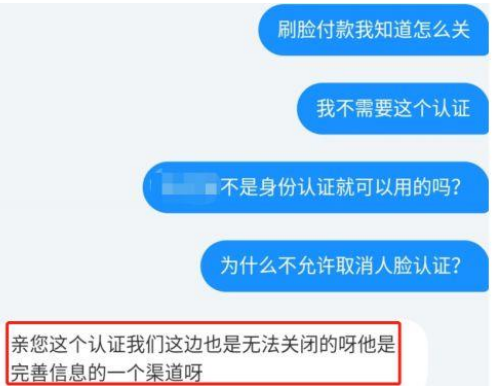
3. 没有提供撤回同意收集使用人脸信息的方法（占比接近 100%）

有网友在尝试使用人脸识别的功能后，担心人脸信息被挪作他用，想撤回之前同意提交的人脸信息，可以与客服沟通发现，并没有提供这样的撤回机制。实现撤回同意的机制往往被视为保障用户选择权的重要体现，比如，手机提供了控制提供可收集个人信息权限的机制，用户可以通过关闭地理位置、摄像头等方式改变之前的同意决定，防止个人信息被继续处理。

就人脸识别而言，对“撤回同意”的理解与实践存在一定的复杂性。比如，由于在 App

端，用户自行决定不再使用刷脸支付可以避免人脸信息被继续处理，是否算是对刷脸支付的撤回？因此就无需额外提供人脸识别的撤回机制。然而，这个理由所阐述的逻辑并不完备，如果用户计划以后不再使用人脸识别功能，而又无渠道和机制向 App 运营者反馈其意愿，而 App 运营者则可能以其不清楚用户是否还会再次使用为由，“在服务期间”长期保留用户的人脸特征信息，而事实上，所保留的这些信息已经超出达成前期的处理目的需要，有不符合最短期限内存储原则的嫌疑，无意之间增加了泄露、滥用隐患。因此，向用户提供撤回收集人脸信息的明确方法和机制是一种向用户负责的体现。否则，用户面临“一旦提供人脸，则无追回余地”的境地，怎能不让用户心生顾虑。





此外，人脸识别技术准确性的问题也不可忽略，此前“小学生使用打印照片破解人脸识别功能的新闻”让人大跌眼镜。当然，人脸相关的原始图片、特征信息等还可能应用到人脸识别相应技术、模型的训练、优化，这些虽然与为用户提供服务不直接相关，但又与服务过程的安全息息相关。此时，如果希望得到用户理解与支持，将规则透明化则显得尤为重要，否则换来的可能是更多的猜疑和反感。

而除了 App 普遍存在的以上现象和问题，其他应用人脸识别技术的场景下，用户“知情权”和“选择权”的丧失也非常普遍，由此带来的用户对大数据时代下隐私保护现状的“失望”，是对利用大数据造福社会的一种“看似无形”而又“无法忽视”的阻碍。

几点建议

随着人脸识别技术广泛应用于各 App 及生活场景下，人脸信息的保护成为个人信息保护工作中的重中之重，必须高度重视对此类信息的收集使用行为，保障用户知情权和选择权，确保各环节安全。

以下建议供相关方参考：

1、收集人脸信息前，需确保其目的合法、正当、必要，只有业务本身涉及用户重大利益或特殊监管需求时考虑使用，不把人脸识别作为提供所有业务功能的前提；

2、除了在隐私政策等文本中体现外，单独向个人信息主体告知收集、使用人脸信息的目的、方式和范围，以及存储时间等用户关心的规则，并征得个人信息主体的明示同意；

3、原则上不存储原始的人脸信息（如样本、图像等），优先在采集终端中直接使用人脸实现身份识别、认证等功能，如需通过服务器端实现的，在实现功能后选择删除可提取人脸特征信息的原始图像；

4、使用人脸识别技术时，需采取加密传输、存储及严密的权限控制、审计等措施确保收集使用环境的安全可信；

5、使用人脸信息进行身份核验、比对时，应选择与公安部门等官方授权机构进行合作；

6、逐步完善用户对其人脸信息的控制权，比如查询收集使用情况，撤回对收集人脸信息的同意，以及查询是否还继续持续留存了人脸信息等；

7、原则上避免对人脸信息的共享、转让，杜绝未经用户明示同意，私自对外提供人脸信息行为；

8、可优先将人脸识别作为辅助手段进行应用，以兼顾便捷性与安全性，比如小额支付、快速通道等。

人脸识别等新技术、新应用自出现以来，可谓争议不断，很多时候究其原因，是忽视了用户的“选择权”、“知情权”，如此做法，谈何消除顾虑，获取用户信任。随着民众安全意识的提升，个人信息保护早已成为衡量民众在互联网上“获得感”、“安全感”的重要砝码。企业不应只盯着新技术、新应用的商业价值，而是赋予其更多社会价值，才是赢得更多发展空间的一剂良方 。

根据《关于开展 App 违法违规收集使用个人信息专项治理的公告》，受中央网信办、工信部、公安部、市场监管总局委托，全国信息安全标准化技术委员会、中国消费者协会、中国互联网协会、中国网络空间安全协会成立 App 专项治理工作组，本公众号主要受理对 App 违法违规收集使用个人信息的举报，并发布有关新闻、通知、文章等。（来源：APP 治理工作组）

四、政府之声

➢ 国务院办公厅发布《国家政务信息化项目建设管理办法》

2020 年 1 月 21 日，近日，国务院办公厅印发《国家政务信息化项目建设管理办法》（以下简称《办法》），对国家政务信息系统的规划、审批、建设、共享和监管作出规定。

《办法》指出，要规范国家政务信息化建设管理，推动政务信息系统跨部门跨层级互联互通、信息共享和业务协同，强化系统应用绩效考核。国家政务信息系统主要包括：国务院有关部门和单位负责实施的国家统一电子政务网络平台、国家重点业务信息系统、国家信息资源库、国家信息安全基础设施、国家电子政务基础设施（数据中心、机房等）、国家电子政务标准化体系以及相关支撑体系等符合《政务信息系统定义和范围》规定的系统。


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 > 综合政务 > 政务公开
索引号: 000014349/2019-00146
主题分类: 综合政务\政务公开
发文机关: 国务院办公厅
成文日期: 2019年12月30日
标题: 国务院办公厅关于印发国家政务信息化项目建设管理办法的通知
发文字号: 国办发（2019）57号
发布日期: 2020年01月21日
主题词:
国务院办公厅关于印发国家政务信息化项目建设管理办法的通知
国办发〔2019〕57号
各省、自治区、直辖市人民政府，国务院各部委、各直属机构：
《国家政务信息化项目建设管理办法》已经国务院同意，现印发给你们，请认真贯彻执行。
相关报道
国务院办公厅印发《国家政务信息化项目建设管理办法》
解读
国家发展改革委有关负责人就《国家政务信息化项目建设管

《办法》强调，国家政务信息化建设管理应当坚持统筹规划、共建共享、业务协同、安全可靠的原则，充分发挥国家政务信息化建设规划的统筹作用。各有关部门编制规划涉及政务信息化建设的，应当与国家政务信息化建设规划进行衔接。

《办法》在简化优化项目申报和审批流程的基础上，要求对中央本级政务信息系统全口径纳入管理平台进行统一管理。各部门所有新建政务信息化项目，均应当在全国投资项目在线审批监管平台政务信息化项目管理子平台报批或者备案。各部门应当在管理平台及时更新

本部门政务信息系统目录。管理平台汇总形成国家政务信息系统总目录。

《办法》提出，加强国家政务信息化项目建设投资和运行维护经费协同联动，对于未按要求共享数据资源、未纳入国家政务信息系统总目录、不符合密码应用和网络安全要求等情况的政务信息系统，不安排运行维护经费。加强对绩效评价和项目后评价结果的应用，将评价结果作为下一年度安排政府投资和运行维护经费的重要依据。坚持“联网通办是原则，孤网是例外”，对部门认为根据有关法律法规和党中央、国务院要求不能进行信息共享，但是确有必要建设或者保留的，经国务院批准后方可建设或者保留。

《办法》强调，有关部门要建立国家政务信息化建设管理的协商机制，做好统筹协调，开展督促检查和评估评价，推广经验成果，形成工作合力。（来源：新华社）

- **国务院办公厅关于印发国家政务信息化项目建设管理办法的通知国办发〔2019〕57 号**
- **全文：**http://www.gov.cn/zhengce/content/2020-01/21/content_5471256.htm

➢ 市场监管总局《关于开展商用密码检测认证工作的实施意见（征求意见稿）》

2020 年 2 月 20 日，国家市场监管总局发布《关于开展商用密码检测认证工作的实施意见（征求意见稿）》公开征求意见的通知，征求意见表示，商用密码认证机构应当符合有关行政法规、规章规定的基本条件，具备从事商用密码认证活动的专业能力，并经市场监管总局征求国家密码管理局意见后批准取得资质。

为推进商用密码检测认证体系建设，促进商用密码产业健康有序发展，根据《中华人民共和国产品质量法》《中华人民共和国密码法》和《中华人民共和国认证认可条例》，市场监管总局、国家密码管理局联合起草了《关于开展商用密码检测认证工作的实施意见（征求意见稿）》（见附件），现向社会公开征求意见。欢迎各有关单位或个人提出修改意见，并于 2020 年 3 月 6 日前反馈市场监管总局（来源：国家市场监管总局）

- **《关于开展商用密码检测认证工作的实施意见（征求意见稿）》**
- **全文：**http://www.samr.gov.cn/hd/zjdc/202002/t20200220_311881.html

➢ 央行发布《个人金融信息保护技术规范》

2020 年 2 月 13 日，全国金融标准化技术委员会（简称“金标委”）发布了《个人金融

信息保护技术规范》（以下简称“《规范》”），据移动支付网了解，个人金融信息是个人信息在金融领域围绕账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息等方面的扩展与细化，是金融业机构在提供金融产品和服务的过程中积累的重要基础数据，也是个人隐私的重要内容。

《规范》规定了个人金融信息在收集、传输、存储、使用、删除、销毁等生命周期各环节的安全防护要求，从安全技术和安全管理两个方面，对个人金融信息保护提出了规范性要求。 《规范》将个人金融信息由高到低分为 C3、C2、C1 三个类别，C3 主要为各类账户密码，C2 主要为账户、身份证信息、短信口令、KYC 信息、住址等，C1 主要为开户时间、支付标记信息等。在信息收集方面，《规范》要求“不应委托或授权无金融业相关资质的机构收集 C3、C2 类别信息”，这一条使得许多非持牌机构在金融信息的收集上异常被动。（来源：全国金融标准化技术委员会）

- **《个人金融信息保护技术规范》（JR/T 0171-2020）**
- http://www.cfstc.org/bzgk/gk/view/bzxq.jsp?i_id=1856

➢ 工信部《关于做好疫情防控期间信息通信行业网络安全保障工作的通知》

2020 年 2 月 18 日，工信部办公厅发布《关于做好疫情防控期间信息通信行业网络安全保障工作的通知》，旨在切实做好疫情防控和经济社会运行的网络安全支撑保障工作，确保疫情防控期间网络基础设施安全，防止发生重大网络安全事件。

《通知》要求全力保障重点地区重点用户网络系统安全，加强信息安全和网络数据保护，进一步强化责任落实和工作协同。具体而言，加强重点用户网络安全技术支撑，加强重点地区网络基础设施安全防护，加强涉疫情网络安全威胁监测处置，加强疫情期间电话用户入网服务保障。

此外，《通知》要求加强涉疫情电信网络诈骗防范，加强网上涉疫情相关信息监测处置，加强个人信息和数据安全保护。充分利用微信、微博、短彩信、APP 等平台开展涉疫情电信网络诈骗的宣传引导和风险提示。进一步强化个人信息收集、使用等各环节的规范管理，将个人信息和数据安全保护各项要求落到实处。（来源：工业和信息化部）

- **工业和信息化部办公厅关于做好疫情防控期间信息通信行业网络安全保障工作的通知**
- http://www.miit.gov.cn/n1146295/n1652858/n1652930/n4509650/c7681741/content.html

五、本期重要漏洞实例

➢ 工信部发布涉新冠肺炎疫情的网络安全风险提示

发布日期：2020-02-13
更新日期：2020-02-13
描述：

近期，工业和信息化部网络安全威胁信息共享平台收到网络安全企业及机构报告，发现多起利用新冠肺炎疫情实施网络攻击的行为。经研判分析，攻击者利用疫情对公众的心理影响，将计算机病毒、木马、移动恶意程序等伪装成包含“肺炎病例”“防护通知”等热门字样的信息，通过钓鱼邮件、恶意链接等方式传播，一旦点击下载，可能导致计算机、手机等终端设备被窃取信息或远程控制。

为降低网络安全风险，工业和信息化部网络安全管理局组织相关单位加大对伪装成疫情信息传播计算机病毒、木马、移动恶意程序等监测力度，采取了屏蔽病毒木马控制端、下载恶意程序等措施，对发现的网络威胁进行处置。同时，提醒公众提高网络安全风险意识，采取以下措施进行防范：

一、不轻易打开来历不明的电子邮件及其附件。

二、不轻易点击短信或微信中不明来源的链接。

三、从正规应用商店或官方网站下载安装应用程序。

四、安装杀毒软件并及时更新。

下一步，工业和信息化部网络安全管理局将继续组织加强涉疫情网络安全威胁监测与处置工作，欢迎向工业和信息化部网络安全威胁信息共享平台（网址 http://www.cstis.cn，邮箱 cstisaccount@caict.ac.cn）报送涉疫情相关网络威胁信息线索，切实维护网络秩序和公共利益。
链接：http://www.miit.gov.cn/newweb/n973401/n7647394/n7647414/c7676445/content.html

➢ Cisco FXOS Software CLI 命令注入漏洞

发布日期：2020-02-26
更新日期：2020-02-28
受影响系统：
Cisco FXOS Software
描述：

CVE(CAN) ID: CVE-2020-3169
Cisco FXOS Software 是一套运行在思科安全设备中的防火墙软件。

Cisco Firepower 4100 Series 和 Firepower 9300 Security Appliances 上 FXOS Software 由于没有充分验证发送到 CLI 命令的参数，CLI 中存在操作系统命令注入漏洞，本地攻击者可利用该漏洞在底层的 Linux 操作系统上以 root 权限执行任意命令。

<*来源：Cisco

*>

建议：

厂商补丁：

Cisco

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200226-fpwr-cmdinj

➢ IBM Sterling B2B Integrator 跨站脚本漏洞

发布日期：2020-02-26

更新日期：2020-02-27

受影响系统：

IBM Sterling B2B Integrator Standard Edition 5.2.0.0-5.2.6.5

描述：

CVE(CAN) ID: CVE-2019-4596

IBM Sterling B2B Integrator 是一套集成了重要的 B2B 流程、交易和关系的软件。

IBM Sterling B2B Integrator 5.2.0.0-5.2.6.5 版本，在实现中存在跨站脚本漏洞。远程攻击者可利用该漏洞向 Web UI 注入任意的 JavaScript 代码，更改某些功能，导致信息泄露。

<*来源：IBM （ncsupp@ca.ibm.com）

*>

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://exchange.xforce.ibmcloud.com/vulnerabilities/167879

https://www.ibm.com/support/pages/node/3144369

➢ Apache Tomcat 文件包含漏洞

发布日期：2020-02-11
更新日期：2020-02-21
受影响系统：
Apache Group Tomcat 9 < 9.0.31
Apache Group Tomcat 8 < 8.5.51
Apache Group Tomcat 7 < 7.0.100
Apache Group Tomcat 6
不受影响系统：
Apache Group Tomcat 9.0.31
Apache Group Tomcat 8.5.51
Apache Group Tomcat 7.0.100
描述：

CVE(CAN) ID: CVE-2020-1938
Tomcat 是 Apache 软件基金会中的一个重要项目，性能稳定且免费，是目前较为流行的 Web 应用服务器。
Apache Tomcat 由于 Tomcat AJP 协议存在缺陷，在实现上存在文件包含漏洞。攻击者利用该漏洞可通过构造特定参数，读取服务器 webapp 下的任意文件。若目标服务器同时存在文件上传功能，攻击者可进一步实现远程代码执行。

<*来源：anonymous
*>

建议：

厂商补丁：
Apache Group

目前官方已在最新版本中修复了该漏洞，请受影响的用户尽快升级版本进行防护，官方下载链接：
版本号　下载地址
Apache Tomcat 7.0.100　http://tomcat.apache.org/download-70.cgi
Apache Tomcat 8.5.51　http://tomcat.apache.org/download-80.cgi
Apache Tomcat 9.0.31　http://tomcat.apache.org/download-90.cgi

六、本期网络安全事件

➢ 家长注意！教育部发布今年第 1 号预警，已有多人受骗！

2020 年 2 月 17 日，教育部网站发布《全国治理教育乱收费联席会议办公室关于谨防有人利用疫情防控期间线上教学名义进行网上收费诈骗的预警（2020 年第 1 号预警）》。

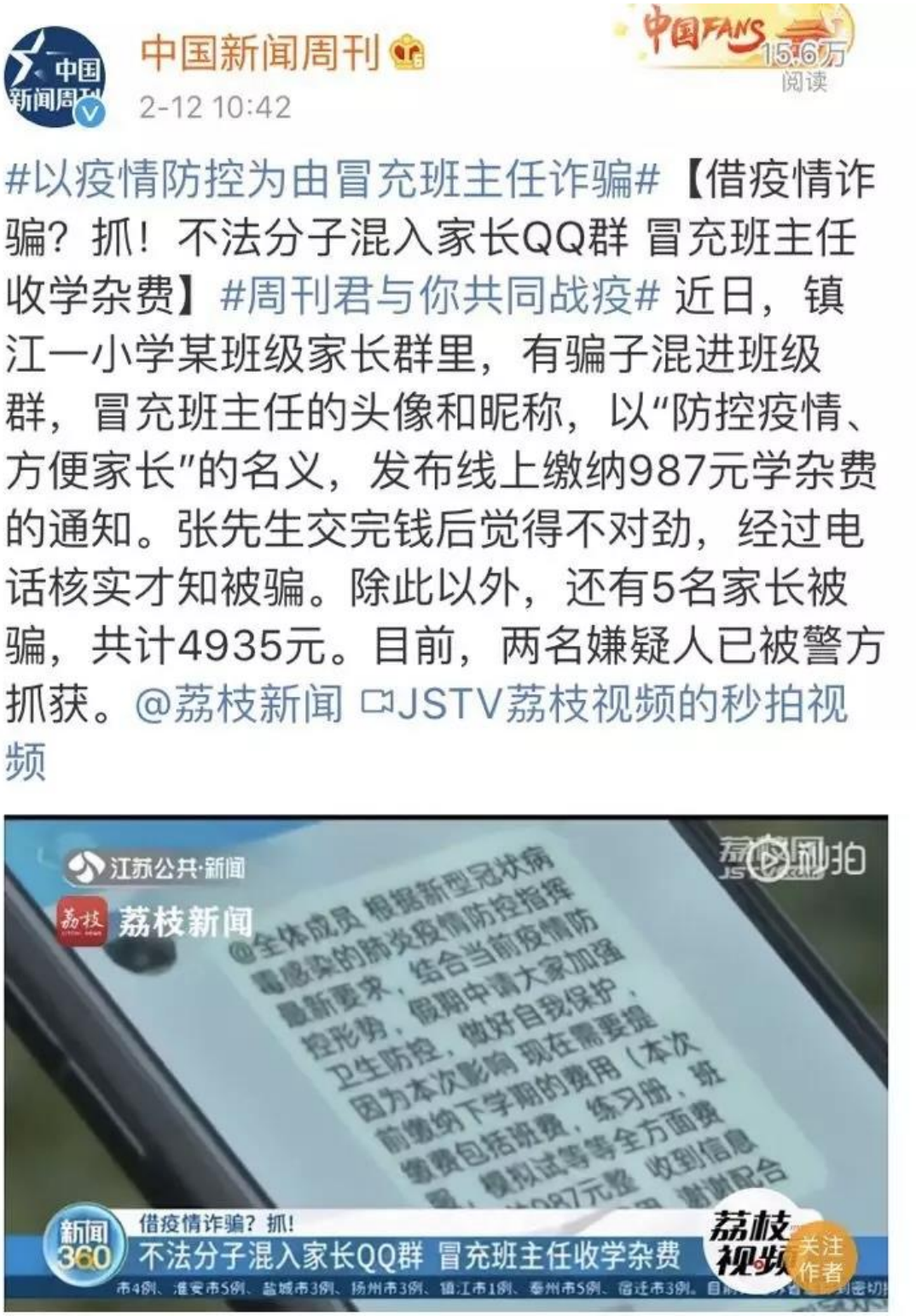
近期，据一些中小学生家长反映，有人通过班级微信群、QQ 群等媒介假冒学校教师或班主任身份，以延期开学和组织开展线上教学为由发布诈骗信息，要求学生家长通过微信、支付宝等网上支付方式缴纳各项费用，致使部分家长上当受骗。

对此，预警提醒，延期开学期间，教育部整合国家、有关省份和学校优质教学资源，开通国家中小学网络云平台和中国教育台电视空中课堂及部分省份网络学习平台，并提供有关教材电子版、“人教点读”数字教学资源库等学习资源，均为免费提供。

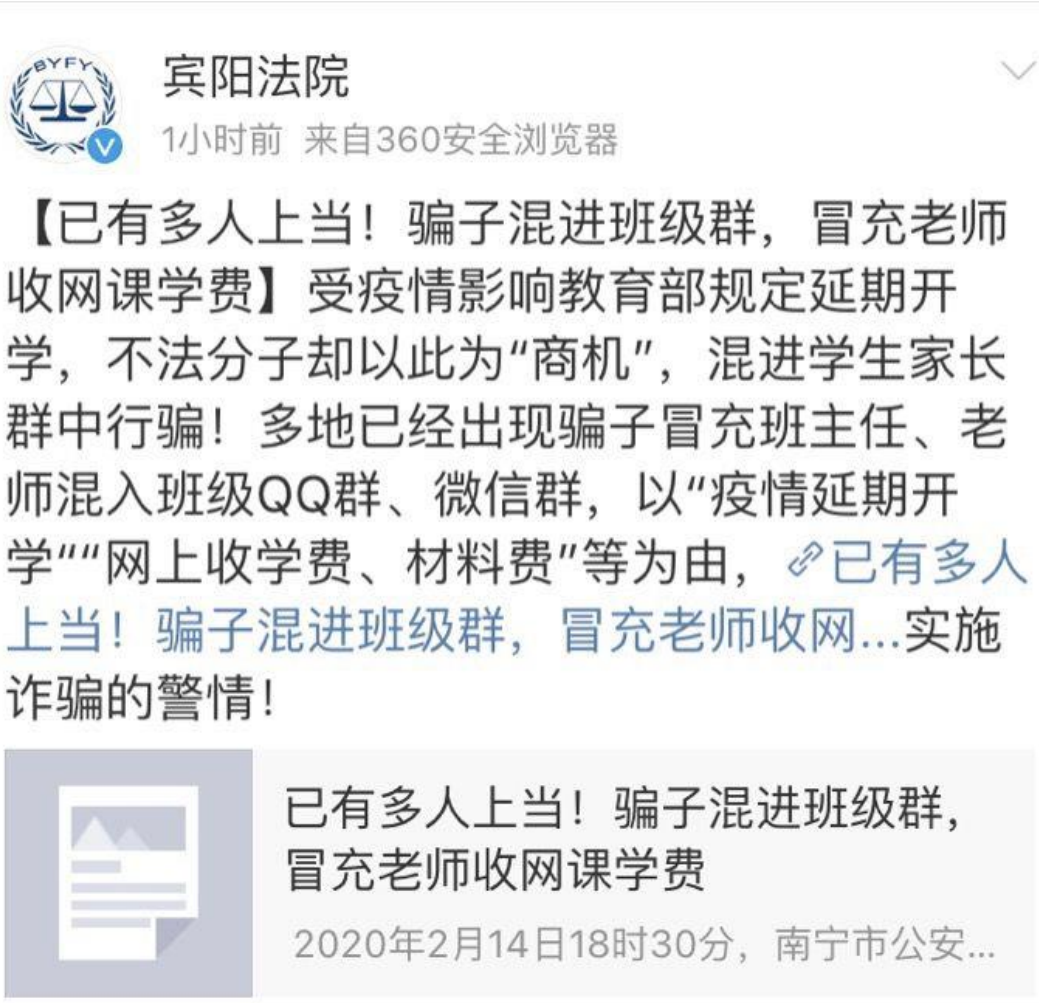
建议广大中小学生和家长，在积极做好疫情防控、有序开展线上学习的同时，对借此名义收取相关费用的行为，一定要提高警惕，增强防范意识，以免上当受骗，遭受不必要的经济损失。一旦发现可疑情况，应及时向学校和老师反映，并保存好相关证据、及时报警。

预警提出，严禁以疫情防控期间开展线上教学的名义擅自设立收费项目、违规收费。同时，对学校和班级建立的微信群、QQ 群等，要严格落实群主管理责任，严格核实所有成员身份，严格落实实名制度，严格入群批准验证，杜绝陌生人随意入群现象，对身份存疑的尽快清除出群。对确有需要通过网上支付的合规收费事项，建议学生和家长要与学校和老师进行确认，不可盲目进行网上支付。

此前，针对利用延期开学实施诈骗的行为，工信部也曾发布重要提醒，警惕疫情期间电信网络诈骗新套路——谨防延期开学，冒充老师骗取学费。



这样的骗术需小心



经搜索发现，利用疫情冒充班主任行骗的案件不在少数，已有多名家长“中招”。

警方提示：网上转账一定要核实真伪

对此，警方提醒：家长要学会分辨信息真假。学校一般不会在群内发送二维码，要求家长通过网络转账的方式支付学费。因此，不管是在微信群还是 QQ 群，家长在收到任何扫码交学费的消息，切勿急于汇款，一定要直接与班主任或校方核实真伪。

学校老师要加强联络群的管理。请老师（或群管理员） 开启入群验证功能 ，并实行实名制，对每一位入群的成员身份进行审核，避免陌生人随意加入家长 QQ、微信群。另外，各位老师应立刻对本班家长 QQ、微信群成员身份进行核查，对身份可疑人员，尽快清除出群。（来源：中国青年报）

➢ 美国一天然气公司在感染勒索软件后关闭两天

2020 年 2 月 20 日，美国国土安全部网络安全和基础设施安全署的公告显示，有一家未

公开名字的天然气公司在感染勒索软件后关闭设施两天。感染发生在该公司的天然气压缩设施，攻击始于钓鱼邮件内的恶意链接。

攻击者从其 IT 网络渗透到作业 OT 网络，其 IT 和 OT 网络都被勒索软件感染。感染没有扩散到控制压缩设备的可编程逻辑控制器，因此该公司没有失去对操作设施的控制。工作人员关闭了压缩设施两天，但由于管道传输的依赖性，它的关闭连带影响到了其它地方的压缩设施。（来源：solidot）

➢ 1060 多万名米高梅酒店客人信息被公布在黑客论坛上

2020 年 2 月 20 日，据外媒报道，本周，超 1060 万名住在米高梅国际度假(MGM Resorts)酒店的客人的个人详细信息被公布在了一个黑客论坛上。除了普通游客之外，遭新曝光的信息还包括了一些名人、科技公司老总、记者、政府官员以及来自全球最大科技公司的职工。米高梅度假村发言人通过电子邮件确认了这一事件。

泄露了什么？

根据外媒 ZDNet 的分析，今天被曝光的 MGM 数据转储包含了 10,683,188 名曾在 MGM 酒店住过的客人的个人详细信息。泄露的文件中包含了个人详细信息，诸如全名、家庭住址、电话号码、电子邮件和生日等。

ZDNet 跟一部分酒店客人进行了联系并确认他们曾住在这家酒店以及他们的时间表和泄漏文件中所含数据的准确性。结果他们得到了来自国际商务旅客、参加技术会议的记者、参加商务会议的 CEO 以及前往拉斯维加斯分支机构的政府官员的确认。

米高梅度假村称他们去年已经通知客人

米高梅发言人告诉 ZDNet，本周被发布到网上的数据源于去年发生的安全事件。“去年夏天，我们发现未经授权的云服务器访问，该云服务器包含了某些以前为米高梅度假村的某些客人提供的信息。我们有信心，这一事件并不涉及任何财务、支付卡或密码数据问题。”这家连锁酒店表示，将根据适用的州法律及时通知所有受影响的酒店客人。

此外，米高梅度假酒店还告诉 ZDNet，他们聘请了两家网络安全取证公司对发生在去年

的服务器数据泄露事件进行内部调查。

这家公司说道：“在米高梅度假酒店，我们非常重视保护访客数据的责任，并且我们已经加强和增强了网络的安全性以防止再次发生这种情况。”

SIM 交换和鱼叉式钓鱼的潜在危险

尽管去年米高梅的安全事件备受关注，但本周在一个人气黑客论坛上发布了此数据转储仍旧吸引了很多黑客的注意。发现此漏洞并通知记者的 Under the Breach 公司则强调了该漏洞存在的高度敏感性。该公司告诉 ZDNet，这些用户现在面临着接收鱼叉式网络钓鱼电子邮件以及 SIM 被更换的更高风险。据 Under the Breach 披露，他们在泄露文件中看到了 Twitter CEO 杰克·多尔西、流行歌手贾斯汀·比伯以及 DHS 和 TSA 一些官员的名字。

对此，米高梅度假酒店告诉 ZDNet，这些数据都是老数据。ZDNet 表示他们确实从今天致电的所有酒店客人中确认了这一说法，这些客人在 2017 年以后都没有入住过这家酒店。另外，该外媒拨打的某些电话号码也已经打不通，不过仍有许多电话号码能够接通并且有人接了电话。（来源：cnBeta）

➢ 4 人非法购买公民个人信息伪造 3D 头像 成功骗过支付宝人脸认证

2020 年 2 月 14 日，支付宝可能怎么也没想到，自己有一天也会被“诈骗”。怎么回事呢？近日，在裁判文书网上发现了一起刑事案件 ，根据浙江省衢州市中级人民法院的判决书显示，从 2018 年 7 月份开始，被告人张富、余杭飞等人以牟利为目的，使用其购买的公民个人身份信息注册支付宝账号，并使用软件将公民头像照片制作成公民 3D 头像，从而通过支付宝人脸识别认证。

通过这种方式来获取支付宝提供的邀请注册新支付宝用户的相应红包奖励（包括邀请新

人红包、通用消费红包、花呗红包等），而每个新注册支付宝至少可以获取 28 元收益。截止案发，该团伙非法收集近 2000 万条公民身份信息，共使用他人公民个人身份信息注册成功至少 547 个通过人脸识别认证的实名支付宝账户，获利 4 万元。

最终，被告人张某犯侵犯公民个人信息罪，判处有期徒刑四年，并处罚金人民币 10000 元；犯诈骗罪，判处有期徒刑一年，并处罚金人民币 5000 元，决定执行有期徒刑四年八个月，并处罚金人民币 15000 元。

虽然说此次被坑的是支付宝，金额也不是很巨大，但仅仅是这 4 个人非法窃取近 2000 万条公民信息并使用软件制作了 1153 个 3D 头像通过支付宝人脸认证的这一事实就足以让大家恐慌了。

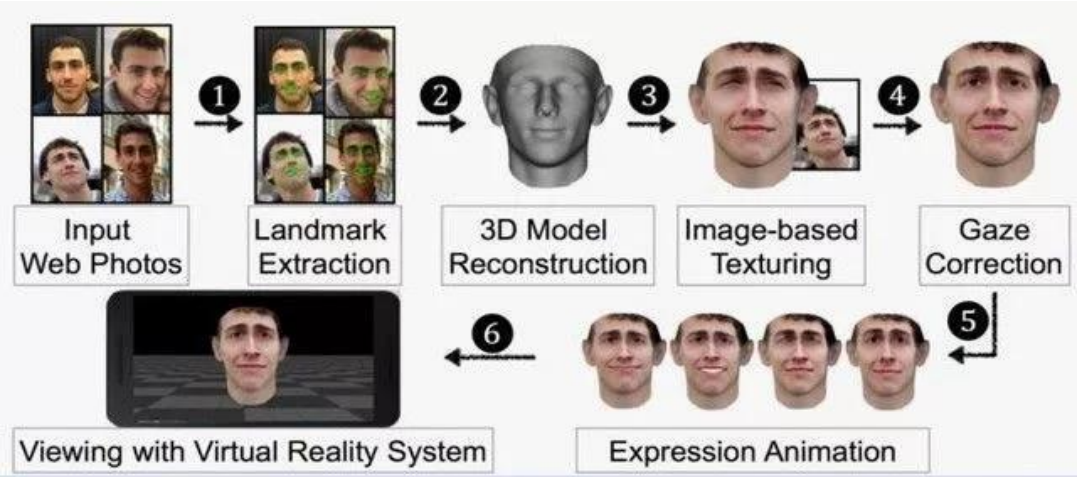
除此之外，编辑还发现一个更令人不安的事实，在本案中，涉案的四人仅仅是使用软件合成了 3D 头像便骗过了支付宝，难道支付宝的人脸认证系统就如此“不堪一击”吗？

其实不然

厦门大学信息学院教授 H 表示，以目前的技术，人脸认证系统还是有漏洞的，一定程度上是可以被破解 的，第一种是活体检测，这种基于活体识别的人脸识别确实有一定概率会被面具突破。

“虽然 AI 可以通过让你眨眨眼、抬抬头、张张嘴等互动，来检测你是不是活体，但不管怎样，AI 智能算法跟人的智能判别、智能识别，目前还是存在很大距离的。如果是精准度非常好并且细节十分到位的面具，那么对机器来说，分辨真假的确还是有难度的。”

第二种是人脸模型实时重建：即通过仿真的人脸建模，实时进行面部动作调整，从而实现真人动作模拟。而在网上公开自己的高清照片，确实有可能被 3D 建模，制作出高精度的面具，所以最好的办法还是保护好个人生物信息。



当然，大家也不用太担心，一般情况下，面具的制作成本高昂，他们是不会付出这么大

代价的，其次，此次的案件并不能说明支付宝的人脸认证系统是不安全的，只是犯罪分子抓住了其认证过程中的一个 bug 。（来源：深圳日报）

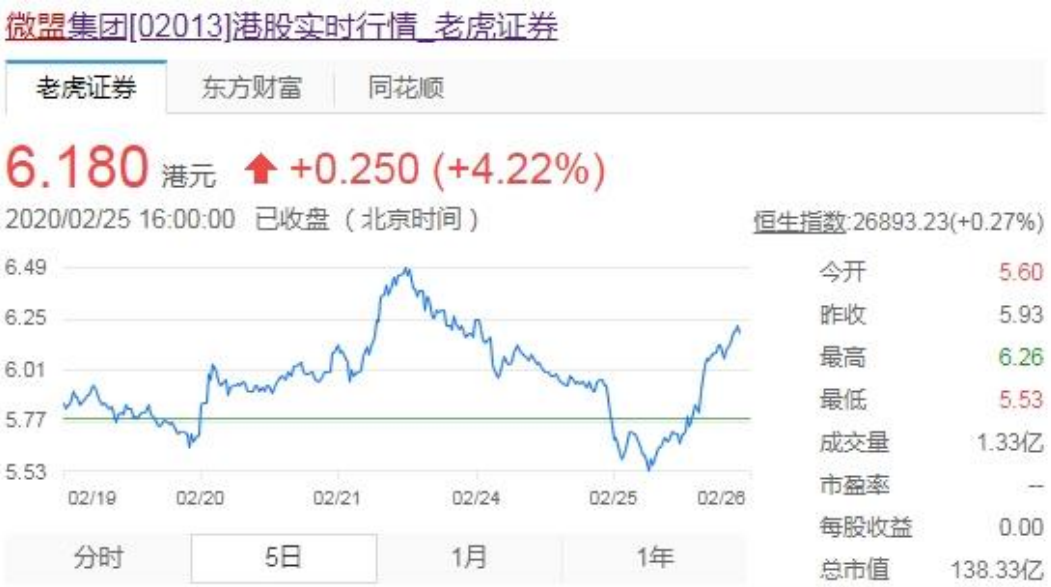
➢ 微盟系统遭运维删掉生产环境及数据宕机 36 小时

2020 年 2 月 25 日，微盟集团在港交所公告称，SaaS 业务数据遭到一名员工“人为破坏”。目前该员工已经被刑事拘留。微盟表示，自 2 月 23 日 19 点左右收到报警以来，公司正在全力恢复数据，拟定相关赔付方案来补偿此次事故而遭受损失的商家。

公司预计 2 月 25 日晚上 24 点前我们的生产环境将修复完成，微盟所有新用户将可恢复服务；老用户预计在 2 月 28 日晚上 24 点前完成。以 2 月 23 日 19 点开始计算，此次微盟出现了长达 53-125 小时的崩溃。

微盟集团官网介绍，微盟集团为香港主板上市企业，成立于 2013 年 4 月，现有员工超 3200 人，渠道代理商超 1600 家，注册商户超 300 万。微盟是中国中小企业云端商业及营销解决方案提供商，同时也是腾讯社交网络服务平台中小企业精准营销服务提供商。

从 2 月 24 日至 2 月 25 日员工恶意破坏事件的一天时间内，微盟集团市值约蒸发了约 9.63 亿港元。不过截至今日收盘，微盟收涨 4.22%，报 6.18 港元/股，已回到 24 日下跌前的水平。



微盟程序员精神崩溃，破坏服务器

微盟在公告中表示，2020 年 2 月 23 日 19 点左右，公司收到系统监控警报，获悉 SaaS

业务服务出现故障，随后公司立即召集相关技术人员进行排查，发现微盟服务器遭到了严重破坏。公司立即启动了应急响应机制，并与腾讯云技术团队一起研究制定修复方案。

截止到 2 月 25 日 7 点，微盟集团的生产环境和数据修复都在有序的进行，预计 2 月 25 日晚上 24 点前微盟集团的生产环境将修复完成，微盟所有新用户将可恢复服务；老用户由于数据修复时间问题，微盟集团将提供临时过渡方案，预计老用户数据修复将可在 2 月 28 日晚上 24 点前完成。

微盟在公告中还表示，“我们事后对恶意破坏生产环境的犯罪嫌疑人进行追踪分析，成功定位到犯罪嫌疑人登录账号及 IP 地址，并于 2 月 24 日向宝山区公安局报案，目前犯罪嫌疑人已经被宝山区公安局进行刑事拘留，犯罪嫌疑人承认了犯罪的事实。”

据悉，犯罪嫌疑人是微盟研发中心运维部核心运维人员贺某，贺某于 2 月 23 日晚 18 点 56 分通过个人 VPN 登入公司内网跳板机，因个人精神、生活等原因对微盟线上生产环境进行了恶意的破坏。

公告最后微盟声称，对于此次事故深表歉意，目前正在拟定相关的方案来弥补商家，同时也对因远程办公而疏忽对员工的精神状态的关注深表痛惜。

恢复时间长达 53 至 125 小时

在微盟崩溃之后，微博上话题“微盟崩溃超 24 小时”已有大量阅读。重多网友纷纷表示，依赖微盟运营的中小商家或许要损失惨重。此次微盟崩溃时间较长，从 2 月 23 日 19 点左右发现崩溃之后，预期新用户全部恢复需要等到 2 月 25 日晚 24 点，耗时 53 小时；老用户数据修复需要等到 2 月 28 日晚 24 点，耗时 125 小时。

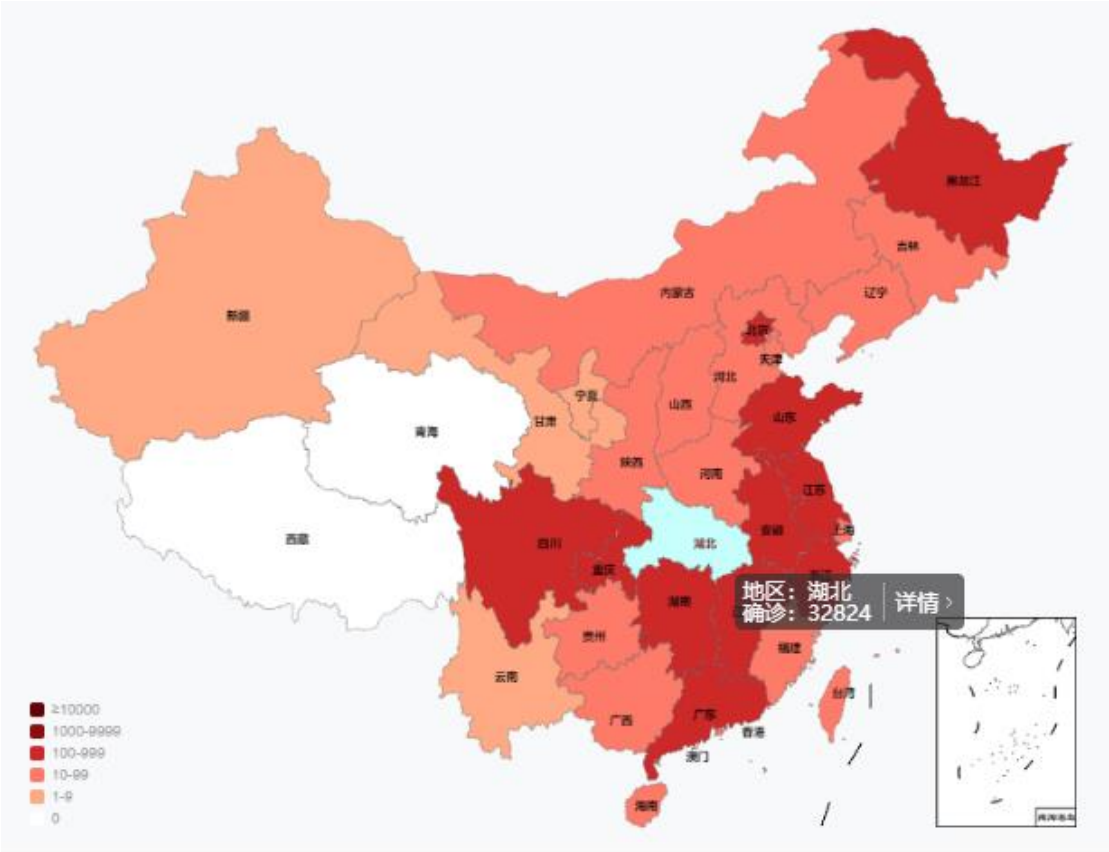
相比之下，去年 12 月 26 日微信公众号崩溃，腾讯恢复仅用 45 分钟。12 月 5 日下午 5 时左右，支付报也因为机房网络出现了短暂抖动，出现了时常 25 分钟左右的崩溃。

早在 2013 年 7 月，因为上海某施工队挖断了通信光缆，微信也曾经宕机 7 小时。但是，此次微盟出现了长达 53-125 小时的崩溃，远超支付宝和微信的记录。

对于微盟崩溃一事，微盟的合作方——腾讯云向观察者网表示：“腾讯云的技术团队已经在第一时间与微盟对接，研究制定修复方案，工程师们正在日夜赶工。我们将尽最大努力协助微盟降低损失。”（来源：观察者网）

➢ 多起泄露疫情信息的案例被通报：他们到底泄露了什么

2020 年 2 月 24 日，新冠肺炎疫情爆发以来，我们每天都能在第一时间获得权威部门发布的防控措施和医疗救治情况，从而全面了解疫情进展，知晓周围环境是否存在感染风险，掌握确诊或疑似人群行动轨迹，做到心中有数，不慌不乱。目前疫情形势已出现向好变化，防控工作取得积极成效。不得不说，在这场硬仗中，信息的及时公开发挥了关键作用。



但是近期网上有一些关于泄露疫情信息的案例通报。其中，有些当事人被免职，或被给予行政处分或行政处罚，还有一些被立案调查。

案例通报

大家可能会有疑问，既然疫情信息要公开透明，那么这些人为何会遭到处分呢，他们到底泄露了哪些不能公开的信息呢？


关于疫情防控工作中7起典型案例的通报
网易新闻 2020年02月06日 15:09
为强化警示震慑作用,督促切实履行疫情防控责任,现将近期查处部分典型案例通报如下...统战委员陈丹,老河口市大数据中心数据资源股股长黄飞违规泄露疫情防控工作信息问题... 查看更多相关资讯>> - 百度快照

公职人员泄露疫情防控信息,贵州遵义一区通报三起违纪案例
澎湃新闻 2020年02月04日 19:00
2月3日,中共贵州省遵义市汇川区纪律检查委员会通报了三起违反工作纪律泄露疫情防控信息的案例。 通报称,当前,正值新型冠状病毒感染的肺炎疫情防控关键时期,但在互联... 查看更多相关资讯>> - 百度快照

贺兰:通报1起违规泄露排查疫情信息的典型案例
新浪 2020年02月02日 08:34
原标题:贺兰:通报1起违规泄露排查疫情信息的典型案例来源:宁夏纪委监委网站1月29日,贺兰县纪委监委通报1起违规泄露排查...
查看更多相关资讯>> - 百度快照

海量涉疫情个人信息泄露 两地公安做出行政拘留处罚
中国经营网 2020年02月05日 10:36
打击涉疫情的造谣之外,对泄露隐私的惩处,也开启了序幕。... 近日,湖南、江西、内蒙古、山西四地,分别曝光了泄露涉疫情个人信息案例。其中,内蒙古、山西公安对泄露者做... 查看更多相关资讯>> - 百度快照

包头市纪委监委关于对三起疫情防控工作失职失责案例的通报
包头新闻网 2020年02月01日 20:03
广大党员干部的责任意识,现将近期查处的三起在疫情防控工作中失职失责案例通报如...将有关疫情防控信息发至社区卫生服务中心工作群,导致

泄露个人隐私

典型案例：2 月 3 日，某医院 5 名工作人员利用职务便利，私自用手机偷拍并通过微信转发传播该院新冠病毒肺炎感染者病程信息，其中包括患者姓名、详细住址、工作单位、诊疗信息等基本情况，造成恶劣影响，其行为已触犯《中华人民共和国治安管理处罚法》第四十二条第六项规定，被当地公安部门依法给予行政处罚。

《中华人民共和国治安管理处罚法》第四十二条规定：有下列行为之一的，处五日以下拘留或者五百元以下罚款；情节较重的，处五日以上十日以下拘留，可以并处五百元以下罚款。

“下列行为”共包含六项，第六项为：偷窥、偷拍、窃听、散布他人隐私的。

上述案例中 4 人受到了行政拘留十日、罚款五百元的处罚；另 1 人被罚款五百元。考虑到疫情原因，4 人的行政拘留暂缓执行。

之前还出现了集中登记的返乡人员姓名住址、联系方式、身份证号码等信息在朋友圈、微信群里被疯狂转发的情况。

疫情当前，大众迫切需要掌握高危人群的具体信息，这种心理完全可以理解。但是个

人信息比如联系方式的泄露，导致了通过电话骚扰、辱骂甚至威胁他人的不理性行为出现，给这些人群及家庭带来了干扰和伤害。

包括个人信息在内的大数据资源是我们防疫抗“疫”的一大法宝。比如，病例接触史等信息资源的公布共享，使得社区、医院等各方面能够掌握疫情防控的主动权。但是也要看到，在数据使用过程中，出现了违规收集、非法利用个人信息的情况，侵犯了个人隐私权，对他人造成二次伤害。

泄露工作秘密、内部信息

典型案例：某市政府拟恢复部分受到疫情影响的公交线路。在参与方案讨论过程中，2 月 2 日上午，该市公交公司运营管理部部长范某在方案未经上级批准的情况下，擅自将《关于恢复部分公交线路的通告（讨论稿）》发布至公司微信群。在没有证实信息准确性的情况下，公司 5 名中层干部在朋友圈进行了转发，造成了不良社会影响。该市公交公司党委决定对范某给予免职处理，其他 5 人给予诫勉谈话处理。

《中华人民共和国政府信息公开条例》第十六条规定：…… 行政机关在履行行政管理职能过程中形成的讨论记录、过程稿、磋商信函、请示报告等过程性信息以及行政执法案卷信息，可以不予公开。法律、法规、规章规定上述信息应当公开的，从其规定。

案例中被泄露的文件内容涉及疫情期间公共出行等备受关注的民生话题，且该方案处于讨论阶段，其中的公交线路信息和恢复时间都未最终确定。泄露后，一是会误导民众，造成人心不稳，特别是在疫情期间，会给民众本就因疫情造成的精神压力雪上加霜，从而产生对政府的不信任感；二是给日常生活秩序和社会秩序造成影响；三是给疫情期间的政府工作开展带来困难，给决策政令的施行造成被动。

身处疫情防控的非常时刻，要掌握好知情权与隐私权的平衡，拿捏好信息公开与保密的分寸。

意识要跟上

“各项工作都要为打赢疫情防控阻击战提供支持”。保密工作尤其要发挥出保平安、保稳定的作用。要清醒认识到，当前保护好秘密信息和个人隐私，与及时准确公开疫情信息一样，都是保护人民利益、维护国家安全和利益的重要工作，也是抗“疫”胜利的重要保障。既不能打着保密的幌子拒绝公开，也不能借着公开的理由抵触保密。

宣传要跟上

当前，疫情防控处于关键阶段，依法、科学、有序防控至关重要。在宣传信息公开的同时，要加大依法保护秘密信息和个人隐私的宣传力度。通过宣传推动机关、单位依法履

责，在法治轨道上统筹推进各项防控工作，引导广大人民群众增强法治观念，理解、支持和配合各项疫情防控工作。

《公务员法》第五十九条：公务员不得泄露国家秘密和工作秘密。

《民法总则》第一百一十一条：自然人的个人信息受法律保护。任何组织和个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。

措施要跟上

机关、单位特别是战斗在疫情防控一线的工作部门，要严肃保密纪律、落实保密要求，规范工作流程。在信息统计、文件起草等各工作环节，避免出现信息泄露、滥用、丢失等情况。要强化信息发布前的保密审查，按照法定主体、内容、程序、方式、时限等严格开展审查工作，确保上网不涉密、涉密不上网。对于已经泄露的信息，网信部门等应及时制止或阻断，避免对社会产生更多不良影响。对于泄露秘密信息特别是个人隐私的行为，要依法予以严厉打击。

中央网信办《关于做好个人信息保护利用大数据支撑联防联控工作的通知》中明确：任何单位和个人未经被收集者同意，不得公开姓名、年龄、身份证号码、电话号码、家庭住址等个人信息，因联防联控工作需要，且经过脱敏处理的除外。

该保密的严保死守，该公开的公开透明。现在正值防控疫情与复工复产的关键时期，公开+保密才能稳住民心、稳定大局，才能让没有疫情的春天更快到来。（来源：保密观）