国盟信息安全通报

2019 年 10 月 28 日第 204 期

国盟信息安全通报

（第 204 期）

国际信息安全学习联盟

2019 年 10 月 28 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 406 个，其中高危漏洞 100 个、中危漏洞 270 个、低危漏洞 36 个。漏洞平均分值为 5.60。本周收录的漏洞中，涉及 0day 漏洞 84 个（占 21%），其中互联网上出现“WordPressACF-Frontend-Display 插件文件上传漏洞、Libntlm 缓冲区溢出漏洞”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 3527 个，与上周（4763 个）环比减少 25%。

主要内容

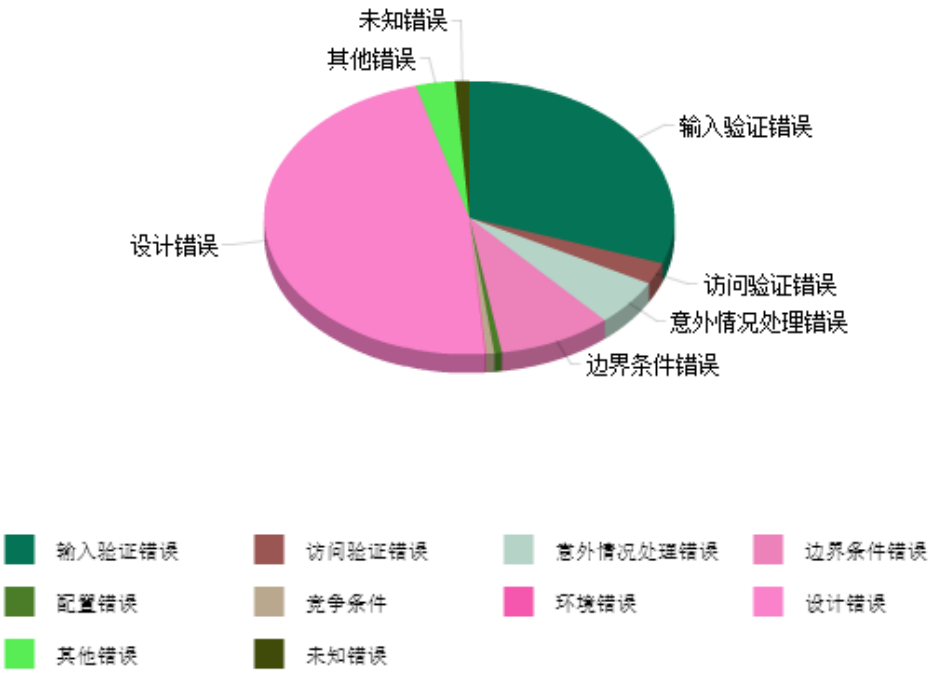
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

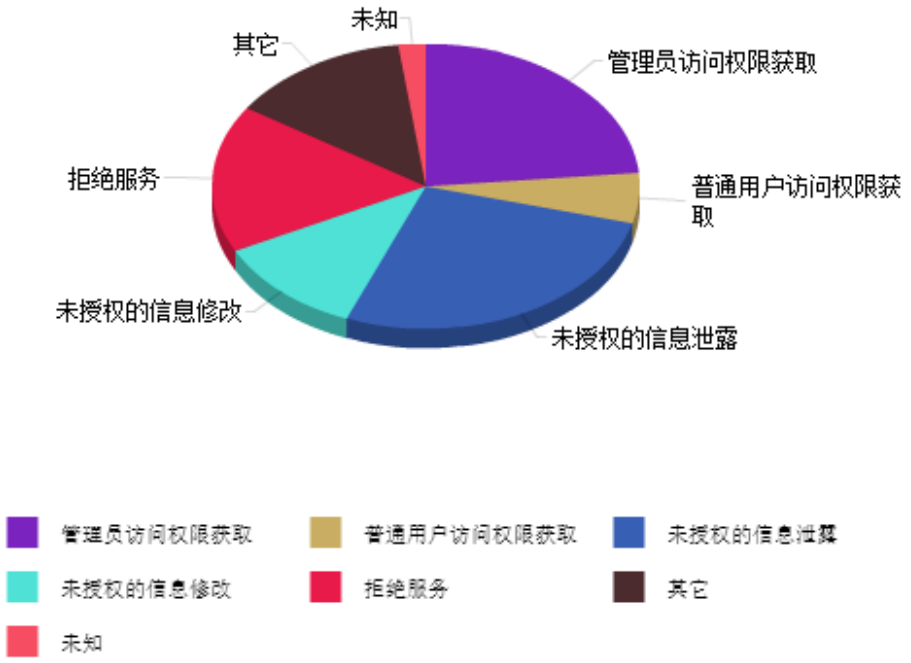
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 406 个，其中高危漏洞 100 个、中危漏洞 270 个、低危漏洞 36 个。漏洞平均分值为 5.60。本周收录的漏洞中，涉及 0day 漏洞 84 个（占 21%），其中互联网上出现“WordPressACF-Frontend-Display 插件文件上传漏洞、Libntlm 缓冲区溢出漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 3527 个，与上周（4763 个）环比减少 25%。

二、安全漏洞增长数量及种类分布情况

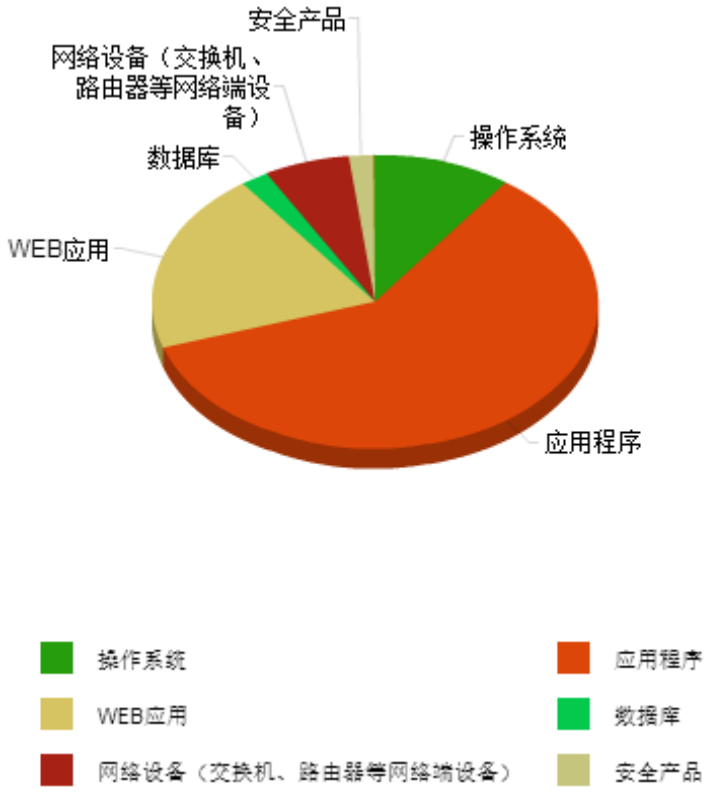
➢ 漏洞产生原因（2019 年 10 月 14 日—2019 年 10 月 28）



➢ 漏洞引发的威胁（2019 年 10 月 14 日—2019 年 10 月 28）



➢ 漏洞影响对象类型（2019 年 10 月 14 日—2019 年 10 月 28）



三、安全产业动态

➢ 习近平总书记关于网络安全和信息化工作重要论述综述

第六届世界互联网大会即将开幕，水乡乌镇又将站在世界的聚光灯下。这是一座因网而变、因网而兴的千年古镇：举办世界互联网大会以来，乌镇地区生产总值从 28 亿元增长至 64.6 亿元，互联网相关企业从 12 家增长为 900 余家。

“信息化为中华民族带来了千载难逢的机遇。”“当今世界，信息化发展很快，不进则退，慢进亦退。”“网信事业代表着新的生产力和新的发展方向。”在习近平总书记关于网络强国的重要思想指引下，我国互联网基础设施加快建设、自主创新能力不断增强、核心技术“弯道超车”、数字经济蓬勃发展、网络安全保障能力不断增强，网信事业取得了历史性成就，为世界互联网发展作出了中国贡献、创造了中国经验。

（1）网信事业代表着新的生产力和新的发展方向

“当今世界，科技革命和产业变革日新月异，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。”10 月 11 日，习近平总书记向 2019 中国国际数字经济博览会致贺信，强调中国正积极推进数字产业化、产业数字化，引导数字经济和实体经济深度融合，推动经济高质量发展。

信息革命、数字经济，是习近平总书记念兹在兹的一件大事。

2014 年 2 月 27 日，习近平总书记主持召开中央网络安全和信息化领导小组第一次会议时就强调，当今世界，信息技术革命日新月异，对国际政治、经济、文化、社会、军事等领域发展产生了深刻影响。信息化和经济全球化相互促进，互联网已经融入社会生活方方面面，深刻改变了人们的生产和生活方式。我国正处在这个大潮之中，受到的影响越来越深。

2016 年 4 月 19 日，在网络安全和信息化工作座谈会上，习近平总书记进一步指出，从社会发展史看，人类经历了农业革命、工业革命，正在经历信息革命。信息革命增强了人类脑力，带来生产力又一次质的飞跃。

2018 年 4 月 20 日，全国网络安全和信息化工作会议召开，习近平总书记发表重要讲话强调，网信事业代表着新的生产力和新的发展方向，应该在践行新发展理念上先行一步，围绕建设现代化经济体系、实现高质量发展，加快信息化发展，整体带动和提升新型工业化、城镇化、农业现代化发展。

科技兴则民族兴，科技强则国家强。1994 年，互联网诞生 25 年后，中国才第一次实现与国际互联网的全功能链接。又过了 25 年，今天的中国数字经济正在实现“弯道超车”。

统计数据显示，截至 2019 年 6 月，我国网民规模达 8.54 亿，互联网普及率达 61.2%，网络支付用户规模达 6.33 亿；2018 年，移动支付规模达 277.4 万亿元，稳居全球第一，数字经济规模超过 30 万亿元，占 GDP 比重达 1/3，居全球第二位……

从无到有、从小到大、由大渐强，中国互联网跨越式发展的背后，是习近平总书记关于网络强国的重要思想的科学引领，是以习近平同志为核心的党中央的坚强领导和大力推进。

（2）让人民群众在信息化发展中有更多获得感、幸福感、安全感

甘肃陇南，素有“秦陇锁钥，巴蜀咽喉”之称，高山峻岭与峡谷盆地相间，自古以来交通就十分不便。

可在“80 后”姑娘梁倩娟眼里，高山挡不住她与外部世界的联系。靠着一根网线，轻点几下鼠标，梁倩娟的网店将地里的辣椒、树上的花椒、山中的野菜卖到了山外，由此带动了 300 多户农户增收，其中包括 100 多户贫困户。

梁倩娟网店的成功，正是“网信事业发展为了谁”的生动回答。

习近平总书记反复强调：“网信事业发展必须贯彻以人民为中心的发展思想，把增进人民福祉作为信息化发展的出发点和落脚点，让人民群众在信息化发展中有更多获得感、幸福感、安全感。”

“相比城市，农村互联网基础设施建设是我们的短板。”习近平总书记对推动农村网络发展有着深深挂念和殷切希望，强调要加大投入力度，加快农村互联网建设步伐，“发挥互

联网在助推脱贫攻坚中的作用，推进精准扶贫、精准脱贫，让更多困难群众用上互联网，让农产品通过互联网走出乡村，让山沟里的孩子也能接受优质教育”。

在各地各部门的持续努力下，我国农村互联网建设进度飞快，网络扶贫行动取得明显成效。截至目前，贫困村通宽带比例达到 97%，纳入电子商务进农村综合示范的贫困县网络零售额超过 1700 亿元，数字乡村发展战略极大地激发了农村的创新活力。

从农村到城市，今天的互联网早已成为人们学习、工作、生活的新空间，成为人们获取公共服务的新平台。

“我们要深刻认识互联网在国家管理和社会治理中的作用，以推行电子政务、建设新型智慧城市等为抓手，以数据集中和共享为途径，建设全国一体化的国家大数据中心，推进技术融合、业务融合、数据融合，实现跨层级、跨地域、跨系统、跨部门、跨业务的协同管理和服务。”2016 年 10 月 9 日，习近平总书记在主持中共中央政治局第三十六次集体学习时强调，随着互联网特别是移动互联网发展，社会治理模式正在从单向管理转向双向互动，从线下转向线上线下融合，从单纯的政府监管向更加注重社会协同治理转变。

在杭州，“城市大脑”每天要汇入来自全市 70 余个部门和企业的数据，日均新增数据达到 8000 万条以上，包括警务、交通、城管、文旅、卫健等 11 大系统、48 个应用场景，给老百姓生活带来方方面面的新变化；在深圳，借助互联网大数据研判车流监测准确率达 95%以上，道路通行能力提高 8%以上，30 分钟就能形成交通情报精准推送。

“数字红利”加快释放，“互联网+”深入生活，深刻地改变了每个人的生活方式，越来越多的人享受到了网络和信息化的发展成果。

（3）网络空间是亿万民众共同的精神家园

“我和我的祖国，一刻也不能分割……”国庆前夕，一段“快闪”视频风靡互联网，激发出全体中华儿女热爱祖国的澎湃热情和强烈共鸣。近年来，类似这样满满正能量的作品屡屡引爆互联网。

“网络空间是亿万民众共同的精神家园。网络空间天朗气清、生态良好，符合人民利益。网络空间乌烟瘴气、生态恶化，不符合人民利益。”习近平总书记多次强调，要依法加强网络空间治理，加强网络内容建设，做强网上正面宣传，培育积极健康、向上向善的网络文化，用社会主义核心价值观和人类优秀文明成果滋养人心、滋养社会，做到正能量充沛、主旋律高昂，为广大网民特别是青少年营造一个风清气正的网络空间。

依法治网、依法办网、依法上网，让互联网在法治轨道上健康运行，这是修复和营造良好网络生态的关键环节。针对过度炒作娱乐八卦、宣扬炫富拜金等错误价值观的现象，多个

部门协同发力、重拳出击，荡涤污泥浊水；针对互联网黑色产业链猖獗，涉网犯罪案件高发的情况，“净网”行动雷霆出击、犁庭扫穴；针对移动互联网应用强制授权、过度索权、超范围收集个人信息的现象，加强立法工作，从源头堵住漏洞……

互联网是一个社会信息大平台，亿万网民在上面获得信息、交流信息，这会对他们的求知途径、思维方式、价值观念产生重要影响，特别是会对他们对国家、对社会、对工作、对人生的看法产生重要影响。习近平总书记强调：“为了实现我们的目标，网上网下要形成同心圆。什么是同心圆？就是在党的领导下，动员全国各族人民，调动各方面积极性，共同为实现中华民族伟大复兴的中国梦而奋斗。”

为此，习近平总书记明确要求，各级党政机关和领导干部要学会通过网络走群众路线，善于运用网络了解民意、开展工作，“网民来自老百姓，老百姓上了网，民意也就上了网。群众在哪儿，我们的领导干部就要到哪儿去，不然怎么联系群众呢？”

互联网的迅猛发展，同样深刻改变着舆论生成方式和传播方式。

2019 年 1 月 25 日，中共中央政治局在人民日报社就全媒体时代和媒体融合发展举行第十二次集体学习。习近平总书记在讲话中强调，全媒体不断发展，出现了全程媒体、全息媒体、全员媒体、全效媒体，信息无处不在、无所不及、无人不用，导致舆论生态、媒体格局、传播方式发生深刻变化，新闻舆论工作面临新的挑战，“宣传思想工作要把握大势，做到因势而谋、应势而动、顺势而为。我们要加快推动媒体融合发展，使主流媒体具有强大传播力、引导力、影响力、公信力，形成网上网下同心圆，使全体人民在理想信念、价值理念、道德观念上紧紧团结在一起，让正能量更强劲、主旋律更高昂。”

没有网络安全就没有国家安全，没有信息化就没有现代化

全球知名网络企业被曝遭黑客攻击，涉及近 5000 万用户；某著名连锁酒店有超过 1.3 亿入住用户的数据包被非法出售，泄露数据总数高达 5 亿条；芯片公司宣布芯片存在严重设计漏洞，引发“计算机史上最大安全事件”；勒索病毒肆虐全球，一天之内横扫 150 多个国家和地区……

当网络空间成为国家继陆、海、空、天之后的第五疆域，保障网络空间安全就是保障国家主权。

“没有网络安全就没有国家安全，没有信息化就没有现代化。”习近平总书记的这一重要论断，把网络安全上升到了国家安全的层面，为推动我国网络安全体系的建立，树立正确的网络安全观指明了方向。

安全是发展的前提，发展是安全的保障，安全和发展要同步推进。习近平总书记指出，

网络安全和信息化是相辅相成的，“网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进、统一实施。做好网络安全和信息化工作，要处理好安全和发展的关系，做到协调一致、齐头并进，以安全保发展、以发展促安全，努力建久安之势、成长治之业。”

近年来，我国网络安全法治建设取得突破性进展。2016 年 11 月，《中华人民共和国网络安全法》高票通过，成为我国网络安全领域的首部专门法律，为依法治网、化解网络风险提供了法律武器；2017 年 3 月，十二届全国人大五次会议通过《民法总则》，明确对个人信息、数据、虚拟财产予以保护；最高法、最高检出台一系列司法解释，阐明相关法律问题；中央网信办、公安部、工信部、文化部等出台多个部门规章，对互联网信息搜索、移动互联网应用程序等及时依法规范……

网络安全威胁和风险日益突出，并逐渐向政治、经济、文化、社会、生态、国防等领域传导渗透。这是令世界各国都头疼的难题，我国也不例外。

9 月 16 日，2019 年国家网络安全宣传周在天津拉开帷幕。习近平总书记作出重要指示强调，国家网络安全工作要坚持网络安全为人民、网络安全靠人民，保障个人信息安全，维护公民在网络空间的合法权益。要坚持网络安全教育、技术、产业融合发展，形成人才培养、技术创新、产业发展的良性生态。要坚持促进发展和依法管理相统一，既大力培育人工智能、物联网、下一代通信网络等新技术新应用，又积极利用法律法规和标准规范引导新技术应用。要坚持安全可控和开放创新并重，立足于开放环境维护网络安全，加强国际交流合作，提升广大人民群众在网络空间的获得感、幸福感、安全感。

网络安全产业迅速发展领跑全球、中国网络空间安全协会等各类新型网络社会组织纷纷成立、“网络空间安全”成为一级学科、连续多年举办全国高校网络安全联赛、国家网络安全宣传周走进寻常百姓……近年来，在各方面的齐抓共管下，网络安全的共治共建渐入佳境。

让网络空间命运共同体更具生机活力

从北京飞纽约最少需要 13 个小时，而在北京访问纽约的网站，一秒钟都用不了。从诞生以来，互联网就以其“无远弗届”的特点，迅速发展壮大。在虚拟的网络空间里，三维世界成了二维平面，人类从来没有如现在这般紧密相连。

“每一次产业技术革命，都给人类生产生活带来巨大而深刻的影响。现在，以互联网为代表的信息技术日新月异，引领了社会生产新变革，创造了人类生活新空间，拓展了国家治理新领域，极大提高了人类认识世界、改造世界的能力。互联网让世界变成了‘鸡犬之声相闻’的地球村，相隔万里的人们不再‘老死不相往来’。可以说，世界因互联网而更多彩，

生活因互联网而更丰富。”2015 年 12 月 16 日，习近平总书记在第二届世界互联网大会开幕式上发表主旨演讲。正是在这篇演讲中，习近平总书记率先提出推进全球互联网治理体系变革应坚持的“四项原则”：尊重网络主权、维护和平安全、促进开放合作、构建良好秩序。他还就共同构建网络空间命运共同体提出“五点主张”：加快全球网络基础设施建设，促进互联互通；打造网上文化交流共享平台，促进交流互鉴；推动网络经济创新发展，促进共同繁荣；保障网络安全，促进有序发展；构建互联网治理体系，促进公平正义。

自此，“乌镇声音”成为引领互联网国际合作的友谊之声，“共同构建网络空间命运共同体”的主张，也逐渐成为全球共识。在这份充盈着中国智慧的中国方案中，传递出负责任大国的勇毅担当。

“世界各国虽然国情不同、互联网发展阶段不同、面临的现实挑战不同，但推动数字经济发展的愿望相同、应对网络安全挑战的利益相同、加强网络空间治理的需求相同。各国应该深化务实合作，以共进为动力、以共赢为目标，走出一条互信共治之路，让网络空间命运共同体更具生机活力。”2018 年 11 月 7 日，习近平总书记在致第五届世界互联网大会的贺信中希望大家集思广益、增进共识，共同推动全球数字化发展，构建可持续的数字世界，让互联网发展成果更好造福世界各国人民。

“‘中国网络观’让人印象深刻。”著名计算机科学家罗伯特·卡恩说，习近平主席的一揽子阐述，表明了互联网是一个非常独特的共同家园，所有人都应该共同承担责任。

从《网络空间国际合作战略》的发布，到杭州 G20 峰会《二十国集团数字经济发展与合作倡议》的签署；从共同推动互联网关键资源管理权完成转移，到积极助推互联网域名地址分配机构的国际化进程……中国在推动构建网络空间命运共同体中扮演的角色越来越重要。

在习近平新时代中国特色社会主义思想指引下，我们有信心也有决心探索网络强国建设新路径，开拓全球网络治理新境界，让互联网成为实现中华民族伟大复兴中国梦的强大助力。

（来源：人民日报）

➢ 详解个人信息安全规范：注销时不得额外收集信息人工处理 15 天内完成

2019 年 10 月 24 日，App 专项治理工作组公布了国家标准 GB/T 35273《信息安全技术 个人信息安全规范》更新后的征求意见稿。相比 6 月份的征求意见稿，新版征求意见稿规定，App 应提供简便易操作的注销功能，核验身份时不得要求用户提供超过注册、使用时收

集的个人信息。

用户注销时不应提供多于注册时收集的信息

一直以来，App“注册容易注销难”被用户广泛诟病。隐私护卫队曾实测 12 款常用 App 的注销功能，发现有七款无法注销，有的注销选项位置隐蔽，还有 App 注册时用手机验证码登录即可，注销时却必须满足上传手持身份证照片、解绑其他账号等多个条件。

中国电子技术标准化研究院信安中心审查部总监何延哲举例说，有 App 甚至要求用户提供 2019 年 5 月 1 日使用 App 的地点。此外，不少 App 没有在隐私政策中承诺注销后会对相关个人信息采取删除或匿名化处理。上述问题均在新版征求意见稿中得到了更加细致地规范。

新版征求意见稿要求，App 应提供便捷的注销功能交互界面，及时响应用户的注销请求；需人工处理的，应在承诺期限内（原则上不超过 15 天）完成核查和处理。

此外，注销核验身份时不得要求用户重新提供多于注册、使用等服务环节收集的个人信息；注销时不应设置不合理的条件或提出额外的要求增加个人信息主体的义务，比如注销单个账户视同注销多个产品或服务等。

何延哲指出，注销规定的变化“非常明显”。“用户收集、使用个人信息时要合法、正当、必要，注销时也应如此。”他认为，出于对用户账号利益的保护，为避免账号被盗、被恶意注销等，注销时核验用户身份是可以的，但不能借着核验的目的“实现别的心思”，如防止用户流失、多获取用户其他信息等。“不是说注销要一味地追求简单，而是要合情合理不能设置过分的要求”。何延哲强调，注销既要从用户角度考虑，也要考虑企业的要求。

App 未告知第三方身份或将在信息泄露事件中负全责

在互联网产品和服务的生态中，App 为实现多种功能，跟第三方的合作必不可少。南都个人信息保护研究中心、中国金融认证中心于今年 7 月发布的《常用第三方 SDK 收集使用个人信息测评报告》显示，平均每款 App 使用 19.3 个第三方 SDK（软件开发工具包），有些用户的个人信息也可能流入 SDK。

除了嵌入第三方 SDK，与第三方公司合作也十分常见。最近 51 信用卡被警方调查就是因为其合作的第三方催收公司采取恐吓、滋扰等软暴力手段催收债务。据了解，借款人的电话号码、通信记录等个人信息通常是与催收公司共享的。

那么，如果因第三方保管不力而发生信息泄露事件，双方应分别承担哪些责任？何延哲告诉隐私护卫队，“结合实践中发现的问题，（新版征求意见稿）把双方责任进行了细化。”

新版征求意见稿要求，在作出委托时，个人信息控制者不应超出用户授权同意的范围，且需确保受委托者达到一定安全能力，还要监督受委托者。责任划分方面，因共享、转让个人信息发生安全事件而对用户合法权益造成损害的，个人信息控制者应承担相应的责任。

值得注意的是，如果个人信息控制者未明确告知用户第三方身份，以及自身和第三方应分别承担的责任和义务，个人信息控制者应承担因第三方引起的个人信息安全责任。分享、转让个人信息，委托第三方处理等现象，是业态的常规做法，有时为了完成某些功能，必须这么做，但“这个过程容易造成问题，容易失控”，何延哲说。

他指出，未分享、转让时，用户可找第一方落实权利，而共享、转让之后，第三方也变成了个人信息的控制者，且可以决定用途，此时，用户的控制能力下降，权利落实也更加困难。“第一方既然能决定把个人信息给谁，也应该履行一部分监督、管理的责任，同时，第三方成为控制者之后也应落实安全规范。”

关闭新闻推送时 App 应提供删除或匿名化个人信息的选项

App 收集用户浏览记录、搜索记录、文章阅读偏好等个人信息最主要的用途之一，就是用户画像，进而被用于精准推送。在 App 的“后台”，每一个用户的每一次点击都被剖析和标签化。

App 为用户打上了哪些标签，用户有权了解吗？用户能通过编辑标签，决定推送广告的内容吗？据了解，目前绝大多数 App 并没有相关功能。

新版征求意见稿建议，App 向用户提供个性化展示的，宜建立用户对个人信息（如标签、画像维度）的自主控制机制，保障用户调控个性化展示相关程度的能力。

隐私护卫队注意到，关闭或退出新闻相关的精准推送功能，App 被要求“提供删除或匿名化定向推送活动所基于的个人信息的选项”，广告推送则没有。

“新闻推送比广告信息更敏感。”何延哲表示，用户看到定向推送的广告，可以不购买商品或服务，而新闻不一样，只要看到就接收了信息，“相当于不买也得买，且会影响人的判断”。所以，对新闻的定向推送应该管控的更严格一点，给用户的选择权更大一点。

新版征求意见稿还进一步定义，能够单独或和其他信息结合识别用户或反应用户活动的用户画像和特征标签属于“个人信息”；通过加工处理后的信息，一旦泄露、非法提供可能危害人身安全，极易导致个人名誉受损等，属于个人敏感信息。

并且，App 不得以改善服务质量、提升用户主体体验、研发新产品、增强安全性等为由，强迫用户同意收集个人信息。“如果以上述理由收集用户的个人信息，是要有条件的。”何延哲强调，首先鼓励 App 将上述内容详细阐述；其次 App 不能把上述条件当成兜底条件，凡是搭边的信息都收集；最重要的是不能因为上述条件而强迫用户同意。（来源隐私护卫队）

- **GB/T35273《信息安全技术 个人信息安全规范（征求意见稿）1024 最新版》全文**
- http://pip.tc260.org.cn/assets/wz/2019-10-23/266aa3db-af73-4c65-bdcd-d1743713c190.pdf

➢ 做好网络安全工作须把握五个要点

习近平总书记对国家网络安全宣传周作出重要指示，强调要坚持安全可控和开放创新并重，坚持促进发展和依法管理相统一，提升广大人民群众在网络空间的获得感幸福感安全感，这是对当前网络安全工作提出的具体要求和行动指南。贯彻落实总书记重要指示精神，做好网络安全工作要瞄准一个总体目标，理清两个主要关系，把握三个通用原则，聚焦四项重点任务，统一五个标准规范。

瞄准一个总体目标。聚焦于党的领导下网络强国建设的统一目标，实现从网络大国到网络强国跃升。正如习近平总书记所强调的，“要从国际国内大势出发，总体布局，统筹各方，创新发展，努力把我国建设成为网络强国”。具体来讲，就是要建设网络强国、数字中国、智慧社会，推动互联网、大数据、人工智能和实体经济深度融合，发展数字经济、共享经济，培育新增长点、形成新动能。

理清两个主要关系。理清网络安全与信息化发展、网络使用与网络监管的关系，牢牢把握网络安全的战略地位。一是处理好网络安全与信息化发展的关系。习近平总书记强调，“网络安全和信息化是相辅相成的。安全是发展的前提，发展是安全的保障，安全和发展要同步

推进”“网络安全和信息化要同步推进，网络安全和信息化是一体之两翼、驱动之双轮”“没有网络安全就没有国家安，没有信息化就没有现代化”。二是处理好网络使用与网络监管的关系。网络空间不是法外之地，有使用就要有监管，要进一步加大监督管理力度。国家层面有《网络安全法》以“法”的形式对网络运行、信息安全和网络行为作出了明确规定。企业层面有《互联网新闻信息服务管理规定》《微信公众平台运营规范》等一系列规定，做到了有法可依。无论是网络使用者，还是平台建设者，都要遵守国家法律法规和社会道德规范。

把握三个通用原则。就是要理解好三个“对立统一”，处理好促进发展与依法管理的矛盾。一是既要齐抓共管，又要百花齐放。无论是网络管理者，还是服务提供者，在思想认识上都必须与党和国家的要求高度统一，在具体网络应用领域可以各有特色，鼓励个性化发展，满足个性化需求。在资源整合和网络监管等方面，要统一标准，共管共治，共同维护信息安全和网络清明。二是既要从上到下，又要自下而上。无论是国家层面，还是地方层面，在网络建设和信息化发展的顶层设计、规划制定时，可以采取从上到下的方式，便于统一标准和贯彻执行。在具体项目和系统开发时，可以采取自下而上的方式，积极鼓励试点和经验推广。三是既要安全保底，又要加快发展。在网络和信息化发展方面，各地情况不同，应当结合实际因地制宜开展工作。要将网络安全摆在首位，牢牢守住安全底线，但又不可因噎废食成为约束，要边建设边防护，将制度约束和技术措施结合起来，正确处理好网络安全和信息化发展之间的关系。

聚焦四项重点任务。就是要坚持安全可控和开放创新并重，做好网络的“管”“防”“建”“用”。一是加强互联网管理。在已有法律法规和管理规范的基础上，建立健全与互联网有关的管理制度，细化相关实施细则，做到有章可循，明确政府、企业、个人在维护网络安全

和网络清明等方面的职责义务。二是加强网络安全防护。建立健全网络风险评估、网络安全预警、情况通报等制度，努力建设高素质的网络安全和信息化人才队伍，确保人员、技术双到位。三是加快网络建设和推广。从网络大国到网络强国是国家战略，不同主体、不同个人应有不同职责。网络服务提供者要结合实际，从用户需求出发，提供安全稳定的网络环境和方便快捷的应用体验。网络管理者要加强对网络和信息系统开发的指导和监督，提升信息化的应用效果。四是加快互联网成果应用。加快互联网知识普及，加快网络基础设施建设，加快数据资源建设共享，加快最新信息技术转化，使互联网更加“接地气”，提高人民群众在网络空间的获得感幸福感安全感。

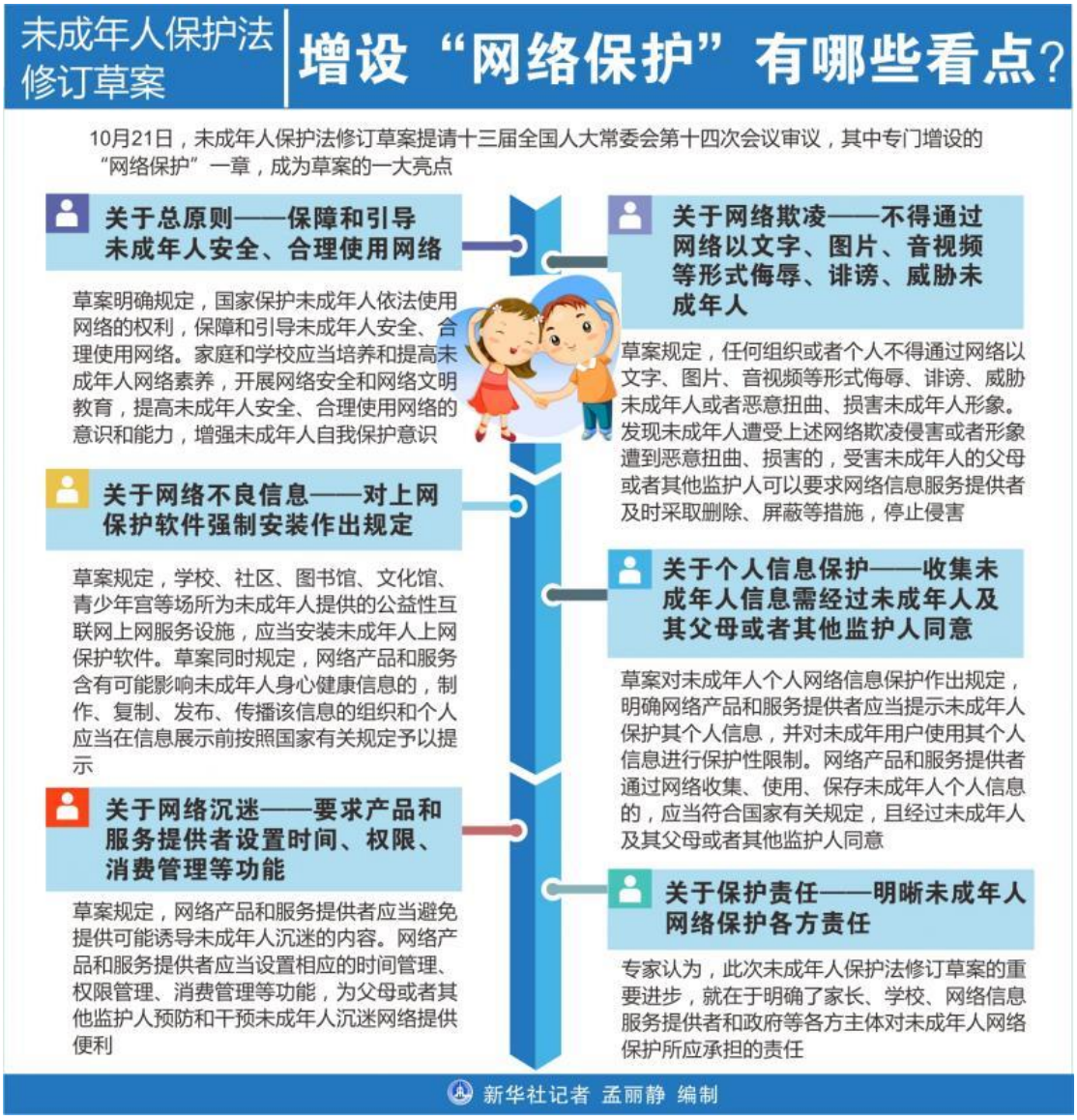
统一五个标准规范。就是要规范“制度““技术”“数据”“安全”“考核”五类标准。一是完善规章制度。建章立制，规范管理，建立统一的使用管理机制，是确保网络安全、加快互联网成果转化的前提。目前来看，法律条款、行为规范已经很多，但具体的管理办法、有效的网络安全机制等操作层面的内容还较为紧缺。二是统一技术规范。按照国家信息系统整合共享的基本要求，加强信息部门的统一规划能力，建立信息系统先评估、后建设、再使用制度。在方案设计、网络和信息系统开发等方面，应当遵循国家标准、行业规定或国际惯例，采用最新最成熟的信息化技术手段。三是统一数据格式。从互联网应用的角度看，数据资源共享等方面还缺少统一的规范标准，不利于国家提倡的信息资源整合共享的总体思路，应当尽快研究制定国家层面的数据资源建设、应用的规范标准并加快推广。四是统筹安全规划。互联网发展过速，安全防护未能及时跟上。整体来看，符合国情民情的网络安全评估规划较少，且各自为政尚未统一。不同类型的网络建设者应当结合各自实际，拟制网络安全长期或短期规划，作为开展网络安全工作的依据。五是完善考评标准。加强对网络建设者和网络服务商的管理迫在眉睫，应当尽快引入考核评估和督查手段，将网络安全摆在首位，先防护、再建设，边建设、边规范，利用技术手段加强技术治理，从建设源头和使用末端同时发力，共同保护好网络安全，维护好网络清明。（来源：学习时报　作者：刘海军　李晴）

➢ 未成年人保护法修订草案增设“网络保护”，哪些看点值得关注？

2019 年 10 月 21 日，未成年人保护法修订草案提请十三届全国人大常委会第十四次会议审议，其中专门增设的“网络保护”一章，成为草案的一大亮点。

全国人大社会建设委员会主任委员何毅亭在作关于修订草案的说明时介绍，修订草案增

设“网络保护”专章，对网络保护的理念、网络环境管理、网络企业责任、网络信息管理、个人网络信息保护、网络沉迷防治、网络欺凌及侵害的预防和应对等作出全面规范，力图实现对未成年人的线上线下全方位保护。



【看点一】关于总原则——保障和引导未成年人安全、合理使用网络

草案明确规定，国家保护未成年人依法使用网络的权利，保障和引导未成年人安全、合理使用网络。家庭和学校应当培养和提高未成年人网络素养，开展网络安全和网络文明教育，提高未成年人安全、合理使用网络的意识和能力，增强未成年人自我保护意识。

中国互联网络信息中心今年 8 月 30 日发布的《第 44 次中国互联网络发展状况统计报告》显示，截至 2019 年 6 月，我国网民规模达 8.54 亿，其中 19 岁以下网民占比超过 20%。

“网络已经成为当代青少年无法回避的生活现实，不少父母、老师对青少年使用网络表示忧虑，不少学校限制或禁止学生带手机入校，也反映出相关法律法规亟待完善。”中国传

媒大学传播研究院副研究员张洁说，此次草案针对这些问题作出规定，及时回应了社会需求。

【看点二】关于网络不良信息——对上网保护软件强制安装作出规定

针对暴力、色情、涉毒等不良网络信息问题，草案明确提出：国家鼓励和支持有利于未成年人健康成长的网络内容的创作与传播，鼓励和支持专门以未成年人为服务对象、适合未成年人身心发展特点的网络技术、设备、产品、服务的研发、生产和使用。

草案规定，学校、社区、图书馆、文化馆、青少年宫等场所为未成年人提供的公益性互联网上网服务设施，应当安装未成年人上网保护软件。草案同时规定，网络产品和服务含有可能影响未成年人身心健康信息的，制作、复制、发布、传播该信息的组织和个人应当在信息展示前按照国家有关规定予以提示。

“调查显示，大量涉及未成年人的犯罪案件背后，都存在未成年人不正常接触不良网络信息的问题。”陕西省律师协会常务理事王浩公说，草案的规定有利于动员全社会参与未成年人网络保护。特别是对未成年人吸引力较强的平台和产品，相关部门应积极入驻，主动发挥监管作用。

【看点三】关于网络沉迷——要求产品和服务提供者设置时间、权限、消费管理等功能

近年来，未成年人沉迷网游、直播等网络产品和服务不能自拔造成悲剧的事件时有发生。草案规定，网络产品和服务提供者应当避免提供可能诱导未成年人沉迷的内容。网络产品和服务提供者应当设置相应的时间管理、权限管理、消费管理等功能，为父母或者其他监护人预防和干预未成年人沉迷网络提供便利。

在网络游戏方面，草案规定，对未成年人使用网络游戏实行时间管理，具体办法由国务院规定。网络游戏服务提供者应当按照国家有关规定和标准，对游戏产品进行分类，作出提示，并采取技术措施，不得让未成年人接触不适宜其接触的游戏或者游戏功能。

中国政法大学副教授苑宁宁表示，草案回应近年来社会普遍关注的未成年人网络成瘾、网游沉迷等问题，作出制度性设计。按照国家有关规定和标准对网络游戏产品进行分类，有利于促进我国未成年人网络信息分类管理制度的形成。张洁认为，草案对网络沉迷防治和网络游戏管控作出的相关规定，仍需进一步明确概念，例如“可能诱导未成年人沉迷的内容”“不适宜青少年接触的游戏或者游戏功能”的标准等，使法律更具可操作性。

【看点四】关于网络欺凌——不得通过网络以文字、图片、音视频等形式侮辱、诽谤、威胁未成年人

草案规定，任何组织或者个人不得通过网络以文字、图片、音视频等形式侮辱、诽谤、威胁未成年人或者恶意扭曲、损害未成年人形象。发现未成年人遭受上述网络欺凌侵害或者

形象遭到恶意扭曲、损害的，受害未成年人的父母或者其他监护人可以要求网络信息服务提供者及时采取删除、屏蔽等措施，停止侵害。

中国互联网络信息中心发布的《2018 年全国未成年人互联网使用情况研究报告》显示，截至 2018 年 7 月 31 日，我国未成年网民规模达 1.69 亿，15.6%的未成年人表示曾遭遇网络暴力。

专家表示，与现实中的欺凌相比，网络欺凌更加难以调查取证，也加大了打击、处罚此类行为的难度。草案作出相关规定，有利于未成年人的父母及时采取措施制止侵害行为。另一方面，有关部门也应对网络平台加强监管，及时发现和惩治网络欺凌行为。

【看点五】关于个人信息保护——收集未成年人信息需经过未成年人及其父母或者其他监护人同意

草案对未成年人个人网络信息保护作出规定，明确网络产品和服务提供者应当提示未成年人保护其个人信息，并对未成年用户使用其个人信息进行保护性限制。网络产品和服务提供者通过网络收集、使用、保存未成年人个人信息的，应当符合国家有关规定，且经过未成年人及其父母或者其他监护人同意。

“未成年人信息泄露极易让未成年人处在被侵害的风险之中，比如被拐卖、被实施网络侵害等。”苑宁宁说，未成年人的个人信息关系到其切身利益和健康成长，因此有必要对未成年人的个人信息安全专门作出特别保护。

【看点六】关于保护责任——明晰未成年人网络保护各方责任

专家认为，此次未成年人保护法修订草案的重要进步，就在于明确了家长、学校、网络信息服务提供者和政府等各方主体对未成年人网络保护所应承担的责任。

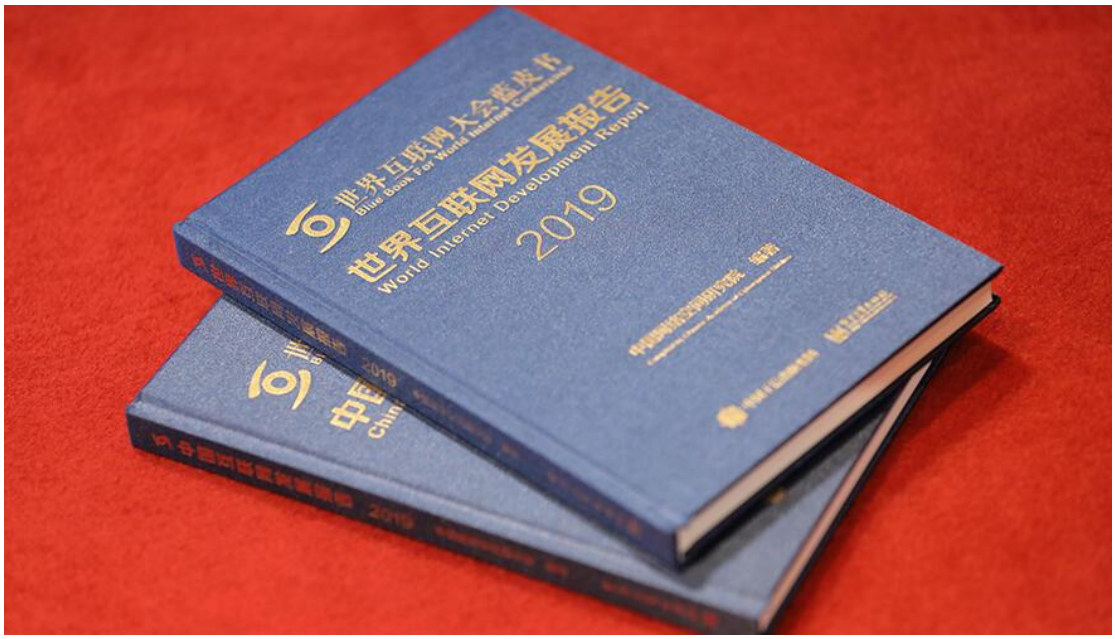
值得注意的是，草案还专门规定，网络产品和服务提供者应当结合本单位提供的未成年人相关服务，建立便捷的举报渠道，通过显著方式公示举报途径和举报方法，配备与服务规模相适应的专职人员，及时受理并处置相关举报。

“实践中，当孩子受到网络侵害，家长常常会面临举报途径不畅、处理效果不理想等问题。草案的这一规定，有望督促网络企业提供便捷的举报途径，并通过专业的方式及时解决相关问题，具有较强的现实意义。”北京青少年法律援助与研究中心主任佟丽华说。（来源：中国青年报）

四、政府之声

➢ 《世界互联网发展报告 2019》和《中国互联网发展报告 2019》蓝皮书发布

2019 年 10 月 20 日下午，由中国网络空间研究院编写的《世界互联网发展报告 2019》和《中国互联网发展报告 2019》蓝皮书在第六届世界互联网大会上正式发布。这是大会的一项重要理论成果，蓝皮书聚焦互联网发展的新动态、新趋势、新变化，回顾成就、总结经验、分析形势，努力为全球互联网发展提供客观情况、经验借鉴、思想引领，是全球互联网发展与治理研究的最新成果。



世界互联网大会蓝皮书由《世界互联网发展报告 2019》和《中国互联网发展报告 2019》两本报告组成，前者侧重国际、后者聚焦国内，从信息基础设施、网络信息技术、数字经济、数字政府和电子政务、互联网媒体、网络安全、网络空间法治建设、网络空间国际治理等 8 个重点领域，紧扣互联网发展前沿热点问题，全面展现 2019 年全球互联网发展的新理论和新实践、新态势和新进展。其中，《世界互联网发展报告 2019》立足全球视野和中国视角，聚焦全球互联网发展实践新技术、新应用、新发展，勾勒出构建网络空间命运共同体的宏伟蓝图。《中国互联网发展报告 2019》以习近平新时代中国特色社会主义思想特别是习近平总书记关于网络强国的重要思想为指导，以鲜活经验和生动案例全景式、立体化呈现 2019 年中国互联网发展新理念、新实践、新成就，阐明中国主张，提出中国方案，贡献中国智慧。

（来源：中国网信网）

➢ 两高关于办理帮助信息网络犯罪等刑案司法解释发布

2019 年 10 月 21 日，最高人民法院、最高人民检察院联合发布：《最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》已于 2019 年 6 月 3 日由最高人民法院审判委员会第 1771 次会议、2019 年 9 月 4 日由最高人民检察院第十三届检察委员会第二十三次会议通过，现予公布，自 2019 年 11 月 1 日起施行。（来源：最高人民法院）

- **法释〔2019〕15 号最高人民法院最高人民检察院《关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》**
- **全文：**http://www.court.gov.cn/fabu-xiangqing-193711.html

➢ 证监会发布《证券期货业软件测试规范》行业标准

2019 年 10 月 18 日，证监会召开新闻发布会，新闻发言人常德鹏表示，近日，证监会发布并实施了《证券期货业软件测试规范》（JR/T0175-2019）行业标准。

常德鹏表示，该标准描述了证券期货业信息系统建设过程中的总体要求、单元测试、集成测试、系统测试、系统集成测试、验收测试等测试活动的内容。标准的发布实施旨在明确证券期货业软件测试工作的要求，增强对测试活动过程和结束的约束，提高行业软件测试过

程的规范化程度。

“下一步，证监会将继续推进资本市场信息化建设工作，降低行业信息系统运行风险，着力增强基础标准化建设，不断提升行业标准化水平。”常德鹏说。（来源：中国证券监督管理委员会）

- **【第 20 号公告】《证券期货业软件测试规范》全文：**
- http://www.csrc.gov.cn/pub/newsite/zjhxwfb/xwdd/201910/t20191018_364648.html

➢ 密码法草案二审 增加密码“安全风险评估”机制

2019 年 10 月 21 日，《密码法草案》提请十三届全国人大常委会二次审议。草案二审稿加入“安全风险评估”机制，规定：密码管理部门根据工作需要会同有关部门建立核心密码、普通密码的安全监测预警、安全风险评估、信息通报、重大事项会商和应急处置等协作机制，确保核心密码、普通密码安全管理的协同联动和有序高效。

核心密码和普通密码属于国家秘密。此前，草案一审稿已对核心密码、普通密码的管理

和使用作了专章规定。有方面建议进一步强化国家对核心密码、普通密码的管理，实行密码安全保密责任制，定期开展安全评估，发现安全隐患风险后应当立即采取相应措施。对此，草案二审稿明确要求实行密码“保密责任制”，并增加“安全风险评估”机制，同时增加规定，发现影响核心密码、普通密码安全的“风险隐患”时，应当立即采取应对措施。

关于商用密码产品强制检测认证制度，草案二审稿完善了与网络安全法的衔接，增加规定：“商用密码产品检测认证应当适用《中华人民共和国网络安全法》的有关规定，避免重复检测认证。”

在完善商用密码应用安全性评估和国家安全审查制度方面，草案二审稿同样与网络安全法作了衔接，规定：“法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估。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。”“关键信息基础设施的运营者采购涉及商用密码的网络产品和服务，可能影响国家安全的，应当按照《中华人民共和国网络安全法》的规定，通过国家网信部门会同国家密码管理部门等有关部门组织的国家安全审查。”

草案二审稿同时强化保密义务，增加规定：“商用密码检测、认证机构应当对其在商用密码检测认证中所知悉的国家秘密和商业秘密承担保密义务”;“密码管理部门和有关部门及其工作人员应当对在履行职责中知悉的商业秘密和个人隐私严格保密，不得泄露或者非法向他人提供。”

在完善法律责任方面，草案二审稿进一步明确相关条款的处罚主体、处罚对象、处罚依据和罚则。同时，二审稿还加强密码人才培养，把人才队伍培养、建设的内容移至总则以突显人才培养对于密码事业的重要性。

值得注意的是，在密码法草案公开征求意见期间，一些国家和组织的驻华机构通过不同渠道向全国人大常委会法工委表达了关切，包括密码法是否会对外国企业的相关密码产品、服务和技术进入中国市场造成一定的限制等。

对此，全国人大常委会法工委发言人日前回应说，密码法草案有关许可和检测认证体系的相关规定，对于内外资企业、对于国内外的产品和服务一视同仁、同等适用，对外资企业的知识产权也要实行同等的保护，“密码法草案不会歧视外资企业以及外资企业的产品和服务，不会对投资和贸易构成任何的限制”。（来源：中新网）

五、本期重要漏洞实例

➢ Cisco Wireless LAN Controller 路径遍历漏洞

发布日期：2019-10-16
更新日期：2019-10-22
受影响系统：
Cisco WLC Software < 8.10
描述：

CVE(CAN) ID: CVE-2019-15266

Cisco Wireless LAN Controller（WLC）Software 是一套用于配置和管理 WLC（无线局域网控制器）的软件。
Cisco WLC Software 8.10 之前版本，在实现中存在路径遍历漏洞，该漏洞源于没有正确过滤描述文件名的命令行参数中用户提交的输入。本地攻击者可利用该漏洞查看包含有敏感信息的系统文件。

<*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-20191016-wlc-pathtrav

➢ Adobe Acrobat 和 Reader 释放后重利用任意代码执行漏洞

发布日期：2019-10-16
更新日期：2019-10-18
受影响系统：
Adobe Acrobat Reader DC < = 2019.012.20040
Adobe Acrobat DC <= 2019.012.20040
Adobe Acrobat 2017 < = 2017.011.30148
Adobe Acrobat Reader 2017 <= 2017.011.30148
Adobe Acrobat 2015 < = 2015.006.30503

Adobe Acrobat Reader 2015 <= 2015.006.30503

描述：

CVE(CAN) ID: CVE-2019-8177

Adobe Acrobat 是一套 PDF 文件编辑和转换工具。Reader 是一套 PDF 文档阅读软件。

Adobe Acrobat 和 Acrobat Reader 中存在释放后重利用漏洞，攻击者可利用该漏洞执行任意代码。

<*来源：Adobe
*>

建议：

厂商补丁：

Adobe

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://helpx.adobe.com/security/products/acrobat/apsb19-49.html

http://get.adobe.com/reader

➢ Oracle Fusion Middleware WebLogic Server 组件安全漏洞

发布日期：2019-10-16

更新日期：2019-10-17

受影响系统：

Oracle WebLogic Server 12.2.1.3.0

Oracle WebLogic Server 12.1.3.0.0

Oracle WebLogic Server 10.3.6.0.0

描述：

CVE(CAN) ID: CVE-2019-2891

Oracle Fusion Middleware 是一套面向企业和云环境的业务创新平台。WebLogic Server 是其中的一个适用于云环境和传统环境的应用服务器组件。

Oracle Fusion Middleware 的 WebLogic Server 组件存在安全漏洞，该漏洞允许攻击者在未授权情况下通过构造恶意的 HTTP 请求并发送给 Console 组件，从而接管受影响的服务器。

<*来源：Oracle
*>

建议：

厂商补丁：

Oracle

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.oracle.com/technetwork/security-advisory/cpuoct2019-5072832.html

➢ Microsoft Excel 远程执行代码漏洞

发布日期：2019-10-08
更新日期：2019-10-14
受影响系统：
Microsoft Excel 2016
Microsoft Excel 2013
Microsoft Excel 2010
Microsoft Office 365 ProPlus
Microsoft Office 2019 for Mac 0
Microsoft Office 2019
Microsoft Office 2016 for Mac
Microsoft Office 2016
描述：

CVE(CAN) ID: CVE-2019-1331

Microsoft Excel 是 Microsoft 为使用 Windows 和 Apple Macintosh 操作系统的计算机编写的一款电子表格软件。
当 Microsoft Excel 软件无法正确处理内存中的对象时，该软件中存在远程执行代码漏洞。成功利用此漏洞的攻击者可以在当前用户的上下文中运行任意代码。

<*来源：Ying Xinlei
*>

建议：

厂商补丁：
Microsoft

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://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-1331

六、本期网络安全事件

➢ ATM 遭受病毒攻击疯狂吐钱黑客盗走 140 万

2019 年 10 月 17 日，计算机给人们的生活带来了种种便利，但也带来了一些弊端，比如电脑病毒就是其中之一。近日德国法兰克福多的一家银行 ATM 疑似遭受了黑客病毒攻击，损失大量现金。这家银行的职员在检查 ATM 时，发现屏幕上显示了“Ho-Ho-Ho 今天来做些炸肉饼吧”，然后 ATM 就开始疯狂吐钱，直到现金用光。

被黑客侵入的 ATM 柜员机

俄语中“炸肉饼”的意思也包含了一沓现金的意思，所以这次 ATM 遭受的攻击很容易被联系到俄国黑客身上。事实上，俄国的黑客也是全球知名的，是十分厉害的角色。

问题在于，银行的 ATM 柜员机通畅是不接入公共互联网的，黑客们又是如何做到的呢？据悉通常他们使用的手段是物理侵入 ATM 的 USB 接口，以此安装恶意软件。

根据德国北莱茵-威斯特法伦州的检察官克里斯托夫·赫贝克的说法，该地区在 2017 年 2 月到 11 月期间发生了至少 10 起 ATM 中毒事件，黑客总共偷走了 140 万欧元的现金。

据该检察官透露，这波黑客应该是团伙和惯犯，2018 年春季以来，他们在不同的州内至少发现了 82 起类似案件，当然黑客也不是每次攻击都成功得手的。检察官也掌握了某些

情况下的录像证据，但是目前为止还没有找到嫌疑人，调查仍在继续。（来源：中关村在线）

➢ 为“薅羊毛”注册了 20 万个假账号，男子被判刑 3 年 6 个月

2019 年 10 月 14 日，一名 90 后小伙儿针对某一 App 购买奶粉买一送一的优惠活动，竟注册了 20 万个账号，利用技术漏洞“薅”走两万多桶奶粉，非法获利六万余元。近日，北京市海淀区人民检察院以被告人黄小天（化名）涉嫌提供侵入、非法控制计算机信息系统程序罪向法院提起公诉。经过法庭审判，被告人黄小天当庭认罪，被判处有期徒刑三年六个月。

为了薅羊毛，注册 20 万个假账号

出生于 1993 年的黄小天初中肄业，对计算机技术情有独钟，也十分了解市场上经常做优惠活动的一些商家信息。2017 年，黄小天发现一家专做母婴用品的 App 在针对购买奶粉用户进行优惠活动。厂家为了鼓励注册半年以上老用户首次消费，规定优惠活动为：老用户首次消费购买奶粉，买一桶送一桶。针对这一优惠活动，黄小天在之后一年的时间里，使用脚本程序批量虚假注册了该 App 的 20 万个账号。

但在上述账号注册半年以后，当黄小天试图用该批账号参加商家买一桶送一桶的优惠活动时，黄小天发现由于账号注册过程中缺少必要审核信息，这批账号无法登录正常的商家 App 客户端。

为了成功实现薅羊毛，黄小天转而研究商家的 App 安装包，并成功对该 App 客户端进行了攻破，将 App 的一些验证功能进行修改，终于让自己注册的虚假、非实名账号能够成功登录商家 App 客户端。

“薅”走奶粉两万多桶，销售账号获利六万余元

随后，黄小天通过互联网销售了两万余个这种虚假注册的账号，这些虚假账号配合他自己开发的冒牌 App，最终让活跃在网络中的羊毛党们又一次成功薅到了商家的羊毛，而黄小天也从中获利六万余元。

在审判中，被告人黄小天供称，他一共注册了 20 万个账号，筛选出两万多个可以参加“奶粉买一赠一活动”的账号出售牟利。而通过这个途径买奶粉的“羊毛党”，薅走的奶粉总共两万多桶。（来源：央视新闻）

➢ 日本“怪异酒店”承认房间服务机器人易遭黑客入侵

2019 年 10 月 24 日，据俄罗斯 RT 网站报道，新的研究发现，日本最奇特的酒店之一 Henn-na 连锁酒店内配备的机器人“客房助理”可能会被黑客用来监视客人。

尽管这家连锁酒店（其名称翻译为“怪异酒店”）表示，这种入侵“风险很小”，但它还是被迫承认，其“塔皮亚”床头机器人上配备的摄像头和麦克风容易受到黑客攻击。

这家连锁酒店本月早些时候在其网站上发布的一篇文章称：“今后，我们将以客户的安全和保障为重，弥补安全漏洞，并补充说，针对未经授权访问，我们已经想出了对策。”

今年夏天，网络安全工程师兰斯·R·维克（Lance R.Vick）发现了酒店这一漏洞后，与这家酒店取得了联系，在酒店保持了近三个月的沉默后，这位技术专家公开了这一消息。

维克本月早些时候发推文说：“日本著名机器人酒店的‘塔皮亚’机器人可以被黑客攻击，让任何人都可以通过遥控摄像机或麦克风窥探所有未来的客人。”

报道称，今年早些时候，Henn Na 为了雇佣更多的人类员工而将其有趣的机器人“裁员”，该新闻成为了当时的头条新闻。然而，该公司现在可能难以吸引客人，他们肯定会被在床边偷窥的机器人所拖累。（来源：环球时报）

➢ 银行数据被黑客窃取 美议员要求 FTC 调查亚马逊

2019 年 10 月 25 日，美国 Capital One 银行遭到黑客攻击，在攻击发生之前，亚马逊有没有保护好 Capital One 的服务器呢？针对此问题，美国两名参议员要求 FTC 对亚马逊展开调查。

参议员罗恩·韦登（Ron Wyden）和伊丽莎白·沃伦（Elizabeth Warren）说，他们希望 FTC 展开调查，看看 AWS 有没有违法。参议员称：“亚马逊继续向企业、政府机构、公众销售存在缺陷的云计算服务。1 亿 Capital One 客户的数据被偷，亚马逊应该承担部分责任。”

Capital One 年初曾说 1 亿美国个体客户和 600 万加拿大客户的个人信息被黑客窃取，当中包括姓名和住址，Capital One 将资料存入亚马逊云服务，结果被窃取。

攻击事件的嫌疑人名叫佩齐·汤普森（Paige Thompson），她是一名女程序员，通过配置错误的 Web 应用程序防火墙，汤普森成功访问 Capital One 数据。（来源：新浪科技）

➢ 微信借钱通过语音确认仍被骗 电信诈骗又出新套路

2019 年 10 月 21 日，近日，多家媒体关注到，利用微信语音包诈骗的案件——一些骗子盗取微信号后，发送借钱语音，受害人听到“声音差不多”的信息，便会信以为真，转账汇款，最终还是落入圈套。这究竟是怎么回事儿？

骗子从微信里发过的语音中提取个人声音生成假语音，还能模仿语气和情绪

江苏南京江宁分局岔路派出所昨天向中国之声介绍了这样一个案例。近日，该局接到报警，10 月 13 号，陈先生微信收到“熟人”王某发来的语音：“借我 5000 块钱吧，我着急买点东西。”

陈先生听到是朋友的声音，没多想，转了 5000 元过去。之后，王某又问陈先生能不能再借 9000 元，陈先生把自己余额还剩 400 元的截图发给王某，王某说：“400 也行，400 也转给我吧”，陈先生才起了疑心，但此时，他的微信已经被“王某”拉黑。“就跟我朋友的声音一模一样，要不是语音，我肯定不会被骗。”

类似的案例还有很多：据媒体报道，2018 年，河北石家庄的董女士收到父亲的微信留言，称在超市买东西，没有带钱，要求转账，收到父亲语音回复的董女士转账过去，回家后才发现父亲根本没去过超市，更没有通过微信要求她转账。

那么，这些相似语音或持续聊天的语音文件，是如何发送的？互联网行业从业者、iOS 应用逆向工程专家沙梓社说，微信本身并没有开放该项功能：“微信语音的原理大概是，第一步把你对着手机麦克风说的话保存成一个录音文件，第二步再把这个文件发送出去。出于对用户隐私的保护，微信是不关心你说的什么的，所以录音文件的内容它是不检查的，只要文件符合微信要求的那个录音的格式，微信就会把这个录音文件发出去，所以理论上微信可以发送任意内容的录音。”

沙梓社解释，问题主要就出在这一步：“在原本的微信中发出去的录音文件，只能是来自用户本人对着手机麦克风说话的这个声音，不能来自其他渠道，但是那些卖家就可以找一些技术人员来篡改这部分功能，生成一个新的微信程序，这个时候的微信就跟原版的微信不一样了，篡改过的微信可以选择录音文件的来源，不局限于用户对着麦克风说的话了。”

骗子是怎么模拟声音发出语音的呢？江苏南京的案例中，暂无更多案情披露。而在石家庄的案例中，警方此前对媒体披露，嫌疑人通过在用户的聊天记录里发出过的语音，取样模拟出了新的录音信息。从技术上来说，只要有样本，就能模拟出新的内容，甚至能模仿恐惧、哭泣等情绪。

网售语音包和语音软件可以生成任何嗓音和内容的音频

而实际上，如今市面上还有一种诈骗方式：微信语音包。比如我是个男的，现在想模仿一个女孩在网上加好友聊天行骗，就可以去买。日前就有媒体报道，在淘宝、qq 群里搜索，就能发现，只需 10 元就可买到 1000 条女声的微信语音信息，如果想要其他内容，还可以按照 2 元每条的价格进行私人定制。还有的，要是花上三十块钱，甚至能获得每日更新的语音

包——从日常聊天到唱歌，素材应有尽有。

在大多数人的认知中，如果只是文字聊天，那么你无法判断对方的真实身份，而微信语音只能是该账号用户按住“说话”键，即时说话，才能发送，在一些用户看来，能够通过语音聊天，是“真实”的象征。

实际上，如今只要花十几块钱购买一个语音包，安装之后，语音包通过篡改微信程序，就可以让用户发送录制好的录音文件，也就是说，哪怕你收到了语音，也不能代表对方是真实的。

记者随机购买了一个商户的商品，对方发来一个激活码、语音包下载地址、软件下载地址：“下载好软件会出现图标。然后找到手机设置权限，把权限都打开，再从权限里找到“悬浮窗”设置，把软件的悬浮窗开启一下，进去软件，有个语音管理，下面有个导入本地音响，找到你下载的语音包，点击添加。”

此时，再回到微信，就会出现一个叫“语音 mm”软件的悬浮窗，语音文件以文字的形式显示，按住想发送的语音文件内容，屏幕上会出现“语音已准备，请录制”，再按下微信的语音输入键，即自动写入语音包中的任意录音。不论使用者的性别、年龄、口音，都可以发出设置好文字的录音。

专家：现有法律只能对可疑账户封堵，制售虚假语音有违法风险

此类语音包同样可以使用在 QQ 及各种游戏平台。北京师范大学法学院教授、亚太网络法律研究中心主任研究员刘德良表示，利用语音包骗取财物的行为构成诈骗：“因为诈骗总是以非法占有他人财物为目的，虚构事实、让受害人相信，自觉得交出财物，实现诈骗的目的以从这个意义上来讲，通过语音包来模仿声音达到诈骗的目的，这是一种方式。”

根据国家法律规定，平台无法针对“一对一”的通信内容进行审查，刘德良说，目前更多的是对可疑账户进行封堵：“在‘一对一’的通信过程中，微信或者 QQ 等平台是不应该进行监管的，因为通信秘密是宪法规定的自由，除非受害人举报了某个嫌疑人利用微信或者 QQ 的语音包来进行诈骗，这种情况下，微信或者 QQ 的运营平台，有义务来对帐号进行封堵。”

今年 6 月，微信安全中心发布《关于打击“微信营销”外挂的公告》，10 月，微信团队表示“外挂软件不仅破坏了微信平台的生态平衡和正常运营，还为恶意营销行为提供了便利条件……针对使用微信外挂软件的现象，微信团队一直在加强打击，近期也进行了专项清理。”

沙梓社认为，技术上，这是一场“道高一尺、魔高一丈”的博弈。在网络黑灰产产业链

中，一些行为的认定，还不够明确，特别是一些游走在法律边缘的灰色产业，对平台和监管部门来说，都是治理难点，恐怕只有当违法成本大于获利，才能从根本上遏制互联网灰黑产的发展。

防骗最有效的方法还是自我加强防范：首先，不要加不明来源的陌生好友；其次，涉及到钱财问题，无论熟人还是朋友，必须要通过电话联系或者当面确认求证是否属实后再借钱。另外，用户如果发现自己微信号被盗取，可以在微信安全中冻结账号，同时，尽可能第一时间告知家人、朋友，以免骗子得手。

律师称，语音包虽然很多时候被包装成娱乐工具，实际上在其制作、售卖和使用中都可能存在违法风险，不要轻易尝试。（来源：中国之声）

➢ 私家侦探跟踪偷拍侵犯个人信息获刑

2019 年 10 月 13 日，“真相只有一个。”这句名侦探柯南的经典台词红遍大江南北。很多人儿时都是通过这句话了解到“私家侦探”的存在。然而现实中调查市场却暗藏不少灰色地带。一些所谓的“私家侦探”打着市场调研、统计调查的名义,干着利用跟踪、偷拍、GPS 定位帮人调查婚外情的勾当。

30 多岁的男子赖某某在江苏省无锡市区成立一家市场调查工作室,通过在网络、街头小

广告等形式招揽“婚恋调查”“市场调查”生意,并招聘王某某担任临时工,协助开展“私家侦探”生意。

赖某某被警方抓获时,他正为委托人跟踪一辆宝马车的轨迹。警方在被跟踪车辆底盘上,查到了一个定位器。这个定位器可与赖某某手机实时连接,车主一般很难发现。随后警方从赖某某的工作室、家里等处,共查获 5 套定位器。

据悉,找赖某某调查的委托人,多因婚恋感情上的烦恼而来。有妻子发现丈夫在外面生了小孩,想要查个水落石出；有妻子怀疑丈夫借口出差带着情人出去玩,要求跟到外地去核实；有人想获取证据,离婚时分割到更多财产……赖某某根据委托人提供的信息,采用全程跟踪手段,根据跟踪的难度和时长确定收费,临时拍一次费用 1000 元至 3000 元,包时间随叫随到的话则有 1 万多元 7 天和两万元 15 天的“套餐”优惠价,到外地“出差”还要额外收费。按照委托人的要求,谈好价钱后,委托人向赖某某提供对方的各种信息,包括工作单位、家庭住址、车牌号等等,赖某某随即安排跟踪调查,在被跟踪对象的车尾部底板安装车载定位器,以文字、照片、视频等形式将对方行踪轨迹信息报告给客户。

经查,2019 年 3 月下旬至 4 月间,被告人赖某某、王某某经事先共谋,通过安装车载定位器的方式获取被害人位置信息,对 3 名被害人进行跟踪拍摄,并将非法获取的行踪轨迹信息提供给他人,违法所得共计人民币 5.09 万元。

近日,由无锡市新吴区检察院提起公诉,无锡市新吴法院审理的无锡首例“私家侦探”侵犯公民个人信息罪案公开宣判,被告人赖某某、王某某分别被判处有期徒刑三年三个月、有期徒刑一年缓刑一年六个月并处罚金二万元、八千元。

法官说法：“个人信息种类多样,包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等,受国家法律严格保护,任何个人或组织未经授权不得侵犯。”新吴区法院法官周倩倩介绍,赖某某和王某某非法获取并出售被害人的行踪轨迹等个人信息,其行为触犯刑法,应当以侵犯公民个人信息罪追究刑事责任。

周倩倩表示,遇到婚恋纠纷要通过合法途径解决,以侵犯他人合法权益或者违反法律禁止性规定的方法取得证据,不仅不能作为法院认定案件事实的依据,对纠纷的解决起到实质性帮助,还可能受到行政处罚甚至刑事处罚,当以侵犯公民个人信息罪追究刑事责任。对于遇到婚恋纠纷的人,建议通过法律途径解决问题,而以侵犯他人权利的方式获得的证据,在诉讼中不会被认可。（来源：法制日报）

信息安全意识产品年服务

021-33663299