国盟信息安全通报

2020 年 12 月 20 日第 231 期

全国售后服务中心

国盟信息安全通报

（第 231 期）

国际信息安全学习联盟

2020 年 12 月 20 日

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 293 个，其中高危漏洞 142 个、中危漏洞 134 个、低危漏洞 17 个。漏洞平均分值为 6.43。本周收录的漏洞中，涉及 0day 漏洞 195 个（占 67%），其中互联网上出现“Wordpress Theme Wibar'Brand Component'跨站脚本漏洞、WordPress 插件 Heroic Knowledge Base SQL 注入漏洞”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 12235 个，与上周（6960 个）环比增加 76%。

主要内容

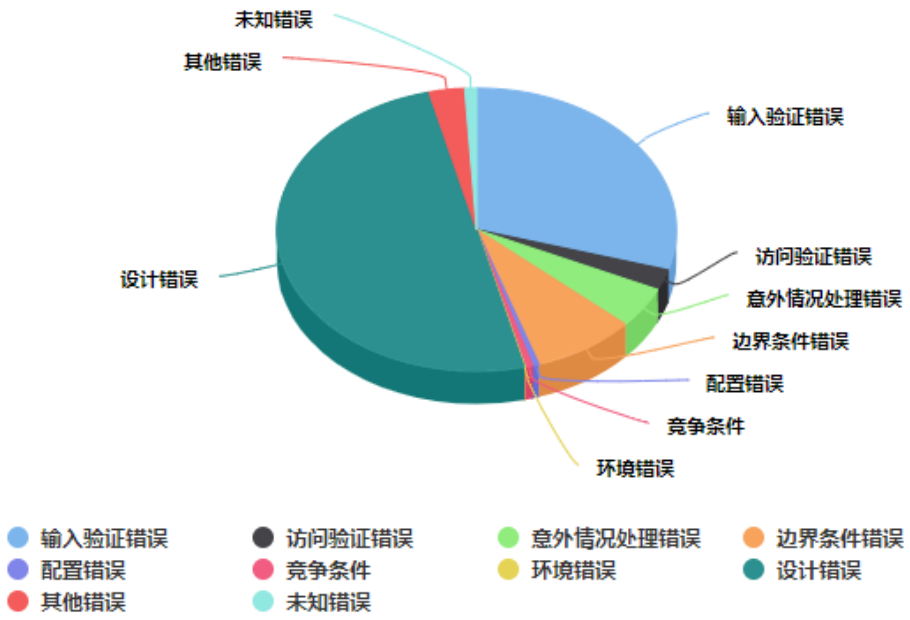
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

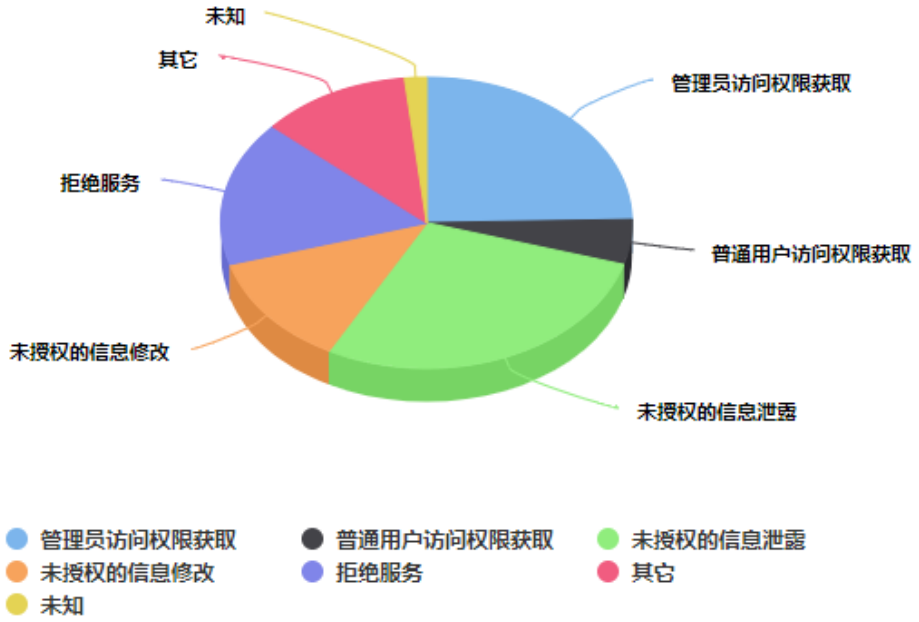
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 293 个，其中高危漏洞 142 个、中危漏洞 134 个、低危漏洞 17 个。漏洞平均分值为 6.43。本周收录的漏洞中，涉及 0day 漏洞 195 个（占 67%），其中互联网上出现“Wordpress Theme Wibar'Brand Component'跨站脚本漏洞、WordPress 插件 Heroic Knowledge Base SQL 注入漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 12235 个，与上周（6960 个）环比增加 76%。

二、安全漏洞增长数量及种类分布情况

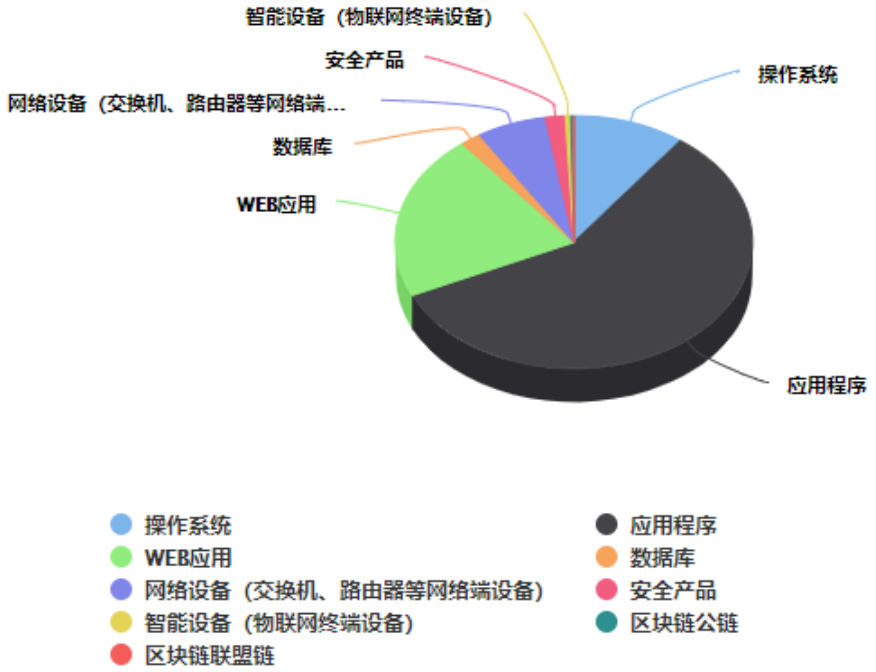
➢ 漏洞产生原因（2020 年 12 月 06 日—2020 年 12 月 20）



➢ 漏洞引发的威胁（2020 年 12 月 06 日—2020 年 12 月 20）



➢ 漏洞影响对象类型（2020 年 12 月 06 日—2020 年 12 月 20）



三、安全产业动态

➢ 未来五年网络空间治理怎么做？这份《纲要》告诉你

2020 年 12 月 7 日，中共中央印发《法治社会建设实施纲要（2020－2025 年）》，旨在加快推进法治社会建设。完善网络法律制度方面，《纲要》要求，通过立改废释并举等方式，推动现有法律法规延伸适用到网络空间。完善网络信息服务方面的法律法规，修订互联网信息服务管理办法，研究制定互联网信息服务严重失信主体信用信息管理办法，制定完善对网络直播、自媒体、知识社区问答等新媒体业态和算法推荐、深度伪造等新技术应用的规范管理办法。完善网络安全法配套规定和标准体系，建立健全关键信息基础设施安全保护、数据安全管理和网络安全审查等网络安全管理制度，加强对大数据、云计算和人工智能等新技术研发应用的规范引导。研究制定个人信息保护法。健全互联网技术、商业模式、大数据等创新成果的知识产权保护方面的法律法规。修订预防未成年人犯罪法，制定未成年人网络保护条例。完善跨境电商制度，规范跨境电子商务经营者行为。积极参与数字经济、电子商务、信息技术、网络安全等领域国际规则和标准制定。

其中，《纲要》为何将“依法治理网络空间”作为法治社会建设的重要任务？

中央依法治国办有关负责同志表示：随着互联网科技的迅猛发展，人们的沟通方式和生活方式发生改变，人类社会进入万物互联时代。技术进步让生活更便利、更舒适、更美好，

但同时存在网络谣言、网络色情、网络侵权盗版甚至网络恐怖主义等违法犯罪行为。与现实社会相比，网络治理面对的问题更为复杂。依法治理网络空间，是维护社会和谐稳定、维护公民合法权益、促进网络空间健康有序发展的必然之举和迫切需要。党的十九大报告提出：“加强互联网内容建设，建立网络综合治理体系，营造清朗的网络空间。”党的十九届五中全会审议通过的《中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议》提出：“加强网络文明建设，发展积极健康的网络文化。”贯彻落实党中央的决策部署，针对网络空间治理中的突出问题，纲要就推动社会治理从现实社会向网络空间覆盖，建立健全网络综合治理体系，加强依法管网、依法办网、依法上网，全面推进网络空间法治化，提出了具体措施。

具体措施梳理：网络治理

1.通过立改废释并举等方式，推动现有法律法规延伸适用到网络空间；

2.研究制定互联网信息服务严重失信主体信用信息管理办法；

3.制定完善对网络直播、自媒体、知识社区问答等新媒体业态和算法推荐、深度伪造等新技术应用的规范管理办法；

4.建立健全关键信息基础设施安全保护、数据安全管理和网络安全审查等网络安全管理制度，加强对大数据、云计算和人工智能等新技术研发应用的规范引导；

5.研究制定个人信息保护法；

6.健全互联网技术、商业模式、大数据等创新成果的知识产权保护方面的法律法规；

7.修订预防未成年人犯罪法，制定未成年人网络保护条例；

8.完善跨境电商制度，规范跨境电子商务经营者行为；

9.积极参与数字经济、电子商务、信息技术、网络安全等领域国际规则和标准制定；

10.提升网络媒介素养，推动互联网信息服务领域严重失信“黑名单”制度和惩戒机制；

11.坚决依法打击谣言、淫秽、暴力、迷信、邪教等有害信息在网络空间传播蔓延；

12.建立健全互联网违法和不良信息举报一体化受理处置体系；

13.加强青少年网络安全教育，引导青少年理性上网；

14.深入实施中国好网民工程和网络公益工程，引导网民文明上网、理性表达；

15.建立完善统一高效的网络安全风险报告机制、研判处置机制，健全网络安全检查制度；

16.加强对网络空间通信秘密、商业秘密、个人隐私以及名誉权、财产权等合法权益的保护；

17.严格规范收集使用用户身份、通信内容等个人信息行为；

18.加大对非法获取、泄露、出售、提供公民个人信息的违法犯罪行为的惩处力度；

19.督促网信企业落实主体责任，履行法律规定的安全管理责任；

20.健全网络与信息突发安全事件应急机制，完善网络安全和信息化执法联动机制；

21.依法查处网络金融犯罪、网络诽谤、网络诈骗、网络色情、攻击窃密等违法犯罪行为；

22.建立健全信息共享机制，积极参与国际打击互联网违法犯罪活动。（来源：中国网信网）

- **《法治社会建设实施纲要（2020－2025 年）》**
- **全文：**http://www.gov.cn/zhengce/2020-12/07/content_5567791.htm

➢ 《民法典》：网络安全制度创新的新里程碑

立足于完善网络治理体系、促进民事主体网络权利保护的角度，《民法典》在个人信息保护、网络安全义务、人格权制度安全义务、网络侵权规则等网络安全相关问题的规定上，实现了十分重要的制度创新。

一、完善个人信息保护规则

2016 年颁布的《网络安全法》是我国首部较为系统地规定个人信息保护的法律。该法

第四章“网络信息安全”规定了个人信息的收集原则、网络运营者的相关义务。2017 年颁布的《民法总则》进一步以基本法律的形式规定个人信息保护。以这些法律规定为基础，《民法典》的“人格权编”在其第六章设定了多个条文，进一步细化个人信息保护内容，并对《网络安全法》《民法总则》有重要发展与创新。

首先，就个人信息而言，《网络安全法》主要适用于以电子形式存储、处理的个人信息；而《民法典》则适用于以所有形式（包括书面形式）存储、处理的个人信息。从这个意义上说，《民法典》是普通法，针对所有的“信息处理者”；而《网络安全法》是特别法，约束的义务主体主要是“网络运营者”。值得注意的是，《民法典》对个人信息的“处理”，采纳了一个包含范围十分广泛的广义范畴。根据第 1035 条第 2 款，个人信息的处理包括“个人信息的收集、存储、使用、加工、传输、提供、公开等”，这与欧盟《一般数据保护条例》（GDPR）中“处理”的内涵比较接近。GDPR 第 4 条第 2 款规定：“处理”是指任何一项或多项针对单一个人数据或系列个人数据所进行的操作行为，不论该操作行为是否采取收集、记录、组织、构造、存储、调整、更改、检索、咨询、使用、通过传输而公开、散布或其他方式对他人公开、排列或组合、限制、删除或销毁而公开等自动化方式。这就最大限度地将个人信息的各类处理操作都纳入《民法典》规制范围。

其次，《民法典》完善了个人信息的概念。以《网络安全法》第 76 条为基础，《民法典》第 1034 条第 1 款规定：“个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等”。其中，“生物识别信息”包括指纹、声音、虹膜、脸相、静脉等生物信息。从国外立法经验看，生物识别信息属于敏感信息，原则上禁止一般机构或个人进行处理，而仅能由为履行法定职责的法定机构进行处理。生物识别信息包含人脸识别信息，因而这一条款在未来有可能用于应对目前亟待规范的人脸识别技术滥用问题。将“健康信息”纳入个人信息的范畴，是总结抗击新冠肺炎疫情经验的结果。健康信息同样属于敏感信息，因为事关信息主体的重大人身利益，如人格尊严。另外，将“行踪信息”纳入个人信息范围也十分重要。如今，大量应用程序（App）都有定位功能，往往在信息主体不知情的情况下默认其同意使用定位信息，从而记录其行踪轨迹，此种情况显然应该加以规范。至于电子邮箱是否属于个人信息，则值得研究。一般的电子邮箱并不具有身份识别功能，在实践中，往往只有在使用特定的工作邮箱等极少数情况下，才可以单独或结合其他信息识别出特定的主体。

再次，《民法典》对私密信息采取了“隐私权+个人信息保护”的双重保护模式，这被认

为是“权利+利益”的二元保护模式。《民法典》第 1034 条第 2 款规定：“个人信息中的私密信息，适用有关隐私权的规定；没有规定的，适用有关个人信息保护的规定”。按照这一规定，私密信息首先适用隐私权保护的规定。这些规定包括：第 1032 条第 2 款“隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息”；第 1033 条第 5 款“除法律另有规定或者权利人明确同意外，任何组织或者个人不得实施下列行为…… （五）处理他人的私密信息”。根据《民法典》第 1034 条第 2 款，仅在隐私权的这些规定无法适用的时候，方可适用个人信息保护的有关规定。因此，对于私密信息，隐私权的规定应优先适用，类似于特别法，因为隐私权是《民法典》明确承认的“民事权利”类型；而个人信息保护由于未明确使用“权利”措辞，因此，属于法律所保护的“利益”范畴，其规则属于普通法，处于辅助性的“补遗”地位。这一做法正好与比较法上以隐私权涵盖个人信息的通例相反，具有独特性。因此，在未来司法适用中，法院需要明确在哪些情况下对于私密信息而言隐私权的制度无法涵盖和适用，此时方可适用个人信息保护的有关规则。

最后，《民法典》增加了个人信息合理使用的相关规定，在保护个人的人格权与社会公共利益之间维持平衡。根据《民法典》第 1036 条，处理个人信息，有下列情形之一的，行为人不承担民事责任：（一）在该自然人或者其监护人同意的范围内合理实施的行为……（三）为维护公共利益或者该自然人合法权益，合理实施的其他行为。本条第 1 款中的同意例外是比较法上的通例，但是，从保护信息主体的人格利益的角度出发，要防止信息处理者滥用信息主体的概括同意，或者防止监护人滥用对处理未成年人信息的同意权。

二、规定网络安全相关义务

近年来，我国发生了多起个人信息数据库被黑客攻破后数据被非法获取的恶性事件，例如 2016 年的“徐玉玉案”。在这类案件中，由于信息的处理者未能履行信息安全义务，导致所存储的个人信息被他人非法获取，最终给信息主体造成巨大的财产和人身损失，教训极为惨痛。

有鉴于此，《民法典》强化了信息收集者、控制者确保其收集个人信息的安全义务。其第 1038 条第 2 款规定：“信息处理者应当采取技术措施和其他必要措施，确保其收集、存储的个人信息安全，防止信息泄露、篡改、丢失；发生或者可能发生个人信息泄露、篡改、丢失的，应当及时采取补救措施，按照规定告知自然人并向有关主管部门报告”。至于何谓“必要措施”，参照欧盟 GDPR 第 32 条的规定，应该在充分考虑最新技术水平、实施成本、处理性质、处理范围、处理背景与目的以及给信息主体权利所带来的损害可能性与严重性后，信息处理者所采取的适当技术措施，这些措施需保障其安全处于与风险相称的水平。

鉴于《民法典》第 1038 条第 2 款明确规定了信息处理者的信息安全义务，因此，如果信息处理者违反此种义务，应承担相应的民事责任。就此而言，可以参考《电子商务法》的有关规定。该法第 30 条规定："电子商务平台经营者应当采取技术措施和其他必要措施保证其网络安全、稳定运行，防范网络违法犯罪活动，有效应对网络安全事件，保障电子商务交易安全。电子商务平台经营者应当制定网络安全事件应急预案，发生网络安全事件时，应当立即启动应急预案，采取相应的补救措施，并向有关主管部门报告"。该法第 38 条第 2 款进一步规定："对关系消费者生命健康的商品或者服务，电子商务平台经营者对平台内经营者的资质资格未尽到审核义务，或者对消费者未尽到安全保障义务，造成消费者损害的，依法承担相应的责任"。此条直接规定了电子商务平台经营者对消费者所负有的安全保障义务。由于个人信息（特别是敏感信息）直接与信息主体的人身和财产安全密切相关，因此，参照《电子商务法》的有关规定，从《民法典》第 1038 条出发，应认为个人信息处理者对所处理的个人信息负有安全保障义务。违反此种义务，应承担安全保障责任。

另外，《民法典》第 1038 条第 1 款规定："信息处理者不得泄露或者篡改其收集、存储的个人信息；未经自然人同意，不得向他人非法提供其个人信息，但是经过加工无法识别特定个人且不能复原的除外"。本条前半句规定了信息处理者禁止泄露或篡改个人信息的义务；后半句规定了禁止与第三方分享的义务，但是，经过个人信息的匿名化或者加密处理、使其无法再用来识别特定信息主体的除外。还值得注意的是，第 1039 条规定："国家机关、承担行政职能的法定机构及其工作人员对于履行职责过程中知悉的自然人的隐私和个人信息，应当予以保密，不得泄露或者向他人非法提供"。在"两会"审议期间，本条在义务主体中增加了"承担行政职能的法定机构"，措辞更为周延。此条文在未来的适用中将产生重要的实践意义，因为在现实中，一些人往往通过其在某些国家机关工作的违规行为获取他人的通信、住址、行踪等个人信息及隐私。未来，此种做法将引发行为人的民事责任及行政责任。

三、网络环境下人格权保护的新问题

《民法典》的"人格权编"对其他具体人格权的相关规定，对于维护网络安全也将具有重要意义。

首先，在肖像权部分，《民法典》第 1019 条规定："任何组织或者个人不得以丑化、污损，或者利用信息技术手段伪造等方式侵害他人的肖像权"。其中，"利用信息技术手段伪造"就是针对目前在实践中出现的"AI 换脸"技术应用所带来的人格权侵害风险。这一风险主要表现在，在肖像权人不知情的情况下，通过"深度换脸"技术，某些应用程序（App）可将其肖像通过移花接木的伪造手段，将其移植、拼接到某些特定场景中，可能严重侵害其人格

利益（例如将其肖像植入色情视频中）。另外，考虑到人脸支付科技应用日益广泛，“换脸”技术将直接事关民事主体的财产安全，因此，这一条文显然具有保护公民财产权的重要价值。

其次，由于语音识别技术的日趋成熟，其应用范围也日益扩展，对声音的保护具有越来越重要的意义。声音具有独特性和可识别性，因此，与特定主体相联系，声音的性质同样是人格要素，声音权应当成为人格权的组成内容之一。在国外法律中，声音权被普遍确立为一项人格权。因此，我国《民法典》的“人格权编”第 1023 条第 2 款也承认了声音权。该条规定：“对自然人声音的保护，参照适用肖像权保护的有关规定”。这就是说，未经自然人同意，不得在导航软件、游戏、视听产品中擅自使用，擅自使用或仿冒他人的声音；禁止未经权利人同意使用、模拟他人的声音，防止通过侵害声音权冒用他人名义或造成不必要的身份混淆。

此外，酒店偷拍视频通过网络等途径泄露后，消费者非常难以举证酒店是否对此存有过错。现有的行政法规仅能在查获直接行为人后对其处以行政拘留等法律责任，而无法对受害者提供民事赔偿。有鉴于此，《民法典》第 1033 条规定：“除法律另有规定或者权利人明确同意外，任何组织或者个人不得实施下列行为……（二）进入、拍摄、窥视他人的住宅、宾馆房间等私密空间；（三）拍摄、窥视、窃听、公开他人的私密活动”。这些条文对于保障公民的隐私安全具有重要意义。从强化人格权预防功能的角度出发，根据比较法上通行的“自设计隐私保护”（privacy by design）原则，从本条出发，可以认为，酒店宾馆等住宿服务经营者负有保护消费者隐私的安全保障义务。这一隐私安全保障义务要求经营者从设计阶段就开始考虑应对各种可能侵犯隐私的行为，并设置合理的预防和处置措施。如果消费者在酒店住宿期间发生被偷拍事件，酒店应就其未尽到隐私安全保障义务承担赔偿责任。

四、优化网络侵权规则

网络侵权规则是保障网络安全的重要制度。相对于 2009 年《侵权责任法》和 2018 年《电子商务法》相关条文，《民法典》在此基础上作出了重要改进。

《民法典》第 1095 条规定：“网络用户利用网络服务实施侵权行为的，权利人有权通知网络服务提供者采取删除、屏蔽、断开链接等必要措施。通知应当包括构成侵权的初步证据及权利人的真实身份信息。……法律另有规定的，依照其规定”。在本条中，“根据构成侵权的初步证据和服务类型”的措辞，明显区别于《电子商务法》第 42 条，因为后者仅针对知识产权的侵权行为，而前者则应涵盖所有的民事侵权行为，不能将后者中“通知—删除”规则简单扩展到前者的适用领域。其原因在于：首先，知识产权的侵权之所以采取“通知—删除”规则，是因为知识产权的侵权判断一般要求具有相当的专业知识与技能，而此为一般人所不

具备。因此，法律授权平台在第一时间可以先从网上删除有争议的涉嫌侵权产品。一般民事侵权领域显然情况有所不同，例如，在网络发帖侵害名誉权、隐私权的情形中，根据双方所提供的初步证据，平台即可以作出是否存在侵权的初步判断。对于普通民事侵权照搬知识产权侵权的“通知—删除”规则的恶果还在于，授权网络平台在出现投诉后，在不征求网络用户本人意见的情况下就直接删除其作品，这样极其不利于网络言论自由的保护和舆论监督作用的发挥，违反了法律的正当程序原则与对席原则。另外，权利人凭简单一纸主张即可要求平台删除网络用户的作品而无须提供任何担保，也不符合法律的比例性原则，不利于对表达自由等基本权利的保护。向平台提交一纸投诉通知，就可以要求网络平台立即将竞争对手的商品下架，这一简单粗暴的规则极其容易被滥用，用以打击对手，助长恶意投诉及不正当竞争行为，而先删除后恢复的机制，也导致资源的无端浪费与损失。

正是基于上述原因，《民法典》大幅完善了《侵权责任法》《电子商务法》的相关规则，强调必须根据网络服务的不同类型决定所应采取的“必要措施”。《民法典》的相关条文要求法院在审理网络侵权争议时，根据网络服务的具体类型（网络接入服务、网络内容服务、网络存储服务、网络技术服务等），详细审查网络平台所采取的处理措施是否“必要”，而非一律采取简单粗暴的删帖措施。另外，从该条文的措辞看，受害人所提交的通知中应当包括构成侵权的初步证据，网络用户提交的声明中也应包括不存在侵权行为的初步证据。这也意味着，网络服务提供者负有义务对这些“初步证据”进行初步审查。当然，这种初步审查可以是形式审查，从形式上得出网络用户是否侵害了权利人民事权利的初步判断。只要其尽到了形式审查义务，尽到了合理的注意义务，即可免于承担责任。实质审查的义务应由法院或行政监管机构承担。对网络服务提供商者设定初步审查义务，对于加强其社会责任、实现对网络用户的表达自由和民事主体的人格权之间的平衡保护、维护网络安全和完善网络治理，都具有积极意义。（来源：《中国信息安全》杂志 2020 年第 10 期）

➢ 李东荣：数字化时代个人金融信息保护的思考

2020 年 12 月 10 日，由中国金融杂志社、中国信息通信研究院共同主办的首届 “中国金融数据治理论坛”在京举行，论坛主题为“银行业金融机构数据治理与价值提升”。**中国互联网金融协会会长李东荣在论坛上发表主旨演讲，深入阐述了对数字化时代个人金融信**

息保护的思考。以下为演讲全文：尊敬的各位嘉宾，各位朋友：

大家上午好。很高兴出席 2020 中国金融数据治理论坛。当前，国家正深入推进要素市场化配置改革，数据作为基础性战略资源和关键生产要素的地位更加凸显，金融业作为科技驱动型和数据密集型行业，如何持续提升数据治理能力、更好平衡数据应用与安全保护是一项重要而紧迫的时代课题。今天论坛汇聚政产学各方专家共同探讨金融业特别是银行业数据治理问题，具有重要的现实意义。

从理论上讲，数据治理是通过系统化的架构、制度、流程和方法，确保数据统筹管理、有效保护、高效运行，并在经营管理中充分发挥价值的动态过程。数据治理作为一项涉及数据全生命周期的系统工程，其基础是数据质量管理，核心是数据融合应用，目标是发挥数据价值，前提则是数据安全保护。鉴于此，借今天论坛的机会，我想就数字化时代背景下个人金融信息保护谈一些个人的思考意见，供大家参考。

根据人民银行 2020 年 2 月发布的《个人金融信息保护技术规范》，个人金融信息是金融业机构通过金融产品和服务或者其他渠道获取、加工和保存的个人信息，主要包括账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、信贷信息等。加强个人金融信息保护是落实人民至上理念、保护消费者合法权益的应有之义，也是促进个人金融信息安全合规应用、发挥金融数据价值的必要之举。近年来，随着数字技术与经济金融活动的加速融合，我国金融管理部门、行业协会以及广大从业机构在个人金融信息保护的制度建设和业务实践方面做了大量工作，取得了阶段性成效：

一是法律规范不断完善。涵盖法律、行政法规、部门规章、规范性文件等在内的多层次、广覆盖的个人金融信息法律规范体系初步形成，个人金融信息保护的理念原则、类别范围、业务规则、工作要求基本明确。

二是技术标准加速出台。在金标委的积极组织推动下，《个人金融信息保护技术规范》《金融数据安全 数据安全分级指南》等相关配套技术规范加速出台，网上银行、金融云、移动金融 APP、金融分布式账本等金融科技标准中均对个人金融信息保护和安全管理提出明确要求。

三是行政监管持续发力。近年来，金融管理部门通过宣传教育、风险排查、投诉处理、行政处罚、行业通报、监管评级挂钩等多种方式，不断提升个人金融信息保护工作针对性和监管有效性，督促从业机构履行客户个人金融信息保护义务，切实保障金融消费者信息安全权。

四是行业实践有序推进。从业机构在金融管理部门的指导和各金融行业协会的组织下，认真贯彻落实有关法律规范、监管要求和自律规则，注重将个人金融信息保护纳入公司治理、消费者保护、数据治理等工作规划，建立健全个人金融信息保护相关内控管理制度。

尽管取得了一定进展，我们还应清醒地看到，数字化时代个人金融信息保护在立法、监管、自律等方面依然有一些新老问题相互交织、亟待破解。比如，个人金融信息保护专门法律制度尚未出台，监管统筹、信息共享和工作联动有待持续加强，监管自律有机协调配合的治理机制尚未完全成熟，部分从业机构在个人金融信息保护方面的主体责任意识有待加强，在内部控制、数据治理、消费者保护等方面仍需进一步补短板、强弱项、堵漏洞，一些金融消费者个人信息保护意识和风险识别能力依然薄弱，在数字金融服务、信息安全防护、投诉维权等方面的知识和技能存在欠缺。

总之，数字化时代下加强个人金融信息保护任重而道远，需要包括政府、市场、社会多方协同、久久为功。具体来说，建议从以下几个方面着力开展工作：

一是持续完善制度规范。立足中国现实国情和经济金融数字化转型实际，科学借鉴欧盟、美国、英国、日本等国家和地区立法经验，合理吸收最小必要、目的限定、隐私安全、权益保护等国际通行原则，探索实现信息可携带权等新型权利形式的可行路径，适时出台《个人信息保护法》《个人金融信息（数据）保护试行办法》及相关配套标准。

二是增强监管科技能力。进一步完善个人金融信息保护领域的监管分工和统筹机制，以保护金融消费者合法权益和督促从业机构履行主体责任为切入点，以个人金融信息采集和处理机构为主要对象，探索运用人工智能、大数据、区块链等监管科技手段，持续深入开展个

人金融信息保护有关监管执法和检查评估工作。

三是发挥行业自律作用。继续发挥中国互联网金融协会等金融行业自律组织在移动金融 APP 备案、金融云备案、金融科技创新监管工具等领域的配合支撑作用，搭建从业机构信息共享和国际交流平台，深入研究行业在统筹个人金融信息保护和合理应用方面所面临的共性问题，督促引导从业机构落实个人金融信息保护有关法律规范和监管自律要求。

四是提升机构履责水平。从业机构应牢固树立以客户为中心、负责任创新的正确理念，切实落实个人金融信息全生命周期的安全防护要求，加强内控制度和数据治理体系建设，完善内部监督和责任追究机制。同时，在依法合规前提下探索应用多方安全计算、联邦学习等技术，加强个人金融信息保护技术支撑，促进信息合理开发利用。

五是加强社会公众参与。加强违法违规行为举报奖励、举报人保护等机制建设，充分调动社会公众参与个人金融信息安全治理的积极性。通过司法解释等方式，明确网络环境下个人金融信息侵权形式，丰富和畅通个人金融信息保护的救济渠道。广泛运用线上线下宣传教育渠道，定期发布个人金融信息保护风险提示和典型案例，提高公众对个人金融信息保护的意识和能力。

各位嘉宾，加强个人金融信息保护是一项长期复杂的系统工程，意义重大，任务艰巨。中国互联网金融协会将一如既往在金融管理部门的指导下，切实发挥好自律管理职责，完善个人金融信息保护体系，不断提升金融业数据治理水平。最后，预祝会议取得圆满成功。谢谢大家。（来源：金融电子化）

➢ 77.7%的网民遭遇过信息安全事件

“圆通内鬼租售账号导致 40 万条个人信息泄露”相关话题日前引发热议。数字时代，信息化、大数据极大便利了人们的生活，但稍有不慎，信息泄露让用户变成互联网上的“透明人”。信息被泄露怎么办？该怎么防？

信息倒卖让人防不胜防

“您好！您的信用卡已经透支，请及时还款。”近日，从事个体职业的马先生接到这样一通“催款”诈骗电话，骗子对他的姓名、电话号码、银行卡号甚至身份证号均了如指掌。“这太可怕了！说‘信息裸奔’绝非危言耸听。”奇怪的是，马先生本人并没有透支信用卡的情况。他猜测，出于工作要求，自己曾在多家银行登记过个人信息，这可能是信息被泄露

的重要原因。马先生遭遇的情况并不鲜见。当下，信息倒卖种类繁多，银行卡客户数据泄露现象颇为严重。据了解，不法分子仅需 5 毛钱便能买到包括姓名、电话、地址、工作单位、开户行等个人信息数据。

网购信息泄露导致的电信诈骗时常发生。骗子以电商客服的名义给消费者打电话，能准确说出消费者的姓名、消费者购买商品的具体信息。随后，骗子以消费者下单的商品存在质量问题、需要办理理赔为由，套取受害人账户信息和密码，骗取钱财。

网购记录、外卖配送地址、门店会员信息……大数据时代，个人信息充分暴露，让人防不胜防。不计其数的推销电话、垃圾短信，层出不穷的网络诈骗……中国消费者协会研究表明，85.2%的公民遇到过个人信息泄露情况。

信息泄露不仅侵犯公民隐私权，往往还会导致名誉受损、经济损失。中国互联网络信息中心发布的《2019 年中国网民信息安全状况研究报告》显示，77.7%的被调查网民遭遇过信息安全事件，并且遭受不同程度的损失，总额大约为 194 亿元。

面对信息采集“零信任”

信息被泄露令人烦心，但许多人缺乏必要的信息安全知识。数据显示，在遭遇过信息泄露的网民中，高达 47.5％的网民选择置之不理，提高公民信息保护意识刻不容缓。

武汉大学网络治理研究院副院长袁康认为，公民应当树立自我保护意识，高度重视个人信息的安全和保护，充分认识到信息泄露可能造成的严重危害，面对信息采集“零信任”，尽可能少向商家、网络服务提供者提供个人信息。

中国消费者协会发布的《APP 个人信息泄露情况调查报告》显示，信息泄露途径繁多，主要有两种：一是平台对个人信息的过度采集；二是不法分子故意泄露、出售或者非法向他人提供个人信息。信息采集方式也层出不穷：旅馆住宿、邮寄快递、银行办证、购房时对身份证件信息的采集；各种“调查问卷”、“趣味”游戏对信息的“无意”采集；手机应用程序、网络购物的“绑定”采集等。

当遭遇个人信息泄露时，公民应采取维权方式保护个人权益。“可以及时向公安机关报案，将涉嫌盗取、出售、公开个人信息等线索向公安机关提交。”袁康认为，公民应及时向泄露和公布个人信息的商家或平台投诉，要求其删除个人信息，防止个人信息进一步泄露；同时搜集相关证据，通过诉讼要求有关责任主体承担相应法律责任，包括停止侵害、排除妨碍、消除影响、赔偿损失等。

筑牢信息安全“防火墙”

此次圆通“内鬼”贩卖客户信息，导致 40 万条个人信息泄露，反映快递行业对个人信息保护的忽视，也暴露了企业数据安全短板。个人信息关系着每个人的生命财产安全，对倒卖个人信息的“黑色产业链”必须严厉打击。

上海市网信办责令要求圆通公司认真处理员工违法违纪事件，做到信息对称、及时公开、正面应对，加快建立快递运单数据的管理制度。圆通公司表示，公司将持续通过“制度+技术”手段，完善信息安全防控系统，对内部账号实时监控，构建内部“防火墙”。

中国政法大学网络法学研究院研究员郭旨龙说：“企业应遵循合法、正当、必要的原则，谨慎采集、使用、存储个人信息，提高身份认证、信息保护等信息安全技术水平，加强内部管控，在数据泄露后及时采取补救措施并通知监管机构与数据主体。”

现阶段，中国已基本构建起以《网络安全法》、《数据安全法（草案）》、《个人信息保护法（草案）》为核心，以《民法典》为依托的个人信息保护体系。专家举例指出，随着人工智能技术的发展普及，人脸识别技术被广泛用于身份识别、信息解锁。如今，仅需一张人脸高清图片便可构建仿真人脸模型，从而“欺骗”人脸识别系统，这就给“网络黑产”倒卖人脸信息以可乘之机。有关法律、制度等应对人脸等生物特征信息的保护做出界定，明确人脸识别技术的红线等。（来源：人民日报）

四、政府之声

➢ 国家密码管理局发布《信息系统密码应用测评要求》

2020 年 12 月 8 日，国家密码管理局依据《中华人民共和国密码法》等法律法规,中国密码学会密评联委会组织编制了《信息系统密码应用测评要求》等 5 项指导性文件,现已公开发布,可供相关单位开展商用密码应用与安全性评估工作参考。

其中包括：1.信息系统密码应用测评要求；2.信息系统密码应用测评过程指南；3.信息系统密码应用高风险判定指引；4.商用密码应用安全性评估量化评估规则；5.商用密码应用安全性评估报告模板（2020 版）。（来源：国家密码管理局）

- **《信息系统密码应用测评要求》等 5 项密码应用与安全性评估指导性文件**
- **全文**：https://www.oscca.gov.cn/sca/xwdt/2020-12/08/content_1060792.shtml

➢ 中国人民银行、中国银保监会发布《系统重要性银行评估办法》

2020 年 12 月 3 日，为完善我国系统重要性金融机构监管框架，建立系统重要性银行评估与识别机制，人民银行会同银保监会制定了《系统重要性银行评估办法》（银发〔2020〕289 号，以下简称《评估办法》），现正式发布。《评估办法》作为《关于完善系统重要性金融机构监管的指导意见》（银发〔2018〕301 号）的实施细则之一，是我国系统重要性银行认定的依据，也是对我国系统重要性银行提出附加监管要求、恢复与处置计划要求、实施早期纠

正机制的基础。

《评估办法》主要内容包括：一是明确评估目的。识别出我国系统重要性银行，每年发布名单，根据名单对系统重要性银行进行差异化监管，切实维护金融稳定。二是确定评估方法。采用定量评估指标计算参评银行的系统重要性得分，再结合其他定量和定性信息作出监管判断。三是明确评估流程。每年确定参评银行范围，收集参评银行数据进行测算，提出系统重要性银行初始名单，结合监管判断，对初始名单进行必要调整，经国务院金融稳定发展委员会确定后发布。（来源：中国人民银行）

- **《系统重要性银行评估办法》全文：**
- http://www.cbirc.gov.cn/chinese/docfile/2020/7f1c0ca35d84450d9c894e2a71da7486.pdf

➢ 证监会发布《证券期货业网络安全事件报告与调查处理办法（征求意见稿）》

2020 年 12 月 11 日，为进一步规范证券期货业网络安全事件报告和责任追究，依据《证券法》《证券投资基金法》《证券期货业信息安全保障管理办法》（证监会第 82 号令）《证券基金经营机构信息技术管理办法》（证监会第 152 号令），证监会对 2012 年发布的《证券期货业信息安全事件报告与调查处理办法》进行了修订，形成了《证券期货业网络安全事件报

告与调查处理办法（征求意见稿）》，现向社会公开征求意见。《证券期货业网络安全事件报告与调查处理办法（征求意见稿）》主要修订内容如下：

中国证券监督管理委员会
CHINA SECURITIES REGULATORY COMMISSION

证券期货监督管理信息公开目录

索 引 号:40000895X/　　分类:其他；征求意见
发布机构:证监会　　发文日期:2020年12月11日
名　　称:关于就《证券期货业网络安全事件报告与调查处理办法（征求意见稿）》公开征求意见的通知
文　　号:无　　主 题 词:

关于就《证券期货业网络安全事件报告与调查处理办法（征求意见稿）》公开征求意见的通知

为进一步规范证券期货业网络安全事件的报告和调查处理工作，减少网络安全事件的发生，维护国家金融安全、社会秩序和投资者合法权益，我会起草了《证券期货业网络安全事件报告与调查处理办法（征求意见稿）》，现向社会公开征求意见。公众可通过以下途径和方式提出反馈意见：

1. 登录中国证监会网站（网址：http://www.csrc.gov.cn），进入首页右侧点击“公开征求意见”栏目提出意见。

2. 电子邮件：anquanzy@csrc.gov.cn。

3. 通信地址：北京市西城区金融大街19号富凯大厦中国证监会科技监管局，邮政编码：100033。

意见反馈截止时间为2021年1月11日。

中国证监会

2020年12月11日

一是将网络安全事件责任主体限定为提供证券期货相关服务的机构。网络安全责任主体进一步明确为：承担证券期货市场公共职能的机构、承担证券期货行业信息技术公共基础设施运营的机构等证券期货市场核心机构及其承担上述公共职能的下属机构，证券公司、期货公司、基金管理公司及其提供证券期货相关服务的下属机构、证券期货服务机构等证券期货经营机构。

二是明确了对证券期货服务机构采取监督管理措施。根据《证券法》《证券投资基金法》《证券期货业信息安全保障管理办法》（证监会第 82 号令）《证券基金经营机构信息技术管理办法》（证监会第 152 号令）等法律法规和我会规章，将证券期货服务机构明确为证券期货业网络安全保障责任主体，网络安全事件相关证券期货服务机构存在人为责任的，中国证监会及其派出机构可以要求其提交说明材料，并依照有关法律、行政法规和规章，采取监督管理措施。

三是与相关法律法规使用相同的用语。为与《网络安全法》等法律法规的表述保持一致，此次起草工作将《证券期货业信息安全事件报告与调查处理办法》改为《证券期货业网络安全事件报告与调查处理办法》。

四是对信息系统进行了统一分类。按照信息系统发生网络安全事件后，对国家金融安全、社会秩序、投资者合法权益造成的损害程度，核心机构和经营机构的信息系统由高到低分为五类，即五类系统、四类系统、三类系统、二类系统和一类系统。

五是增加了定量描述系统服务能力异常的方法。根据交易撮合类系统、行情计算发布类系统、结算类系统、开户类系统、网站类系统等提供的服务的差异性，给出了服务能力异常计算公式，从而可以定量描述系统服务能力异常情况。

六是提出了统一的网络安全事件分级方法。结合信息系统类别和信息系统服务能力异常，提出了统一的网络安全事件分级方法。同时，对于数据泄露、结算金额差错、发布不良信息等网络安全事件，依据数据量和影响程度提出了定级标准。

七是完善了网络安全事件报告流程。增加了通过事件报送平台报告事件情况；考虑到事件发生时，很难判断是否会进一步恶化，要求信息系统发生故障，可能构成网络安全事件的，都应当立即报告；要求机构对事件初步定级、对可能构成特别重大、重大网络安全事件的，每隔 30 分钟至少上报一次事件处置情况，直至信息系统恢复正常运行，其他网络安全事件第一次上报后，无须持续上报事件处置情况,如有重要情况应当立即报告。

八是网络安全事件处罚更加具有针对性和灵活性。对于存在明显过错、疏忽且社会影响较大的网络安全事件，可酌情提高事件定级；从鼓励行业自主创新、网络安全事件实际影响、尽职免责等角度出发，对未发现明显过错、疏忽且不良影响较小的网络安全事件，可酌情从轻分级或不认定为网络安全事件。（来源：中国证券监督管理委员会）

- **《证券期货业网络安全事件报告与调查处理办法（征求意见稿）》**
- **全文：**http://www.csrc.gov.cn/pub/zjhpublic/zjh/202012/t20201211_387802.htm

➢ 国家广电总局发布《广播电视网络安全等级保护定级指南》等标准

2020 年 12 月 9 日，国家广播电视总局批准发布了广播电视和网络视听推荐性行业标准《广播电视网络安全等级保护定级指南》、《数字电视卫星传输信道编码和调制规范》等两项标准文件，这是国内继金融行业后第二个出台等保 2.0 标准的行业。**《指南》建议：**根据广电行业实际情况，按照定级对象的基本特征，综合考虑定级对象的责任单位、业务类型和业务重要性等因素，将广播电视网络安全等级保护对象按照机构类别及承载的业务种类进行分类。（来源：国家广播电视总局）

- **《广播电视网络安全等级保护定级指南》等行业标准的通知**
- **全文：**http://www.nrta.gov.cn/art/2020/12/9/art_113_54118.html

五、本期重要漏洞实例

➢ Microsoft 发布 2020 年 12 月安全更新

发布日期：2020-12-8

更新日期：2020-12-8

12 月 8 日，微软发布了 2020 年 12 月份的月度例行安全公告，修复了其多款产品存在的 58 个安全漏洞。受影响的产品包括：Windows 10 20H2 & WindowsServer v20H2（20 个）、Windows 10 2004 & WindowsServer v2004（20 个）、Windows 10 1909 & WindowsServer v1909（19 个）、Windows 8.1 & Server 2012 R2（6 个）、Windows Server 2012（6 个）、Microsoft Edge (HTML based)（2 个）和 Microsoft Office（15 个）。利用上述漏洞，攻击者可以绕过安全功能限制，获取敏感信息，提升权限，执行远程代码，或发起拒绝服务攻击等。

CVE 编号	公告标题	最高严重等级和漏洞影响	受影响的软件
CVE-2020-17095	**Hyper-V 远程代码执行漏洞**	严重 远程代码执行	Windows 10 Server 2016 Server 2019 Server, version 1903 Server, version 1909 Server, version 2004 Server, version 20H2
CVE-2020-17096	**Windows NTFS 远程代码执行漏洞**	重要 远程代码执行	Windows 10 Server 2016 Server 2019 Server, version 1903 Server, version 1909 Server, version 2004 Server, version 20H2 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-16996	**Kerberos 安全功能绕过漏洞**	重要 安全功能绕过	Server 2016 Server 2019 Server, version 1903 Server, version 1909 Server, version 2004 Server, version 20H2 Server 2012 Server 2012 R2
CVE-2020-17131	**Chakra Scripting Engine 内存破坏漏洞**	严重 远程代码执行	Microsoft Edge (EdgeHTML-based) ChakraCore

CVE-2020-17128	**Microsoft Excel 远程代码执行漏洞**	重要 远程代码执行	Office 2010/2016/2019 365 Apps Enterprise Excel 2010/2013/2016 Office Web Apps 2010/2013 Office Online Server Office 2019 for Mac
CVE-2020-17121	**Microsoft SharePoint 远程代码执行漏洞**	严重 远程代码执行	SharePoint 2010 SharePoint 2013 SharePoint Ent 2016 SharePoint 2019

来源：https://msrc.microsoft.com/update-guide/en-us/releaseNote/2020-Dec

➢ Apache Struts 远程代码执行漏洞

发布日期：2020-12-8
更新日期：2020-12-8
受影响系统：
Apache struts >=2.0.0，<=2.5.25
描述：

CVE(CAN) ID: CVE-2020-17530
Apache Struts 是美国阿帕奇（Apache）软件基金会负责维护的一个开源项目，是一套用于创建企业级 Java Web 应用的开源 MVC 框架，主要提供两个版本框架产品，Struts 1 和 Struts 2。Apache Struts 存在远程代码执行漏洞。攻击者可通过精心构造的请求执行远程代码。
建议：

厂商补丁：
Apache
用户可参考如下供应商提供的安全公告获得补丁信息：
https://cwiki.apache.org/confluence/display/WW/S2-061

➢ WordPress DiveBook plugin SQL 注入漏洞

发布日期：2020-12-13
更新日期：2020-12-13
受影响系统：
WordPress WordPress DiveBook plugin 1.1.4
描述：

CVE(CAN) ID: CVE-2020-14207

WordPress 是 WordPress（Wordpress）基金会的一套使用 PHP 语言开发的博客平台。该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。WordPress DiveBook plugin 1.1.4 版本存在 SQL 注入漏洞，该漏洞源于 divelog 中注入 SQL。允许未经身份验证的用户通过 divelog.php 过滤潜水员参数从数据库中检索数据。目前没有详细的漏洞细节提供。

建议：

厂商补丁：

Wordpress

厂商已发布了漏洞修复程序，请及时关注更新：

https://wordpress.org/plugins/divebook/#developers

➢ Oracle Common Applications 信息泄露漏洞

发布日期：2020-07-15

更新日期：2020-12-17

受影响系统：

Oracle Common Applications 12.2.3<= Version <=12.2.9

Oracle Common Applications 12.1.3

描述：

CVE(CAN) ID: CVE-2020-14717

Oracle E-Business Suite（电子商务套件）是美国甲骨文（Oracle）公司的一套全面集成式的全球业务管理软件。该软件提供了客户关系管理、服务管理、财务管理等功能。Oracle E-Business Suite 中的 Oracle Common Applications 12.1.3 和 12.2.3 至 12.2.9 版本的 CRM User Management Framework 组件存在信息泄露漏洞。攻击者可利用该漏洞通过 HTTP 访问网络破坏 Oracle Common Applications，对 Oracle Common Applications 某些可访问数据进行未经授权更新、插入或删除。

建议：

厂商补丁：

Oracle

Oracle 已经为此发布了一个安全公告（cpujul2020）以及相应补丁：

cpujul2020：Oracle Critical Patch Update Advisory - July 2020

链接：https://www.oracle.com/security-alerts/cpujul2020verbose.html

六、本期网络安全事件

➢ 2000 多万部金立手机被植入木马 牟利近 3000 万元

2020 年 12 月 6 日，“金品质立天下”的广告语曾风靡一时。但是，两千多万部金立手机被暗中植入木马，沦为他人非法敛财工具。一时间，信息安全问题引发网友热议。根据中国裁判文书网判决书显示，深圳致璞公司有预谋地在 2651 万台金立手机中安装木马程序，构成非法控制计算机信息系统罪，其公司负责人及直接责任人被判处有期徒刑。前年夏天，上述公司与另一公司北京佰策公司法人代表合谋，采用具有“拉活”功能的木马程序控制用户手机的方式合作开展“拉活”业务。

所谓的“拉活”，其实是指提升某一款 APP 的用户活跃度。后双方约定将北京佰策公司开发的“拉活木马”程序集成在金立手机的故事锁屏 APP 中，并通过“故事锁屏”软件版本更新将“拉活木马”程序植入到用户的金立手机当中。证据显示，该木马一旦被植入手机，一些 app 就会在后台悄悄打开并长时间运行，而机主对此却毫不知情，而这些手机也成了所谓的“肉鸡”，造成的后果就是手机电量和流量消耗加快，内存被占用，使用体验下降。装有“拉活”功能的手机在用户不知情的情况下自动更新版本，接收“拉活”指令，并在符合配置条件的情况下执行对指定 APP 的拉活，从而达到广告拉活的效果，赚取拉活费用。

法院经审理查明，2018 年 12 月至 2019 年 10 月，双方合伙实施“拉活”（执行成功）

共计 28.84 亿次。2019 年 4 月以来，每月拉活覆盖设备数均在 2175 万台以上，其中 2019 年 10 月涉及金立牌手机 2651.89 台。致璞科技预计在此期间通过“拉活”收入 2785.28 万元，案发前双方已结算的费用为 842.53 万元。

2020 年 11 月，法院判决深圳市致璞科技有限公司犯非法控制计算机信息系统罪，判处罚金人民币四十万元；判决被告人徐黎、朱颖、贾正强、潘琦犯非法控制计算机信息系统罪，处以 3 年到 3 年 6 个月不等刑期，并各处罚金二十万元，没收公司违法所得人民币 840 多万元。（来源：中央政法委长安剑）

➢ 富士康遭勒索软件袭击 100G 数据被盗，黑客要求支付 3400 万美元

2020 年 12 月 8 日，感恩节周末，富士康电子巨头在墨西哥的一家生产设施遭到了勒索软件攻击。攻击者在对设备加密之前先窃取了未经加密的文件。富士康是全球最大的电子产品制造公司，2019 年的营业收入达到了 1720 亿美元，在全球拥有 80 余万名员工。富士康旗下子公司包括夏普、Innolux、FIH Mobile 和贝尔金（Belkin）。

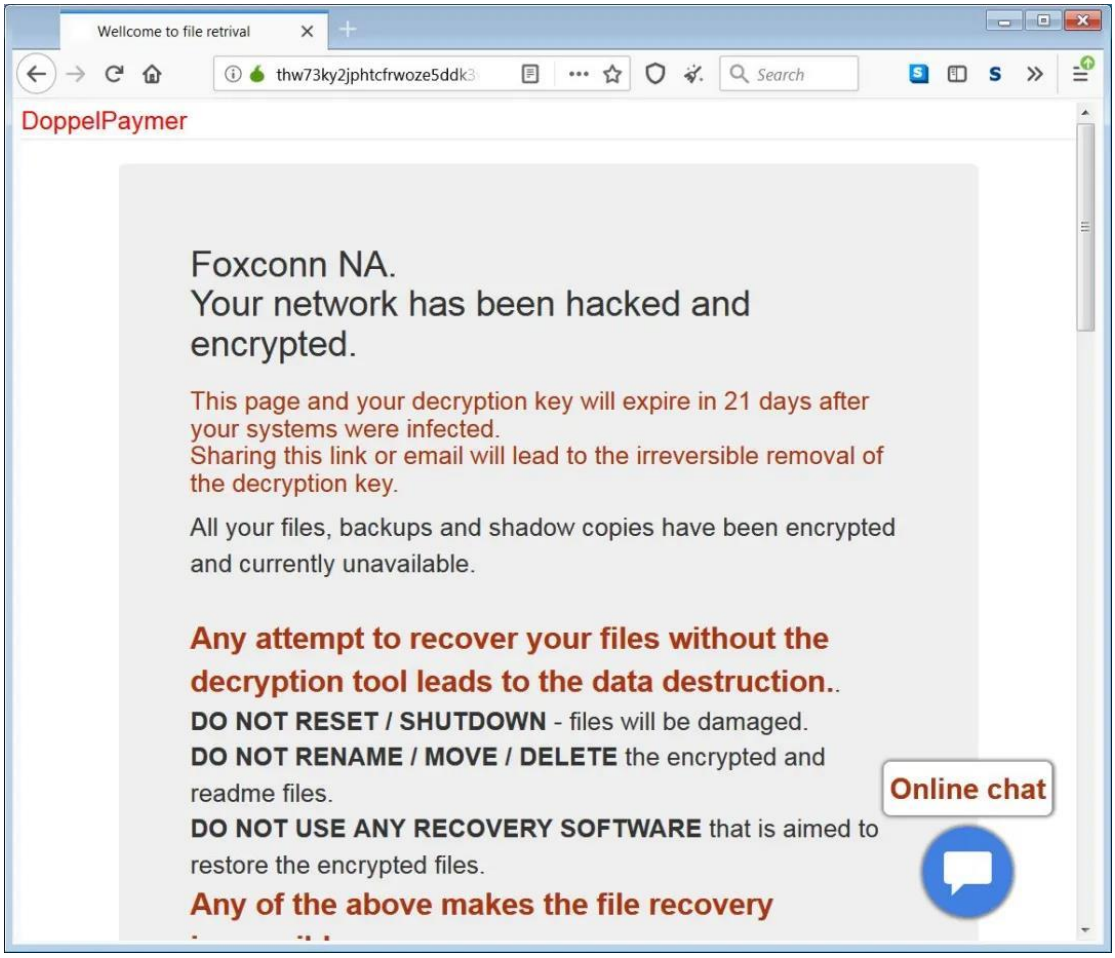
安全外媒 BleepingComputer 一直在密切跟踪感恩节周末发生的坊间传闻的富士康勒索软件攻击。今天，DoppelPaymer 勒索软件在其勒索软件数据泄漏网站上发布了属于富士康的文件。泄漏的数据包括一般的业务文件和报告，但不包含任何财务信息或员工的个人详细信息。网络安全行业的消息人士已证实，富士康于 2020 年 11 月 29 日左右在位于墨西哥华雷斯城的富士康 CTBG MX 生产设施遭到了攻击。

该生产设施于 2005 年开业，被富士康用来将电子设备组装和运输到南美和北美的所有

地区。富士康 CTBG MX 官网页面这样介绍该生产设施：“我们占地 682000 平方英尺的工厂建于 2005 年，位于墨西哥奇瓦瓦州华雷斯城，对面就是得克萨斯州埃尔帕索。富士康 CTBG MX 的位置具有重要的战略意义，支持美洲所有地区。”自攻击以来，该生产设施的官网已瘫痪，目前向访客显示出错信息。

攻击者索要 3400 万美元（2.3 亿人民币）的赎金

消息人士还透露了勒索软件攻击期间在富士康服务器上创建的勒索信。勒索信里面附有指向 DoppelPaymer Tor 付款网站上富士康受害者页面的链接，不法分子索要 1804.0955 个比特币的赎金，按今天的比特币价格折算，约合 34686000 美元（2.3 亿人民币）。



DoppelPaymer 勒索软件团伙在接受采访时证实，他们在 11 月 29 日攻击了富士康在北美的生产设施，但并未攻击整个公司。作为这次攻击的一部分，不法分子声称已加密了约 1200 台服务器，窃取了 100 GB 的未加密文件，并删除了 20TB 至 30 TB 的备份内容。

DoppelPayment 透露这起攻击时表示：“我们加密了北美部分，而不是整个富士康，这涉及大约 1200 台至 1400 台服务器，并不单单针对工作站。它们还有大约 75TB 的其他备份，我们销毁了其中大约 20TB 至 30TB 的备份内容。”过去遭到 DoppelPaymer 攻击的其他受害

者包括康柏（Compal）、墨西哥国家石油公司（PEMEX）、加利福尼亚州托伦斯市、纽卡斯尔大学、乔治亚州霍尔县、班尼杰集团（Banijay Group SAS）和布列塔尼国立高等电信学校（Bretagne Télécom）。 （来源：云头条）

➢ 美国安全公司火眼(FireEye) 遭黑客攻击

2020 年 12 月 10 日，总部位于美国加州的火眼(FireEye)8 日证实，该公司用于测试客户防御能力的软件工具遭到一次高度复杂的国家级别网络攻击。据美国《华尔街日报》9 日报道，火眼表示，此次被黑客攻击的工具名为“红队”，此类工具可以用于检查火眼公司客户的防御系统，找出可能被攻击的漏洞此外，黑客还侵入了一些内部系统，主要寻求有关政府客户的信息。火眼透露，目前为止，还没有任何证据表明，存储客户数据的主系统有数据外泄。火眼公司在全球拥有大量客户，包括索尼等跨国企业，也包括美国国土安全部等美国联邦和地方政府部门。

火眼首席执行官、前空军军官凯文·曼迪亚在 8 日发表的一篇博客文章中说：“我的结论是，我们正在见证一场拥有顶级进攻能力的国家发动的袭击。袭击者专门针对火眼打造了世界级的攻击能力。”火眼表示，正在与美国联邦调查局(FBI)和包括微软在内的行业伙伴合作，继续调查此事。FBI 网络部门助理主管马特·戈汉姆在一份书面声明中表示，“FBI 正在

调查这起事件，初步迹象显示，实施者的老练程度达到了国家级别。”

报道援引了解调查情况人士的话称，黑客训练有素，罕见地使用了多种攻击工具的组合，其中一些工具显然以前没有在任何已知网络攻击中使用过，老练程度非同一般，同时也展示了不寻常的意志决心，而且这些工具是专门用于破坏火眼的。这些黑客据称还采用了先进的手段来隐藏自己的活动与身份。目前还不清楚此次攻击是在何时发生的，也不清楚火眼发现被攻击的确切时间，了解调查情况的人士称，该公司并不确定攻击者是如何入侵自身系统的。

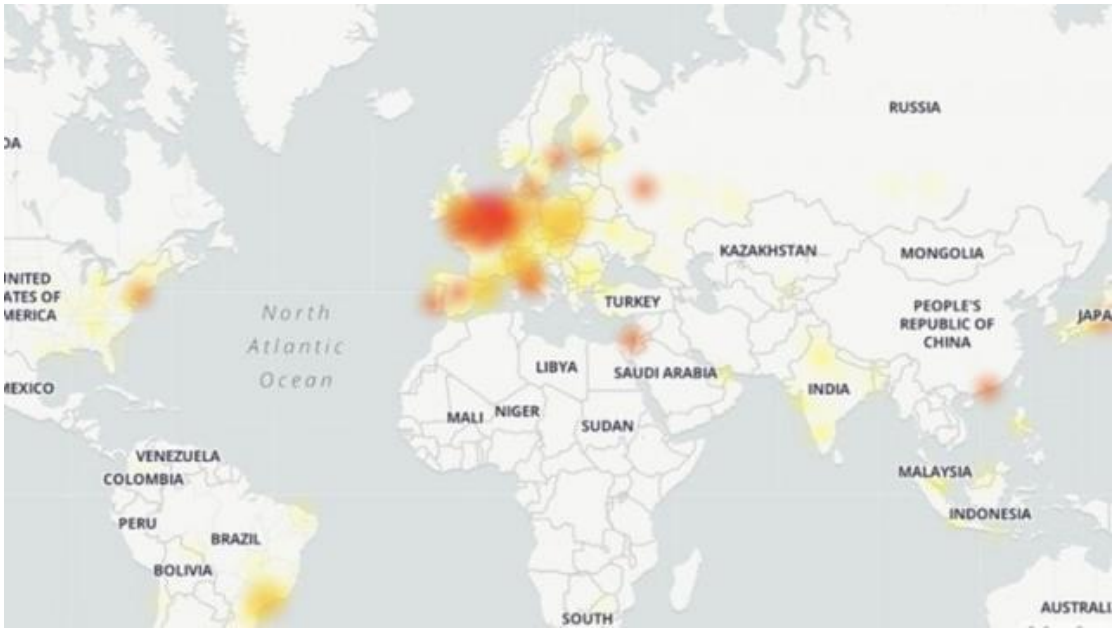
国内一名不具名的网络安全专家 9 日接受记者采访时表示：虽然火眼是全球最大的网络安全公司之一，但“没有黑不了的系统，就算再专业的安全公司也不能保证百分百安全”。这名网络安全专家表示，火眼之所以成为攻击目标，可能是由于拥有专业的网络攻击武器库，并掌握一些行业内尚未发现的漏洞，这些漏洞具有较高的价值。这并非是火眼公司首次遭到黑客攻击。2017 年，火眼旗下的 Mandiant 公司的内网也曾被黑客入侵，导致大量内部资料泄露。

上述网络安全专家表示，由于此次攻击手段主要是 APT 攻击，防御难度较大。所谓 APT 攻击是指高级可持续威胁攻击，不仅会采用传统的网络攻击技术，也会结合一些社会工程学手段，通过人的弱点结合漏洞进行尝试攻击。（来源：环球时报）

➢ 谷歌多项服务宕机 1 小时 数亿用户受到影响

2020 年 12 月 15 日报道，2020 年 12 月 14 日谷歌的多项服务出现无法访问的宕机问题，持续了大约 1 个小时左右。随后谷歌发布公告，表示本次宕机是由于“内部存储配额问题”导致的。虽然本次宕机的持续时间并不长，但由于在疫情期间很多人都在进行远程工作，因此全球有数亿用户受到影响。

那些依靠 Google Docs 和 Gmail 等谷歌服务工作或者教育的用户在这个时间段内无法访问，也无法使用例如 Google Maps 等流行服务。该问题和用户身份认证有关，而很多谷歌服务需要用户登录帐号才能使用。而那些不需要登录的谷歌服务（例如 YouTube），则以“隐身模式”提供。



在宕机发生之后谷歌就发布了声明：“我们对所有受到影响的用户表示歉意，我们将进行彻底的跟进审查，以确保以后不再出现此问题”。全球用户在美国时间上午 11:30 左右开始注意到问题，并报告 YouTube 面临问题。标签“ #googledown”迅速成为 Twitter 上最流行的术语之一。（来源：cnBeta）

➢ 美国政府遭遇大规模黑客袭击 微软竟然也中招了

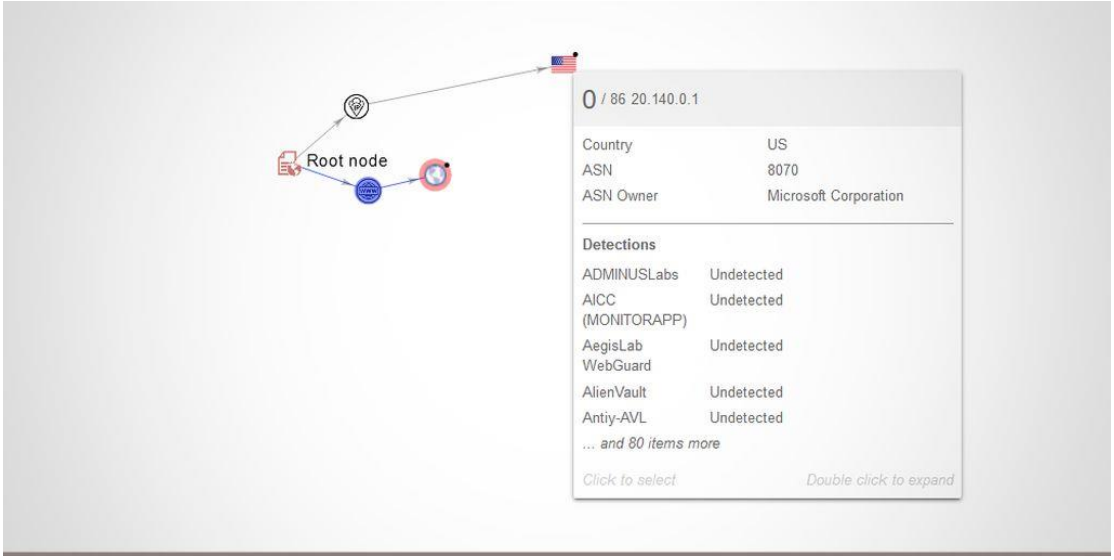
2020 年 12 月 17 日，微软公司表示，在其系统中发现了与美国官员本周披露的大规模黑客行动有关的恶意软件。这意味着，在越来越多的政府机构受到黑客攻击之际，受攻击的名单上增加了一家大型科技公司。据海外媒体报道，到目前为止，已知黑客至少监控了美国能源部、国防部、国务院、财政部、国土安全部、商务部和核安全局等的电子邮件或其他数据。美国候任总统乔·拜登发布声明表示，他将“把网络安全问题提升为整个政府的当务之急”，以防止此类重大黑客攻击。

微软在系统中发现恶意软件

微软公司是 SolarWind 公司广泛部署的网络管理软件 Orion 的客户。Orion 曾被用于疑

似俄罗斯对美国一些重要机构的攻击。知情人士说，微软自己的产品也被用来攻击受害者。

微软发言人表示： “与其他 SolarWinds 客户一样，我们一直在积极寻找该行动者的踪迹，并可以确认在我们的环境中检测到了 Solar Winds 二进制恶意文件，我们将其隔离并删除。”他还补充称，没有发现有“任何迹象表明我们的系统被用来攻击他人。”



一名熟悉黑客行为的人士说，黑客利用了微软的云服务，同时避开了微软的企业基础设施。微软没有立即回应有关这项技术的问题。不过，另一位知情人士说，美国国土安全部(DHS)认为微软是并不是新病毒感染的主要途径。微软和国土安全部仍在继续调查。国土安全部周四早些时候说，黑客使用了多种入侵方式。联邦调查局和其他机构计划在本周五为国会议员举行一次机密简报会。

美国政府多个机构遭到入侵

美国能源部还表示，有证据表明，作为行动的一部分，黑客入侵了能源部的网络。美国媒体早些时候曾报道，管理该国核武器储备的国家核安全局(NNSA)也成为了黑客袭击目标。到目前为止，已知黑客至少监控了美国国防部、国务院、财政部、国土安全部和商务部的电子邮件或其他数据。

能源部发言人表示，恶意软件“仅被局限于商业网络”，没有影响包括国家安全局在内的美国国家安全系统。国土安全部在公告中表示，黑客除了破坏 SolarWind 公司的网络管理软件更新外，还使用了其他技术。据了解，全球有数十万公司和政府机构都使用了 SolarWind 公司的网络管理软件 Orion 的更新版本。美国网络安全和基础设施安全署 （CISA）向调查人员强调，即便没有使用最新版本的 Solar Wing 的软件，也不要假设他们所在的系统就是安全的。CISA 同时指出，黑客并没有侵入他们拥有访问资格的所有网络。CISA 表示，正在继续分

析黑客使用的其他途径。

黑客几乎没有留下任何线索

SolarWinds 公司表示，多达 1.8 万名 Orion 用户下载了包含后门的更新版本。在黑客的入侵活动被发现后，SolarWinds 已经切断了与黑客维护的电脑之间的后门联系。但黑客可能还安装了其他入侵方式，CISA 说，这是 10 年来规模最大的黑客攻击。

据两名知情人士透露，美国司法部(Department of Justice)、联邦调查局(FBI)和国防部(Defense Department)等机构已经将日常通信转移到了据信没有被攻破的机密网络上。知情人士说，他们目前假设所有非机密网络都已被侵入。CISA 和包括 FireEye Inc 在内的私营企业公布了一系列线索，以供各机构查看自己是否受到了攻击。FireEye 是第一家发现并披露其被黑客攻击的公司。

但网络安全专家表示，攻击者非常谨慎，他们已经删除了日志、电子足迹或他们访问过哪些文件的线索。这使得安全专家很难知道他们获取了哪些文件。一些大型公司表示，没有证据表明他们受到了渗透，但在某些情况下，这也可能只是因为黑客删除了所有入侵记录。追踪调查的人士还透露，在大多数网络中，入侵者也能够创建虚假数据，但迄今为止，他们似乎只对获取真实数据感兴趣。

与此同时，国会议员要求提供更多信息，包括被盗文件、被盗方式以及幕后主使。此外，参议员们还要求了解是否黑客获得了个人税务信息。本周四美国众议院国土安全委员会和监督委员会宣布将展开调查。（来源：互联网综合整理）

➢ 黑客因泄露任天堂专有数据被判入狱三年，并赔偿 25.9 万美元

2020 年 12 月 14 日报道，据外媒报道，近日一名加州男子承认入侵日本游戏巨头任天堂的电脑系统，并泄露了公司的专有数据，被判三年监禁。

Ryan S. Hernandez 今年 21 岁，2016 年他和一名助手使用钓鱼技术窃取了任天堂一名员工的证件时，当时他还是未成年。这些凭证被用来访问和下载与该公司的游戏和控制台相关的机密文件，这些文件随后被泄露给公众。泄露的数据包括任天堂 Switch 游戏机的预发布信息。

2017 年，联邦调查局特工联系了 Ryan S. Hernandez 及其父母，就此次黑客袭击事件进行了调查。他网名为“瑞安·韦斯特”(Ryan West)。尽管他向特工保证不会再从事任何网

络犯罪活动，但至少从 2018 年 6 月到 2019 年 6 月，Ryan 继续侵入多个任天堂服务器，窃取有关视频游戏、开发工具和游戏机的机密信息。

这位不谨慎的黑客在 Twitter 和最初为游戏玩家创建的群组聊天平台上吹嘘自己的罪行。2020 年，他甚至创建了一个在线聊天论坛，名字为“Ryan 的地下聚会”，在那里，他与人们谈论了任天堂的产品，分享了从公司窃取的一些数据，并强调了任天堂电脑网络可能存在的漏洞。

美国联邦调查局(FBI)并没有忽视 Ryan 的活动，他们在 2019 年 6 月搜查了他的家，查获了用来获取盗版视频游戏和软件的规避设备。特工们还查获了大量电脑和硬盘，在这些电脑和硬盘上发现了数千份属于任天堂的机密文件。

通过对 Ryan 身上的设备进行分析显示，这名少年利用互联网收集了 1000 多部未成年人进行露骨行为的视频和图片。

2020 年 1 月，Ryan 承认犯有电脑欺诈、滥用职权罪，并同意向任天堂支付 259,323 美元的赔偿金。12 月 1 日，Ryan 被判处 3 年监禁。（来源：E 安全）

信息安全意识产品服务

021-33663299