国盟信息安全通报

2019 年 4 月 29 日第 191 期

国盟信息安全通报

（第 191 期）

国际信息安全学习联盟

2019 年 4 月 29 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 230 个，其中高危漏洞 96 个、中危漏洞 115 个、低危漏洞 19 个。漏洞平均分值为 6.13。本周收录的漏洞中，涉及 0day 漏洞 122 个（占 53%），其中互联网上出现“ApacheAxis 代码执行漏洞、QCMS 跨站请求伪造漏洞”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 1994 与上周（1755 个）环比增长 14%。

主要内容

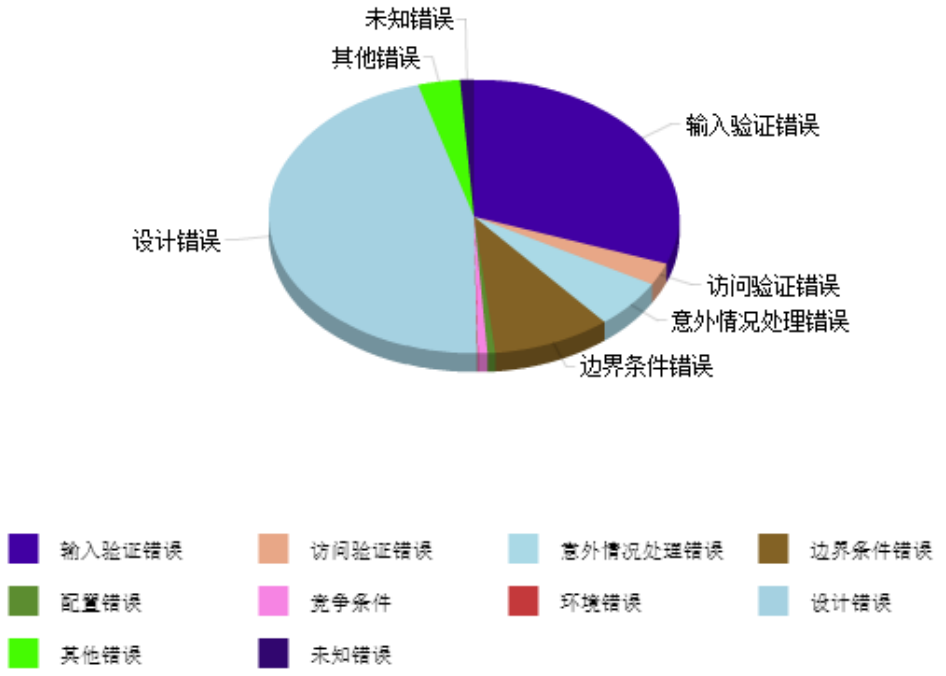
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

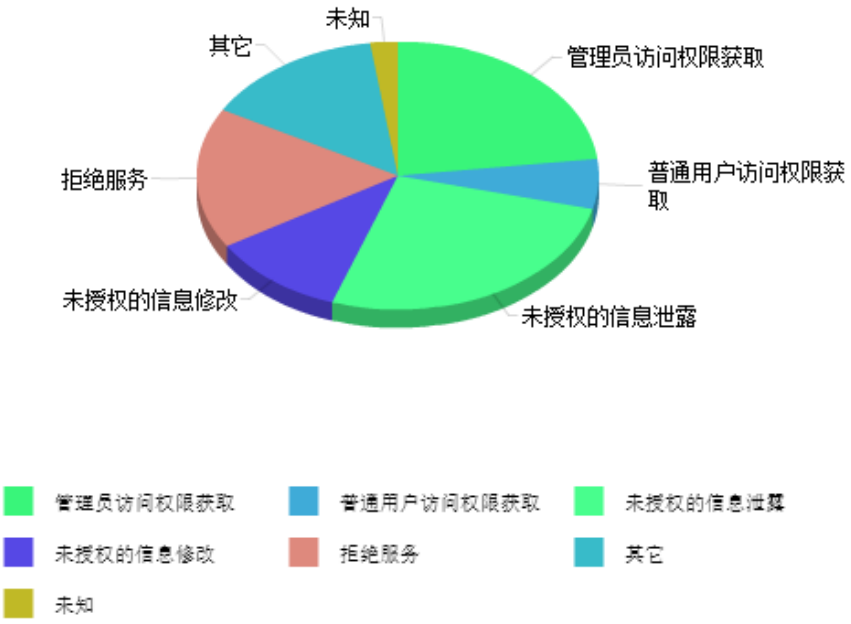
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 230 个，其中高危漏洞 96 个、中危漏洞 115 个、低危漏洞 19 个。漏洞平均分值为 6.13。本周收录的漏洞中，涉及 0day 漏洞 122 个（占 53%），其中互联网上出现“ApacheAxis 代码执行漏洞、QCMS 跨站请求伪造漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 1994 与上周（1755 个）环比增长 14%。

二、安全漏洞增长数量及种类分布情况

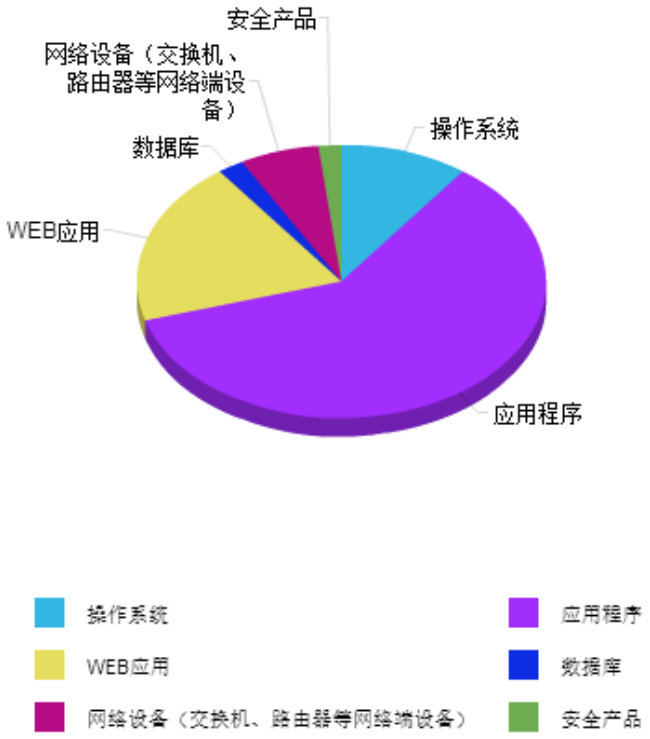
➢ 漏洞产生原因（2019 年 4 月 15 日—2019 年 4 月 29 日）



➢ 漏洞引发的威胁（2019 年 4 月 15 日—2019 年 4 月 29 日）



➢ 漏洞影响对象类型（2019 年 4 月 15 日—2019 年 4 月 29 日）



三、安全产业动态

➢ 确保网信事业始终沿着正确方向前进

党的十八大以来，以习近平同志为核心的党中央系统部署网络安全和信息化工作，不断推进理论创新和实践创新，走出一条中国特色治网之路，形成了网络强国战略思想，我国网信事业取得历史性成就，亿万人民在共享互联网发展成果上拥有更多获得感。

2014 年 2 月 27 日，习近平总书记在中央网络安全和信息化领导小组第一次会议上作出了“没有网络安全就没有国家安全，没有信息化就没有现代化”的重大判断；2016 年 4 月 19 日，习近平总书记在网络安全和信息化工作座谈会上擘画出我国网信事业的宏伟蓝图；2018 年 4 月 20 日，在全国网络安全和信息化工作会议上，习近平总书记高度概括了网络强国战略思想“五个明确”的丰富内涵，深刻回答了当前和今后一个时期我国网信事业发展的一系列方向性、全局性、根本性、战略性问题。

加强党中央对网信工作的集中统一领导

面对互联网领域新情况新问题新挑战，必须切实加强党中央对网信工作的集中统一领导，把网信工作摆在党和国家事业全局中来谋划。要以习近平新时代中国特色社会主义思想为指

导，把网络强国战略思想贯穿到网信工作各方面、诸环节，确保网信事业始终沿着正确方向前进。互联网管理是一项政治性极强的工作，讲政治是对网信部门第一位的要求。网信队伍要不断增强“四个意识”，坚持把党的政治建设摆在首位，自觉维护党中央权威和集中统一领导，自觉在思想上政治上行动上同以习近平同志为核心的党中央保持高度一致，不断完善坚持党的领导的体制机制。党的十八大以来，我们之所以能推动网信事业取得历史性成就，最根本的就在于有以习近平同志为核心的党中央的坚强领导，有网络强国战略思想的正确引领。

网信事业代表着新的生产力和新的发展方向

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。要发展数字经济，加快推动数字产业化；要推动互联网、大数据、人工智能和实体经济深度融合；要坚定不移支持网信企业做大做强，加强规范引导，促进其健康有序发展。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。

核心技术是国之重器

习近平总书记指出：“互联网核心技术是我们最大的‘命门’，核心技术受制于人是我们最大的隐患。”“在别人的墙基上砌房子，再大再漂亮也可能经不起风雨，甚至会不堪一击。”要成为网络强国，必须成为生产力意义上的网络强国，即在核心技术领域实现有效突破，具备网络技术强国的基本特征，能够在基础理论、实验室设计、工业生产以及市场竞争中占据关键地位，将中国建设成为真正的网络技术强国。要下定决心、保持恒心、找准重心，加速推动信息领域核心技术突破。要辩证看待对外开放和自主创新的关系。最关键最核心的技术要立足自主创新、自立自强。一定要坚持开放创新，只有跟高手过招才知道差距，不能夜郎自大。如何实现核心技术从“跟跑”到“领跑”的转变？习近平总书记明确指出要把握三个方面：“一是基础技术、通用技术。二是非对称技术、‘杀手锏’技术。三是前沿技术、颠覆性技术。”

树立正确的网络安全观

网络强国建设，离不开网络安全观的指引。互联网是意识形态工作的主阵地、最前沿，网络安全是国家安全的重要组成部分，“没有网络安全就没有国家安全”。国家安全是国家存在和发展最基本最重要的前提，网信工作必须置于总体国家安全观的视野下开展。“大国网络安全博弈，不单是技术博弈，还是理念博弈、话语权博弈”。网络安全是整体的而不是割

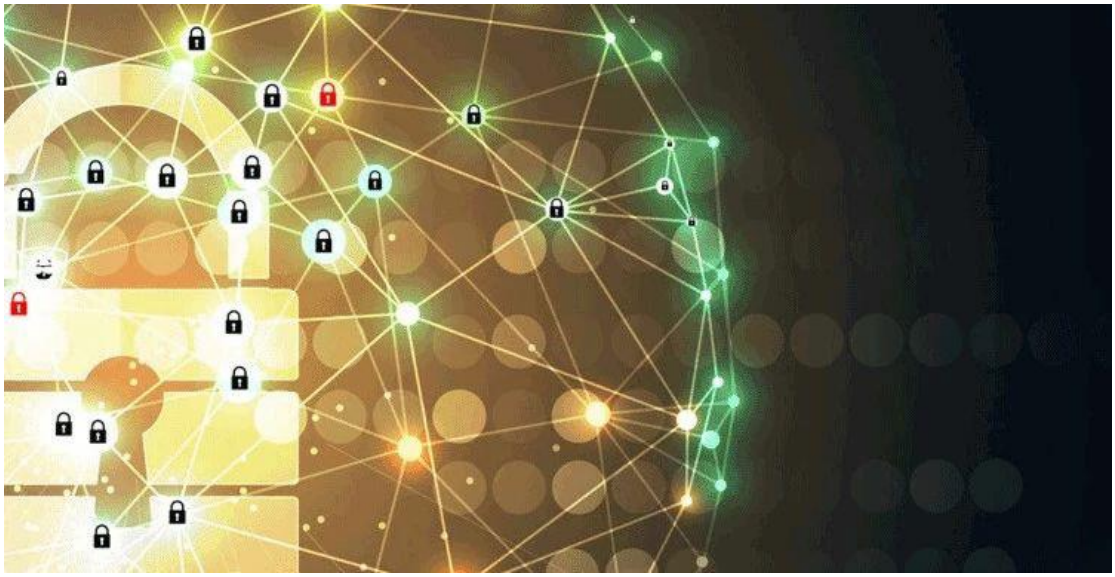
裂的，是动态的而不是静态的，是开放的而不是封闭的，是相对的而不是绝对的，是共同的而不是孤立的。无论是全球网络安全态势的风起云涌，还是中国网络强国建设的具体实践，都证明习近平总书记对网络安全重要论述的科学性，不仅点出了网络安全的要害，也指明了网络强国建设的方向。

推进全球互联网治理体系变革是大势所趋、人心所向

高速发展的互联网对全球互联网治理体系提出全新挑战。习近平总书记指出，国际网络空间治理应该坚持多边参与、多方参与，发挥政府、国际组织、互联网企业、技术社群、民间机构、公民个人等各种主体作用。既要推动联合国框架内的网络治理，也要更好发挥各类非国家行为体的积极作用。中国对互联网发展治理的国际主张，本质上就是要在尊重各国网络空间主权平等原则基础上，推进网络空间国际治理秩序的良性变革，最终建成网络空间命运共同体。（来源：求是网）

➢ 《互联网个人信息安全保护指南》若干要点解读

2019 年 4 月 10 日，公安部网络安全保卫局联合北京网络行业协会、公安部第三研究所正式发布了三部门联合发布《互联网个人信息安全保护指南》（附全文），这份指南是在 2018 年 11 月 30 日公安部网络安全保护局发布的《互联网个人信息安全保护指引(征求意见稿)》基础上，听取和采纳社会各方意见修改而成。



以下为指南的主要起草人就指引的若干内容所进行的解读，供大家参考。

1、编制背景

近年来，侵犯公民个人信息的现象日益增多，侵犯公民个人信息的违法犯罪行为也日益猖獗，更为严重的是，此类违法犯罪已经形成了完整的利益链，甚至是灰色产业链，给人们日常生活带来很大的干扰，直至造成财产损失，甚至危及人身安全。随着网络技术的发展，互联网行业持有个人信息的现象日益普遍，侵犯公民个人信息的违法犯罪也与计算机信息系统密切相关。

鉴于此，公安机关结合侦办侵犯公民个人信息网络犯罪案件和安全监督管理工作中掌握的情况，会同北京网络行业协会和公安部第三研究所等单位，研究制定了本指南。

2、适用范围

指南的第 1 章 范围明确了适用对象为“个人信息持有者”，即对个人信息进行控制和处理的组织或个人，指南正式版将征求意见稿的“互联网企业”进一步明确为“通过互联网提供服务的企业”，并且包含了其他“使用专网或非联网环境控制和处理个人信息的组织或个人”，也就是说除了传统意义的互联网企业，也包含金融、电信、交通、教育、医疗等行业，甚至存有大量公民个人信息的房产中介等企业，都应参考指南保护个人信息安全。

3、指南与一些法律法规的相关性

《网络安全法》特别加强和明确了个人信息保护方面的要求，指南的业务流程主要要求按照《网络安全法》编制的，一些细化要求参考了推荐性国家标准 GB/T 35273—2017《信息安全技术 个人信息安全规范》；

另外，《网络安全法》指出国家实行网络安全等级保护制度，指南的管理要求、技术要求和应急处置，都与《网络安全等级保护基本要求》(《信息系统安全等级保护基本要求》)相一致，履行保护义务，“保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改”为目标，这也是《网络安全法》的明确要求。另一方面，是否存在“窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息”等行为，也是《公安机关互联网安全监督检查规定(公安部令第 151 号)》的检查重点之一。

4、指南与等级保护定级的关系

指南对于网络安全等级保护级别的要求并非明确为三级。指南指出“应满足 GB/T 22239 相应等级的要求，按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改”，这与征求意见稿的“应按照 GB/T 22239—2008 7.1 第三级的…”略有不同，就是说具体按照《网络安全等级保护基本要求》的哪一级进行保护，则是需要经过等级保护定级备案的过程。

这就意味着，根据影响国家安全、社会秩序、公共利益以及相关公民、法人和其他组织

的合法权益的程度，涉及个人信息的数量和类别达到一定规模，仍需按照三级甚至更高级别进行防护。

5、指南中的个人信息是否分级

指南中“个人信息”完全引用了《网络安全法》的定义，与国家标准《个人信息安全规范》在个人信息之外还界定一个个人敏感信息不同，指南并不涉及个人敏感信息这个概念。这说明，指南提出的要求，是个人信息保护的最低要求。

6、关于匿名化的操作

在《个人信息安全规范》中，匿名化是指“通过对个人信息的技术处理，使得个人信息主体无法被识别，且处理后的信息不能被复原的过程。”这个术语与欧盟 GDPR 的匿名化说法有所不同。指南则不使用匿名化这个说法，直接引用《网络安全法》“经过处理无法识别特定个人且不能复原”的描述。

7、对于用户画像的要求

用户画像是互联网企业最常用的营销手段之一，涉及个人信息该如何合法合规使用是企业非常关心的问题。指南指出，“完全依靠自动化处理的用户画像技术应用于精准营销、搜索结果排序、个性化推送新闻、定向投放广告等增值应用，可事先不经用户明确授权，但应确保用户有反对或者拒绝的权利;如应用于征信服务、行政司法决策等可能对用户带来法律后果的增值应用，或跨网络运营者使用，应经用户明确授权方可使用其数据”。

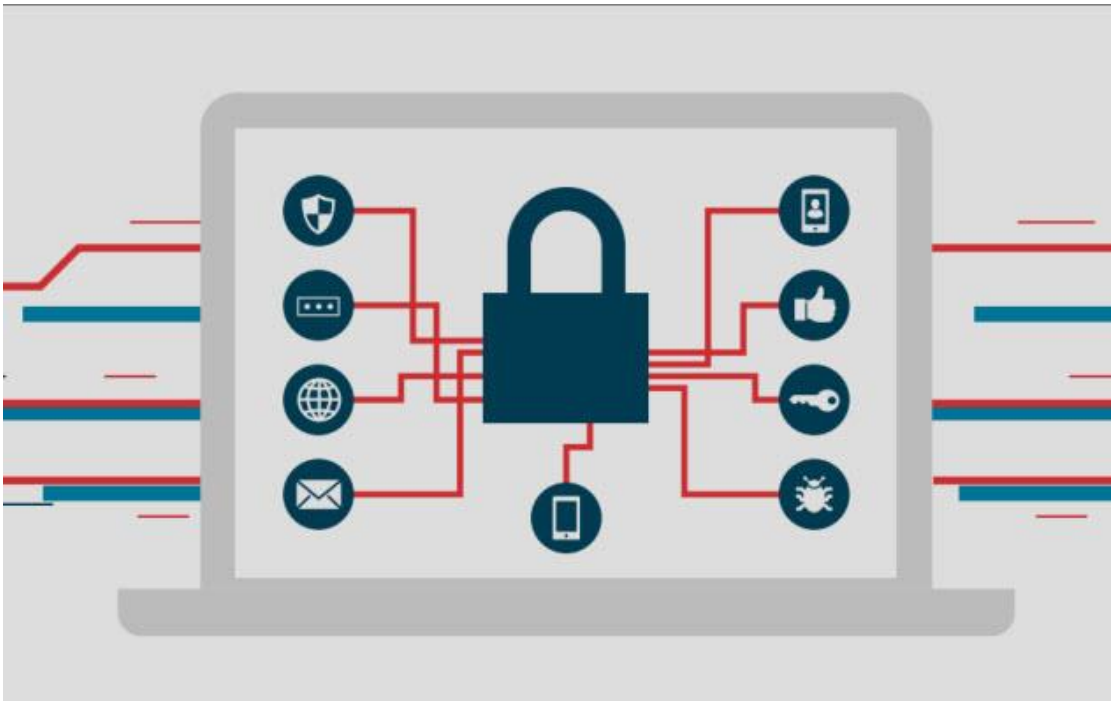
8、指南与 GB/T22239 和 GB/T35273 的章节对比

从具体内容看，指南的第 4 章 管理机制、第 5 章 技术措施、第 6 章 业务流程、第 7 章应急处置，与《网络安全等级保护基本要求》(《信息系统安全等级保护基本要求》)和《信息安全技术个人信息安全规范》两个国家标准从内容和要求上做了对接，具体如下表。（来源：国家网安检测中心）

《互联网个人信息安全保护指南》		GB/T 22239 信息安全技术 网络安全等级保护基本要求（修订中）	GB/T 35273-2017 信息安全技术 个人信息安全规范	其他说明
3 术语和定义			3.2/3.5/3.7 引用 GB/T 35273-2017 的定义	个人信息定义引用《网络安全法》
4 管理机制	4.1 基本要求	“应满足 GB/T 22239 相应等级的要求”		
	4.2 管理制度	8.1.6 安全管理制度	10 组织的管理要求	
	4.3 管理机构	8.1.7 安全管理机构	10.1 明确责任部门与人员	
	4.4 管理人员	8.1.8 安全管理人员	10.4 人员管理与培训	
5 技术措施	5.1 基本要求	“应满足 GB/T 22239 相应等级的要求”		引用《网络安全法》“按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改”
	5.2 通用要求			
	5.2.1 通信网络安全	8.1.2 安全通信网络		
	5.2.2 区域边界安全	8.1.3 安全区域边界		
	5.2.3 计算环境安全	8.1.4 安全计算环境		
	5.2.4 应用和数据安全	8.1.4 安全计算环境，尤其是数据部分	7.1 个人信息访问控制措施	
	5.3 扩展要求			
	5.3.1 云计算安全扩展要求	8.2 云计算安全扩展要求		
	5.3.2 物联网安全扩展要求	8.4 物联网安全扩展要求		
6 业务流程	6.1 收集		5 个人信息的收集	
	6.2 保存		6 个人信息的保存	
	6.3 应用		7 个人信息的使用	
	6.4 删除		7.6 个人信息删除	参考 GB/T 22239 中 8.1.4.10 剩余信息保护的部分要求
	6.5 第三方委托处理		8.1 委托处理	
	6.6 共享和转让		8.2 个人信息共享、转让	
	6.7 公开披露		8.4 个人信息公开披露	
7 应急处置	7.1 应急机制和预案	8.1.10.13 应急预案管理	9.1 安全事件应急处置和报告	
	7.2 处置和响应	8.1.10.12 安全事件处置	9.1 安全事件应急处置和报告 9.2 安全事件告知	

➢ 证券期货监管数据脱敏方案研究与实践

为充分发挥资本市场大数据在辅助监管决策、提升监管能力、创新监管方式、丰富监管手段方面的优势作用，证券期货监管系统正在开展监管科技的建设工作。监管科技的核心是大数据分析，前提是数据的共享和汇集。数据共享过程中，数据脱敏在防止敏感数据泄露、保护敏感数据方面起到重要作用，是大数据分析的一项基础性工作。



数据脱敏工作中的难点和痛点

1.数据脱敏需求不明确。数据脱敏需求部门在申请数据脱敏服务时，大多难以准确描述脱敏数据的需求，包括保留哪些字段、保留字段的哪些属性、哪些字段必须脱敏、哪些字段的统计信息必须保留或隐藏（如分布情况、均值变化、总和不变或是分类属性不变以及其他包含勾稽关系的信息）、针对具体字段使用的脱敏算法，通常简单笼统地提出不明确的需求。

2.敏感信息的不易界定。数据提供方进行敏感数据共享时，会重点考虑数据安全以及合规性，希望按照最小化原则提供数据；而数据使用方想得到更多更完整的数据，这就迫切需要细化对敏感数据的界定。例如，通常涉及公民个人信息，原则上应进行数据脱敏处理，但敏感数据不能简单理解为个人基本信息，因数据量、关联表信息、甚至通过关联其他资料等貌似非关键的信息，都有可能形成可推导出全局或个体信息的情况，造成泄露隐患。

3.数据保护与数据可用性间的平衡。数据脱敏不可避免造成数据信息损失。一方面，选择合适的脱敏规则或方法，需要性能较好的脱敏软件，以及对软件提供的各种工具的熟练掌握；另一方面，数据需求部门需要对脱敏工作充分介入、充分理解，共同寻找敏感数据的保

护程度以及数据可用性之间的平衡。

证券期货监管数据脱敏方案设计

建设完善的证券期货监管数据脱敏方案需要从工作流程和管理制度两个方面共同推进。为此，我们研究了数据脱敏工程方法和管理制度的规范化和标准化。

1.工程方法。数据脱敏的重要前提是明确数据的敏感性以及数据使用场景，依据数据敏感性和应用场景选择脱敏策略和算法。数据需求双方对数据脱敏方案的审核是数据脱敏工程实施的重要保障。按照上述数据脱敏工作思路，我们将数据脱敏工程方法分为“确定待脱敏数据”“确定数据应用场景”“确定脱敏策略和算法”“脱敏实施”“脱敏评价”五个步骤。数据脱敏工程实施流程图如图 1。

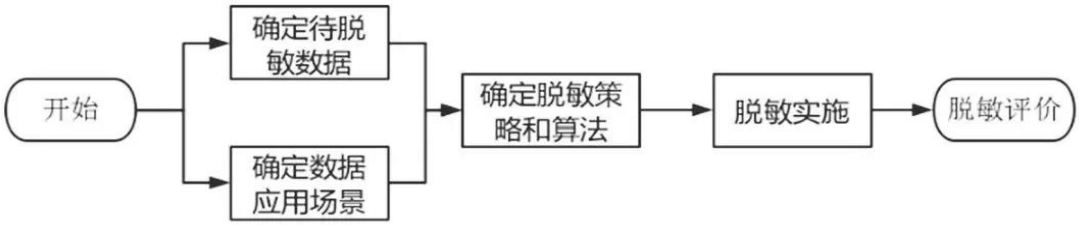


图 1 数据脱敏工程实施流程图

数据脱敏须充分考虑业务需求、数据安全以及法律法规。待脱敏数据通过敏感数据分类分级确定。敏感数据分类分级是有效发现敏感数据的基础性工作，可对敏感数据进行标记，确保数据脱敏能够充分考虑到应用范围、脱敏后数据对原数据业务特性的继承（如保持原数据间的依赖关系）等因素。在“最小够用”的原则下，通过分析数据脱敏需求的业务场景，明确待脱敏数据。针对无需脱敏的单个字段，应充分考虑多字段组合产生的敏感信息。

数据应用场景是数据使用方的网络环境、使用人员等情况的综合描述。其中，网络包括互联网、办公专网和内部网络等，使用人员包括开发、测试、分析人员等。根据网络环境、使用人员两个维度对数据应用场景进行分解，完成分类。

脱敏策略和算法应依据待脱敏数据和数据应用场景而确定，确定时要充分考虑数据的重要性、私密性和指向性，并从保全原始数据的数据特征角度，制定相应的数据脱敏策略和算法。

脱敏实施是在确定待脱敏数据、数据应用场景、脱敏策略和算法后，执行数据脱敏操作，并给出脱敏结果的过程。为保证敏感数据不泄露，数据必须在原网络环境下进行脱敏，数据使用方和提供方分别对数据脱敏需求与方案进行审核，双方确认后可将脱敏后的数据应用到业务所需场景和网络。

脱敏评价用于满足使用方要求、保证脱敏后的数据级别和场景的匹配度。在执行完脱敏操作后，数据使用方应与提供方共同开展脱敏评价，并进行交付。特别地，脱敏实施完成后，数据使用方应与提供方就脱敏后的数据是否会造成不良影响进行验证，验证环节应检查脱敏后数据是否与双方协商达成的数据脱敏方案一致。

2.管理制度。数据脱敏不仅仅依靠工程方法完成对敏感数据进行的共享和保护，还需要在制度上对参与人员的职责和数据安全管理等进行约束和说明。在建立数据脱敏管理制度时，应明确各参与方及其职责、数据访问日志、脱敏方案报备以及脱敏任务定期检查等。其中，数据脱敏参与方包括数据使用方、数据提供方和管理协调方。数据使用方负责提出数据脱敏要求，并对脱敏后的数据进行妥善管理；数据提供方负责评估数据使用方所提出的数据脱敏要求，执行数据脱敏操作，并将脱敏数据提供给使用方；管理协调方负责数据脱敏的组织管理。

数据提供方应记录数据脱敏过程日志，并对脱敏后数据及时清理；数据使用方应建立针对脱敏数据的访问控制机制，保证无关人员不能接触脱敏后数据，并保留脱敏数据访问日志，确保对脱敏数据的访问行为可审计；管理协调方负责对数据提供方与使用方的数据脱敏以及脱敏数据的管理情况进行定期与不定期的检查。

关键问题解决

在数据脱敏任务实施过程中，有三项关键问题需要引起重视：“敏感数据分级分类”“敏感数据应用场景定义”和“数据脱敏策略和算法”。

1.敏感数据分类分级。敏感数据分类分级包括对敏感数据的分类和分级。数据分类参考数据业务属性和数据技术属性。数据业务属性通常可按主体、行为进行分类。主体通常包括但不限于个人信息和机构信息等，行为一般可分为交易行为、监管行为、信息披露行为等。作为数据资产补充，数据技术属性依据数据类型的不同，成为选择脱敏算法的因素之一。字段的数据类型包括但不限于数字、字符串、日期时间、枚举等。遵照上述数据分类原则，数据敏感性分类示例见表 1。

一级分类	二级分类	示例
名称类	简称类	股票简称 、债券简称认购简称等
	全称类	开户人姓名、开户网点名称等
代码、编码类	用户编码类	身份证号、联系电话、个人标识等
	机构类编码类	工商注册登记号、组织机构类别代码等
	业务类	批准文号、海外市场上市标志等
	标识类	委托编号、订单编号、申请编号等
	地址类编码类	注册地址邮编、买入营业部、卖出营业部、交易所等
	交易类编码类	交割方式代码、交割类型代码、买卖标志代码等
	其他主键类	交易时段、周期代码
日期类	日期类	成交日期、委托日期、订单日期等
	时间类	交易时段、持仓日期等
数量类	数量类	成交数量、委托数量、持仓数量等
金额类	金额变化量类	涨跌幅等
	具体金额类	成交金额、成交价格、委托价格等
比率类	比率类	累计转股比例、当前票面利率等
地点类	地址类	公司地址、注册地址、地区名称等
字符串描述类	字符串描述类	资金账户类型描述、错误信息等
非结构化数据	图像类	用户照片、企业营业执照图像等
	文件类	企业内控审计报告等

表 1 敏感数据分类示例

数据敏感性等级认定可根据数据重要性、私密性、指向性的不同进行判断。重要性是指数据对市场运行的影响程度。私密性是指数据因描述个人或机构主体的隐私而不能被他人获取、得知的程度。指向性是指数据能够关联到特定对象的范围，分为单一主体（个人或机构）、特定群体（投资者类别、上市公司行业）或全市场。重要性、私密性、指向性分别用高、中、低三个级别来表示，认定规则见表 2、表 3 和表 4。

	参考说明
高	1. 可能导致全部业务无法开展，造成重大经济损失 2. 可能引发或导致《证券期货业信息安全事件报告与调查处理办法》确定的特别重大事件 3. 可能引发公众广泛诉讼或集体诉讼，甚至引发群体性事件 4. 可能导致监管部门严重处罚（包括但不限于取消经营资格、长期暂停相关业务等）的情况
中	1. 可能导致部分业务无法开展，造成一定经济损失 2. 可能引发或导致《证券期货业信息安全事件报告与调查处理办法》确定的重大事件 3. 可能引发一定数量投资者对本机构诉讼 4. 可能导致监管部门较严重处罚（包括但不限于一段时间内暂停经营资格或业务等）的情况
低	1. 有影响但可忽略，仅可能造成金额较小的轻微经济损失 2. 可能引发与本机构之间的轻微纠纷 3. 可能对本机构声誉造成轻微损害

表 2 重要性级别认定

	参考说明
高	涉及个人隐私或未过披露期的数据
中	涉及非特定对象隐私信息或个人非特征信息
低	不涉及个人隐私或已过披露期的数据

表 3 秘密性级别认定

	参考说明
高	指向某个个体、某个机构、某个产品
中	指向某类群体、某类机构、某类产品、某个行业
低	无确定指向

表 4 指向性级别认定

数据敏感级别可分为四级（1 至 4 级，0 表示非敏感数据），根据数据的重要性、私密性、指向性综合确定数据敏感性，并充分考虑数据量（全量/抽样）、数据关联关系以及数据时效性等因素对数据敏感性的影响。

一个可供参考的数据重要性、私密性、指向性与数据敏感级别对应关系，见表 5 数据定级规则参考表。

重要性	私密性	指向性	数据敏感级别
低	低	低/中/高	1
低	中	低/中/高	2
低	高	低/中	3
低	高	高	4
中	低	低/中/高	2
中	中	低/中	2
中	中	高	3
中	高	低/中	3
中	高	高	4
高	低	低	2
高	中	低/中	3
高	高	低/中	4
高	低/中/高	高	4

表 5 数据定级规则参考表

2.敏感数据应用场景定义。敏感数据应用场景定义通过分析待脱敏数据的各种应用场景，

并兼顾应用场景的网络环境，应用场景可分为五类。（1）内部分析。内部分析是指在同类业务网络中，由分析人员使用脱敏数据开展数据分析工作。（2）系统仿真。系统进行仿真实验所在网络与系统运行环境属于同一网络环境，使用人员多为开发测试人员。（3）监管协作。监管协作是将脱敏数据提供给其他会管单位或外部监管协作机构，在其业务网络中使用，使用人员为监管业务人员。（4）外部分析。外部分析用于互联网环境下分析人员使用。较内部分析而言，网络环境开放、安全级别较低。（5）开放测试。开放测试用于互联网开放测试，即：使用人员不限、网络环境开放、安全级别最低。

3.数据脱敏策略和算法。在进行数据脱敏时，脱敏策略和算法的选择需充分考虑数据类型。脱敏策略包括字段的全部或部分脱敏、可逆或不可逆；常见数据脱敏算法包括置常数、随机查表替换、固定参数查表替换、码值随机偏移、码值固定参数偏移、随机算数置换、固定参数算数置换、随机生成定长字符串、随机生成不定长字符串、字符串部分屏蔽、时间部分替代等。其中，数据脱敏策略和算法与数据类型之间的适用关系见表 6。

	全部脱敏算法	部分脱敏算法	可逆算法	不可逆算法
字符型	随机查表替换、随机生成定长字符串、随机生成不定长字符串、字符串部分屏蔽	字符串部分屏蔽	无	随机查表替换、随机生成定长字符串、随机生成不定长字符串、字符串部分屏蔽
日期型	置常数、随机查表替换、固定参数算数置换、时间部分替代	固定参数算数置换、时间部分替代	固定参数算数置换	置常数、随机查表替换、时间部分替代
数字型	置常数、随机查表替换、码值随机偏移、码值固定参数偏移、随机算数置换、固定参数算数置换	随机算数置换、固定参数算数置换	固定参数算数置换、码值固定参数偏移	置常数、随机查表替换、码值随机偏移、随机算数置换
枚举型	随机查表替换、固定参数查表替换、码值固定参数偏移	无	码值固定参数偏移、固定参数查表替换	随机查表替换

表 6 数据脱敏算法与数据类型之间的适用关系

数据脱敏实践

2018 年，我们在研究证券期货监管数据脱敏方案的基础上，开展了数据脱敏试点工作，在“脱敏工具选择”“数据脱敏实施”和“数据脱敏审计”等三项具体工作中有如下体会。

1.数据脱敏工具选择。数据脱敏工具需内置敏感数据匹配模式，帮助用户发现部分敏感数据。此外，工具还需内置常用的脱敏算法，并提供脱敏算法扩展接口，方便用户扩展脱敏

算法。经脱敏后的数据应在格式、内涵及数据间关系上保持与原数据一致，方便业务人员理解和应用数据。同时，数据脱敏工具应具备高效性和可靠性，保证数据脱敏工作效率，并确保脱敏结果的有效性。

2.数据脱敏实施。保证数据安全以及规范数据操作是数据脱敏的前提，数据脱敏工作应严格按照上述工程方法和管理制度进行数据脱敏实施。目前，我们已在实践中完善了脱敏流程和脱敏工具，验证了工程方法和管理制度的正确性。

3.数据脱敏审计。数据脱敏检查工作按照事前、事中和事后分别进行检查，事前、事中检查按照监管科技数据脱敏工程方法和数据脱敏管理制度实施；事后检查依靠数据脱敏审计，对数据提供方与使用方的数据脱敏以及脱敏数据的管理情况进行定期与不定期的检查。

（来源：本文节选自《金融电子化》2019 年 3 月刊）

➢ 《2018 年我国互联网网络安全态势综述》报告发布

2019 年 4 月 16 日，由国家互联网应急中心（以下简称“CNCERT”）主办的《2018 年我国互联网网络安全态势综述》（简称“2018 年态势报告”）发布会在京举行。来自中央网信办、工业和信息化部、公安部等政府部门、重要信息系统单位、电信运营企业、域名注册管理和服务机构、互联网和安全企业等 80 多家单位的专家和代表出席会议。

CNCERT 卢卫副书记表示，2018 年，我国进一步健全网络安全法律体系，完善网络安全管理体制机制，持续加强公共互联网网络安全监测和治理，构建互联网发展安全基础，构筑

网民安全上网环境，特别是在党政机关和重要行业方面，网络安全应急响应能力不断提升，恶意程序感染、网页篡改、网站后门等传统的安全问题得到有效控制。全年未发生大规模病毒爆发、大规模网络瘫痪的重大事件，但关键信息基础设施、云平台等面临的安全风险仍较为突出，APT 攻击、数据泄露、分布式拒绝服务攻击等问题仍较为严重。

中央网信办网络安全协调局刘博处长表示，2018 年态势报告对了解我国网络安全形势、提高网络安全意识具有重要参考意义。中央网信办网安局将继续发挥统筹协调作用，从强化网络安全工作责任制落实、统筹推进关键信息基础设施保护、强化数据安全保护、增强态势感知和应急指挥能力、促进网络安全产业发展、加强网络安全人才培养和意识教育等方面持续发力，筑牢国家网络安全屏障。工业和信息化部网络安全管理局袁春阳副处长介绍了工信部作为行业主管部门在电信、互联网和工业领域开展的网络安全管理工作。公安部网络安全保卫局盘冠员处长总结了 2018 年网络安全突出特点，并介绍了公安机关针对当前互联网安全隐患问题开展的行动。

会上，CNCERT 发布了 2018 年态势综述报告，并对该报告进行了详细阐述。报告坚持立足于 CNCERT 自有监测数据与工作实践，结合 2018 年典型网络安全事件、网络安全新趋势及日常网络安全事件应急处置实践成果编撰而成，为我国党政机关、行业企业及社会公众提供了有力参考。报告从网络安全法律法规、网络安全威胁治理、勒索软件威胁、APT 攻击、云平台安全、拒绝服务攻击、工业控制系统安全、恶意移动应用和数据安全等共九个方面对 2018 年我国互联网网络安全状况进行了总结。报告还对网络安全趋势进行了四点预测，认为 2019 年带有特殊目的和针对性更强的网络攻击、国家关键信息基础设施安全、个人信息与数据安全、5G 与 IPv6 等新技术安全值得关注。（来源：国家互联网应急中心）

- **《2018 年我国互联网网络安全态势综述》报告**
- **全文：**http://www.cert.org.cn/publish/main/upload/File/2018situation.pdf

四、政府之声

➢ 工信部部署开展 2019 年 IPv6 网络就绪专项行动

2019 年 4 月 16 日， 为深入贯彻落实《推进互联网协议第六版（IPv6）规模部署行动计划》（以下简称“《行动计划》”），持续推进 IPv6 在网络各环节的部署和应用，全面提升用户渗透率和网络流量，加快提升我国互联网 IPv6 发展水平，工业和信息化部近期印发了《工业和信息化部关于开展 2019 年 IPv6 网络就绪专项行动的通知》工信部通信函〔2019〕95 号。（以下简称“《专项行动》”），对 2019 年 IPv6 规模部署相关任务的组织实施工作提出了具体的改造措施和相应目标要求。

2018 年基础电信企业已经基本完成 LTE 网络、城域网、接入网、5 个互联网骨干直联点 IPv6 改造，初步实现 IPv6 网络连通、承载能力。但据部分互联网企业反应，IPv6 网络质量不佳导致用户访问体验受到影响，成为互联网企业在应用上线、用户放量阶段的主要顾虑。为此，工业和信息化部专门对 IPv6 网络性能进行监测，发现三家基础电信企业部分骨干、城域 IPv6 网络平均时延、丢包率等指标较 IPv4 网络偏大，客观存在 IPv6 网络性能较差的问题，急需优化。

针对上述突出问题，2019 年《专项行动》将提升 IPv6 网络和服务的质量作为本年度 IPv6 规模部署的重点举措，一是要求基础电信企业持续优化 IPv6 网络传输性能，保证用户在 IPv6 环境下的实际访问体验不会降低；二是要求数据中心、内容分发网络、云服务平台为用户提供与 IPv4 趋同质量的 IPv6 服务。到 2019 年第三季度末，IPv6 网络基础设施、应用基础设施的平均丢包率、时延等网络指标与 IPv4 性能相比劣化不超过 10%。（来源：国家广播电视总局）

- **《工业和信息化部关于开展 2019 年 IPv6 网络就绪专项行动的通知》全文：**

- http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757020/c6791277/content.html

➢ 三部门联合发布《互联网个人信息安全保护指南》

2019 年 4 月 19 日，公安部网络安全保卫局、北京网络行业协会、公安部第三研究所联合发布《互联网个人信息安全保护指南》

为深入贯彻落实《网络安全法》，指导个人信息持有者建立健全公民个人信息安全保护管理制度和技术措施，有效防范侵犯公民个人信息违法行为，保障网络数据安全和公民合法权益，公安机关结合侦办侵犯公民个人信息网络犯罪案件和安全监督管理工作中掌握的情况，会同北京网络行业协会和公安部第三研究所等单位，研究制定了《互联网个人信息安全保护指南》。现正式发布，供互联网企业、联网单位在个人信息安全保护工作中参考借鉴。

（来源：公安部网络安全保卫局）

- **《互联网个人信息安全保护指南》**
- **全文：**http://www.beian.gov.cn/portal/index.do

➢ 国资委印发《中央企业负责人经营业绩考核办法》

2019 年 3 月 7 日，国务院国有资产监督管理委员会发布了新版《中央企业负责人经营业绩考核办法》，该办法将于自 2019 年 4 月 1 日起施行。与旧版的考核办法不同的是，新的考核办法中增加了对网络安全事件的考核要求。

具体体现在新办法的第 34 条和 48 条，如下：

第三十四条 建立重大事项报告制度。企业发生较大及以上生产安全责任事故和网络安全事件、重大及以上突发环境事件、重大及以上质量事故、重大资产损失、重大法律纠纷案件、重大投融资和资产重组等，对经营业绩产生重大影响的，应及时向国资委报告。

第四十八条 企业发生下列情形之一的，国资委根据具体情节给予降级或者扣分处理；违规经营投资造成国有资产损失或其他严重不良后果，按照有关规定对相关责任人进行责任追究处理；情节严重的，给予纪律处分或者对企业负责人进行调整；涉嫌犯罪的，依法移送国家监察机关或司法机关查处。

(一)违反《中华人民共和国会计法》《企业会计准则》等有关法律法规规章，虚报、瞒报财务状况的；(二)企业法定代表人及相关负责人违反国家法律法规和规定，导致发生较大及以上生产安全责任事故和网络安全事件、重大及以上突发环境事件、重大质量责任事故、重大违纪和法律纠纷案件、境外恶性竞争、偏离核定主业盲目投资等情形，造成重大不良影响或者国有资产损失的。（来源：国有资产监督管理委员会）

- **《中央企业负责人经营业绩考核办法》**
- **全文：**http://www.sasac.gov.cn/n2588035/n2588320/n2588335/c10652592/content.html

➢ 国务院印发政府网站与政务新媒体检查指标、监管工作年度考核指标

2019 年 4 月 18 日，国务院办公厅秘书局关于印发政府网站与政务新媒体检查指标、监管工作年度考核指标的通知。通知要求：各省、自治区、直辖市人民政府办公厅，国务院各部委、各直属机构办公厅（室）：

为进一步推动全国政府网站和政府系统政务新媒体健康有序发展，国务院办公厅制定了《政府网站与政务新媒体检查指标》和《政府网站与政务新媒体监管工作年度考核指标》，现印发给你们，请认真贯彻执行。各地区、各部门要进一步加强和完善政府网站及政务新媒体日常管理和常态化监管工作。国务院办公厅将每半年对全国政府网站及政务新媒体运行情况进行抽查，每年度对有关监管工作进行考核，抽查和考核结果将予以公开通报。（来源：国务院办公厅秘书局 ）

- **《政府网站与政务新媒体检查指标、监管工作年度考核指标的通知》**
- **全文：**http://www.gov.cn/zhengce/content/2019-04/18/content_5384134.htm

五、本期重要漏洞实例

➢ Linux Kernel 本地信息泄露漏洞

发布日期：2019-02-07
更新日期：2019-04-24
受影响系统：
Linux kernel <= 4.20.5
描述：

BUGTRAQ ID: 106963
CVE(CAN) ID: CVE-2019-7222
Linux kernel 是美国 Linux 基金会发布的开源操作系统 Linux 所使用的内核。
Linux kernel 4.20.5 及之前版本的 KVM 执行存在一个信息泄露漏洞。攻击者可利用此漏洞获取信息。

<*来源：Felix Wilhelm
链接：
https://git.kernel.org/pub/scm/virt/kvm/kvm.git/commit/?id=353c0956a618a07ba4bbe7ad00ff29fe70e8412a
*>
建议：

厂商补丁：
Linux

Linux 已经为此发布了一个安全公告（CVE-2019-7222）以及相应补丁：
CVE-2019-7222：KVM: x86: work around leak of uninitialized stack contents
链接：
https://git.kernel.org/pub/scm/virt/kvm/kvm.git/commit/?id=353c0956a618a07ba4bbe7ad00ff29fe70e8412a

➢ OpenSSH 用户枚举漏洞

发布日期：2018-08-16
更新日期：2019-04-24
受影响系统：
OpenSSH OpenSSH <= 7.7
描述：

BUGTRAQ ID: 105140

CVE(CAN) ID: CVE-2018-15473
OpenSSH（OpenBSD Secure Shell）是 OpenBSD 计划组所维护的一套用于安全访问远程计算机的连接工具。该工具是 SSH 协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。
OpenSSH 7.7 及之前版本存在一个用户枚举漏洞，原因是在完全解析含有请求的报文之前不能推迟对无效验证用户的救助。此漏洞与 auth2-gss.c、auth2-hostbased.c 和 auth2-pubkey 相关。

<*来源：OpenSSH

链接：https://bugzilla.redhat.com/show_bug.cgi?id=1619063
*>

建议：

厂商补丁：
RedHat

RedHat 已经为此发布了一个安全公告（CVE-2018-15473）以及相应补丁：
CVE-2018-15473：openssh: User enumeration via malformed packets in authentication requests
链接：https://bugzilla.redhat.com/show_bug.cgi?id=1619063

➢ Symantec Endpoint Protection 安全绕过漏洞

发布日期：2019-04-23
更新日期：2019-04-23
受影响系统：
Symantec Endpoint Protection <= 12.1 RU6 MP9
Symantec Endpoint Protection < 14.2 RU1
描述：

BUGTRAQ ID: 107999
CVE(CAN) ID: CVE-2018-12244
Symantec Endpoint Protection（SEP）是美国赛门铁克（Symantec）公司的一套防病毒软件。该软件可跨物理和虚拟系统提供安全防护功能。

SEP 12.1 RU6 MP9 及之前版本、14.2 RU1 之前版本存在一个安全绕过漏洞，允许攻击者绕过安全限制并进行越权操作。

<*来源：Ayushman Dutta

链接：https://support.symantec.com/en_US/article.SYMSA1479.html
*>

建议：

厂商补丁：
Symantec

Symantec 已经为此发布了一个安全公告（SYMSA1479）以及相应补丁：
SYMSA1479：Norton SEP Multiple Issues
链接：https://support.symantec.com/en_US/article.SYMSA1479.html

➢ Apache Pony Mail 跨站脚本漏洞

发布日期：2019-04-20
更新日期：2019-04-20
受影响系统：
Apache Group Pony Mail 0.9
Apache Group Pony Mail 0.8B
Apache Group Pony Mail 0.10
不受影响系统：
Apache Group Pony Mail 0.11
描述：

BUGTRAQ ID: 108046
CVE(CAN) ID: CVE-2019-0218

Apache Pony Mail 是美国阿帕奇（Apache）软件基金会的一款具有邮件归档、查看和交互功能的插件。Apache Pony Mail 0.8 至 0.10 版本存在一个跨站脚本漏洞，允许攻击者在 Pony Mail 界面中的 JavaScript 通过特制 URL 进行反射型跨站脚本攻击。

<*来源：Francesco Soncina - ABN AMRO Red Team

链接：
https://lists.apache.org/thread.html/18a7ff26bc31a77e32e5e02e65dc86b1c41b610c753f8927d2cf955a@%3Cdev
*>
建议：

厂商补丁：
Apache Group

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：
http://www.apache.org

六、本期网络安全事件

➢ Facebook 承认员工可获取数百万 Instagram 用户的明文密码

2019 年 4 月 19 日，Facebook 周四称，该公司员工可在一个内部数据库中看到数以百万计的 Instagram 用户密码，这些密码以可搜索的格式存储在数据库中。Facebook 此次宣布的这一消息是对上个月发表的一篇博文的更新，当时该公司披露信息称，公司员工可以看到数百万 Facebook 用户密码。

Facebook 在这篇博文中提供的最初说法是，数以千计的 Instagram 密码被泄露。网络安全记者布赖恩·克雷布斯（Brian Krebs）则在 3 月报道称，最多 6 亿个 Facebook 密码遭到泄露。

Facebook 在博文中表示，除了此前提到的数千名用户以外，该公司将进一步向密码被泄露的数百万名 Instagram 用户发出通知。Facebook 还称，该公司在进行内部调查后确定，这些密码并未“被滥用或不正当地访问”。但是，数千名 Facebook 员工本可看到这些密码，而且自此事在今年 3 月被首次曝光以来，Facebook 一直都没有提供调查的最新信息。

在纳斯达克周四的常规交易中，Facebook 股价小幅下跌 0.50 美元，报收于 178.28 美元，跌幅为 0.28%。（来源：新浪科技）

➢ 搜 Wi-Fi 热点 Android 应用数据泄露涉 200 多万 WiFi 密码

2019 年 4 月 22 日，一款流行的 Android 热点（WiFi）搜寻 App“WiFi Finder”暴露了 200 多万个网络的 WiFi 密码。目前已有数千人下载了这款 WiFi Finder 应用，它允许用户搜索附近的 WiFi 网络。但同时，这款应用也允许用户将 WiFi 密码从自己的设备上传到数据库，供其他人使用。

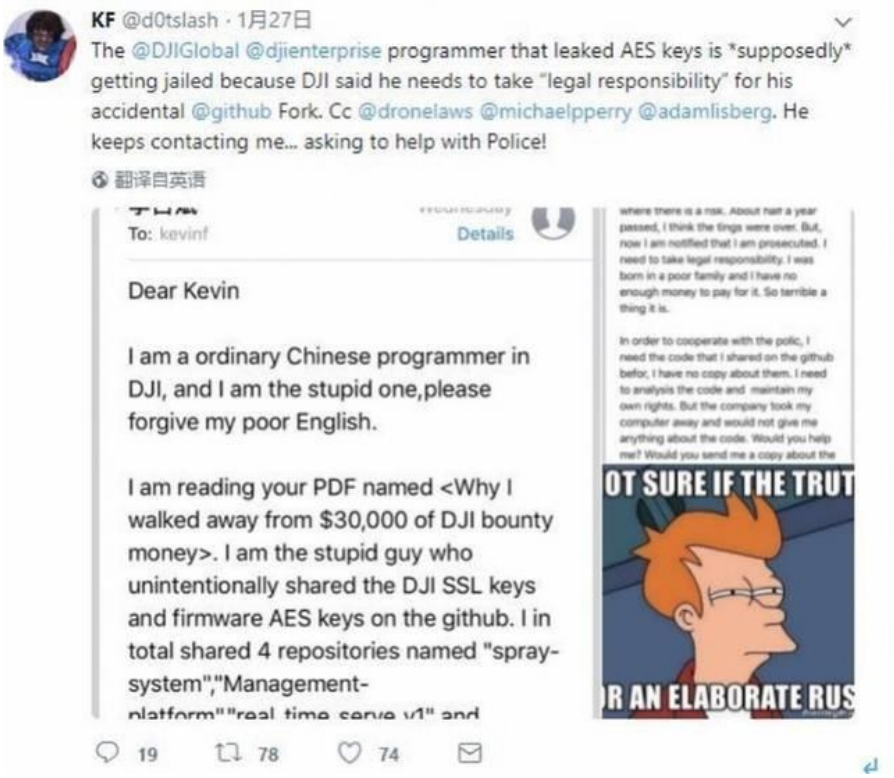
这个包含了 200 多万个网络密码的数据库并未受到任何保护，允许任何人访问，并批量下载这些内容。

网络安全研究人员萨亚姆·杰恩（Sanyam Jain）率先发现了这个数据库，并将其发现报告给了 TechCrunch。TechCrunch 试图联系开发商，但无济于事。

最后，TechCrunch 联系上了数据库托管商 DigitalOcean，后者在一天内就关闭了该数据库。据悉，数据库中的每条记录都包含了 WiFi 网络名称、精确的地理位置、基本服务集标识符（BSSID）和明文存储的网络密码。（来源：新浪科技）

➢ 泄露公司源代码造成百万损失：大疆前员工被罚 20 万获刑半年

2019 年 4 月 27 日，据深圳法院近日对大疆源代码泄露案做出一审判决，综合考虑犯罪情节以及自愿认罪、有悔罪表现，以侵犯商业秘密罪判处大疆前员工有期徒刑六个月，并处罚金 20 万人民币。据悉，这些泄露出去的代码，已用于该公司农业无人机产品，具有实用性。尽管大疆公司采取了合理的保密措施，但该次事件依然给大疆造成经济损失 116.4 万元人民币。



根据深圳市人民检察院披露的内情，2017 年安全研究员 Kevin Finisterr 在大疆的网络安全方面发现了一个非常严重的漏洞。这个漏洞能让攻击者获取到 SSL 证书的私钥，并允许他们访问存储在大疆服务器上的客户敏感信息，这使得大疆的所有旧密钥毫无用处，从而可能导致大疆服务器上的用户信息、飞行日志等私密信息能被下载。

经过大疆公司的调查，这个漏洞是大疆的一名前员工通过一个计算机指令，将含有公司农业无人机的管理平台和农机喷洒系统两个模块的代码上传至 GitHub 网站的“公有仓库”，造成了源代码泄露。

据悉，该员工之前在大疆的子公司担任软件工程师，公司对他很器重，负责编写农业无人机的管理平台和农机喷洒系统代码。他在 Github 开设账号，并建立了“公有仓库”。

据悉，Github 网站是全球最大的代码分享社区，拥有超过 900 万开发者用户，去年被微

软斥巨资收购，足见其影响力。在该网站上，程序员可以设立“公有仓库”或“私有仓库”存放代码，其中“共有仓库”对全球用户可见，用户可以通过搜索发现并下载别人分享的代码。众所周知，源代码意味着高新企业的财产权、竞争力乃至生命线，是公司千方百计保护的对象。

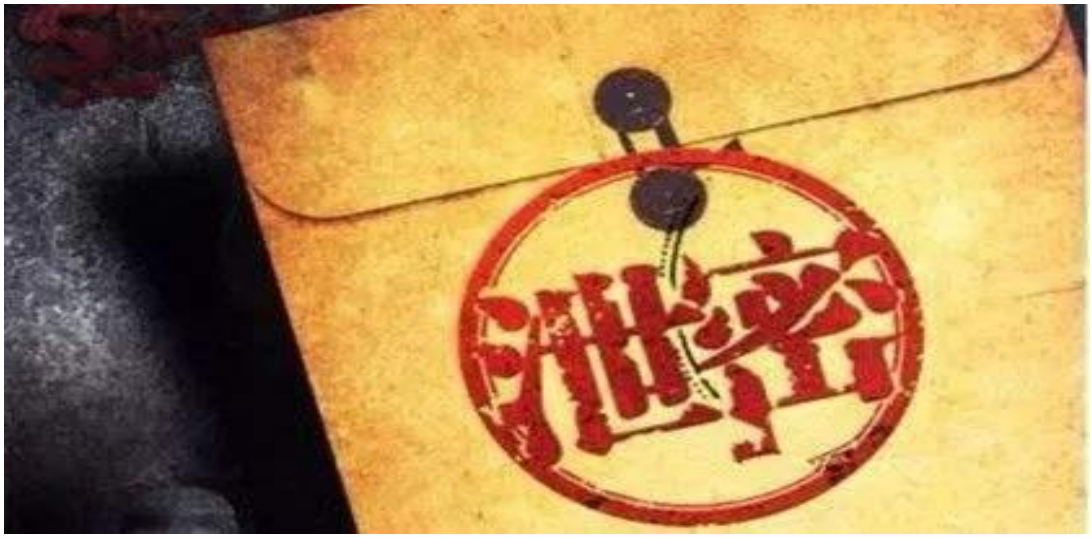
经鉴定，大疆这些泄露出去的代码具有非公知性，且已用于该公司农业无人机产品，属于商业秘密。经评估，这次泄漏公司造成经济损失 116.4 万元人民币。案发后，这位员工第一时间删除了相关代码，并积极配合调查，防止事态扩大。

他在推特上表示，“无意泄露了大疆的机密”、“我很后悔自己没有法律意识，我愿意承担相应的法律责任。”根据刑法规定，违反权利人关于保守商业秘密的要求，披露其所掌握的商业秘密，造成严重后果，应当以侵犯商业秘密罪追究刑事责任。（来源：快科技）

➢ 国家安全机关公布三起「境外网络攻击窃密」案件

2019 年 4 月 18 日，随着我国综合国力和国际地位显著提升，境外间谍情报机关将我国作为主要目标，日益将网络攻击窃密作为其情报窃密的主要方式之一。国家安全机关工作中已发现多个国家和地区的间谍情报机关对我国实施网络攻击窃密活动，攻击目标涉及计算机、电子邮箱、移动智能终端、重要信息系统、关键信息基础设施等。

国家安全机关正持续加大对境外间谍情报机关网络攻击窃密的打击力度，有效控制境外间谍情报机关对我国网络攻击窃密造成的危害。近日，国家安全机关发布三起破获的境外间谍情报机关对我国实施的网络攻击窃密案件，旨在进一步提高全社会网络安全意识，筑牢信息安全防线。



案件一：N 网络科技公司重要信息系统被境外间谍情报机关攻击窃密案

N 网络科技公司是国内重要的电子邮件系统安全产品提供商，主要负责客户单位内部电子邮件系统的设计、开发和维护。因为具有涉密邮件管理系统建设资质，该公司在很多重要领域拥有广泛的客户群体。随着口碑的积累和业务不断发展，N 公司的客户持续增加。

由于公司人员有限，所以经常会出现一个员工对接多个客户，或者一个客户面对不同员工的情况。于是，N 公司把众多客户的地理位置、网管人员身份等敏感信息储存在公司的内网服务器中，以便员工随时查询使用。但与此同时，为节约成本，N 网络科技公司网络安全防范措施很不到位，相关设备系统陈旧，安全漏洞多，安全保密制度执行不严格，公司员工违规在内外网之间搭建通道，长期存在严重网络安全隐患。

国家安全机关工作发现，从 2014 年起，该公司的核心应用服务器先后被三家境外间谍情报机关实施了多次网络攻击，窃取了大量敏感数据资料，对我国网络安全和国家安全构成危害。

该案发生后，N 公司被责令停业整改，并被行业主管部门处以罚款，同时，国家安全机关要求 N 公司逐一对此次事件涉及的用户单位进行安全加固，消除危害影响。

案件二：W 市某机关人员计算机违规存储涉密资料网络窃密案

2018 年 8 月，国家安全机关工作发现，W 市农业局人事科干部王某使用的办公计算机被境外间谍情报机关远程控制。经对王某的计算机进行核查取证，发现里面除了日常办公文档，还有多份标注密级的地形图。

王某称，这些地形图是帮同事肖某制作方案而留存的。肖某是该局下属某事业单位工作人员，每年会接到工作任务，在编制方案的时候，需要做工程规划布局图。不会电脑制图的肖某便找王某帮忙。肖某从档案室借出当地的航拍地形图，分区扫描成电子版并保存在自己的办公电脑中，通过 QQ 从互联网上将图发送给王某。按照肖某的要求，王某使用制图软件在地形图上标注涉及工程建设的信息，完成制图后，再通过 QQ 邮箱将这些图发送给肖某。

国家安全机关工作人员检测发现，王某电子邮箱曾收到一封异常邮件，在点击阅读后，导致其计算机被植入一款伪装成 QQ 的特种木马程序，从而导致其计算机被境外间谍情报机关远程控制，存储的文档资料全部被窃取，其中包括多份标记密级的地形图。

因案情重大，已对我国国家安全构成严重危害，该市立即启动追责工作。有关责任人员受到相应法律惩处和党纪政纪处分。

案件三：Z 市某机关人员违规使用电子邮箱传递涉密文件资料网络窃密案

国家安全机关工作发现，Z 市某局使用的电子邮箱被境外间谍情报机关控制窃密。Z 市

地处我国边陲，边境线上驻扎着边防部队。调查发现，该单位长期将办公室电话号码作为邮箱密码使用，境外间谍情报机关利用技术手段从互联网上搜集到 Z 市某局电话号码和邮箱账号，猜解出密码并非法控制了该邮箱。

对该案调查过程中发现，邮箱中存储的大量文档资料被境外间谍情报机关窃取，被窃的文件资料中记载了 Z 市的驻军分布信息。

由于该单位违规使用互联网电子邮箱传输涉密文档资料，违反了保密安全相关规定，已构成危害国家安全的情形。有关单位对涉及此次网络窃密案件相关领导干部和多名相关工作人员进行追责、问责处理。

网络安全为人民，网络安全靠人民，维护网络安全是全社会共同责任。国家安全机关提醒社会公众，如发现危害国家安全的可疑情况，可拨打国家安全机关举报受理电话 12339，或登陆国家安全机关举报受理平台 www.12339.gov.cn 进行举报。（来源：新华社）

➢ 员工非法获取他人征信报告 1000 余份被判刑 1 年

2019 年 4 月 25 日，北京法院审判信息网公布了一份关于侵犯公民个人信息的刑事判决书。经了解，涉案人员为交银国际信托有限公司项目经理沈某相。2018 年 2 月 5 日、3 月 23 日，沈某相采用“撞库”等方式获取中国人民银行个人征信系统用户名和密码，通过中国人民银行与交银国际信托的专线互联终端机，非法登录中国人民银行个人征信系统，查询并下载保存他人征信报告共计 100 份。

沈某相于 2018 年 4 月 24 日被抓捕归案，经法院审理查明，沈某相于 2013 年-2014 年

间，采用上述同样作案手段，查询并下载保存他人征信报告共计 1000 余份。

北京市西城区人民法院认为，沈某相非法获取公民个人信息，且情节严重，构成侵犯公民个人信息罪，判处沈某相有期徒刑 1 年，并处罚金 4 千元。

另据和讯银行获悉，4 月 22 日，交银国际信托武汉分行因未经同意查询个人信息和企业的信贷信息被中国人民银行武汉分行处罚款人民币 29 万元。

据资料显示：“交银国际信托有限公司”成立于 1981 年 6 月，原名为湖北省国际信托投资公司，2007 年 5 月，经中国银监会批准，公司引进交通银行股份有限公司实施战略重组。重组完成后，公司更名为“交银国际信托有限公司”，现注册资本 57.65 亿元，交通银行股份有限公司持有 85%的股份，湖北省财政厅持有 15%的股份。（来源：和讯网）

➢ 提醒：山寨微信留“后门” 盗取语音来诈骗

2019 年 4 月 24 日新华社报道：“在吗？能不能借 500？”河南许昌一男子突然收到微信好友发来的借钱信息，还用语音说了声“是我”，听到是好友本人，该男子马上把钱转了过去。然而，该男子向对方再次核实时，朋友却直呼没有借钱，是自己的微信号被盗了。

近期，全国已发生多起类似的微信语音诈骗案件。记者调查发现，这些案件背后都有山寨微信的“身影”。一些不法软件开发者开发的山寨微信具有多种正版微信没有的功能，包括转发语音、红包秒抢、防止撤回、修改微信定位、一键克隆朋友圈等。

总是弹出广告？你手机里的微信可能是假的！

使用微信时总弹出广告，不小心就点到不知名网站？微信官方客服表示，官方微信不会弹出广告。近期，已接到不少类似反馈，经核实，这些广告并非微信官方推送，而是由于加密网络传输协议被人破解导致。简单来说，就是被安装了山寨微信。

浙江省警方曾破获一起在“老人机”（操作简便、字体较大、功能简单，便于老人使用的手机）上预装假微信软件的案件。一家名叫鹈鹕网络科技有限公司的两个合伙人和 20 多名工程师未经授权开发功能机微信软件，并将其植入“老人机”。该软件让超过 1500 万台“老人机”成为“肉鸡”，除了接收弹出式广告，账号还容易被盗取。该团队通过“后门”远程监控“老人机”状态，如果发现某账号久未使用就会将账号密码窃取，再将账号进行售卖。

目前，因这些“李鬼”软件而造成经济损失的案件已在全国多地“上演”。去年 3 月，腾讯安全联合团队配合浙江、湖南警方成功打掉国内首个集微信恶意注册、群控外挂、赌博于一身的黑产团伙，抓获了公司负责人、技术、运营者在内的 52 名犯罪嫌疑人，冻结资金 8000 多万元。

上海市闵行区去年 6 月份对某科技公司提起了公诉，原因是其制作了一批预装山寨微信手机，并以“微商手机”进行销售。微商通过该手机可以使用一台手机同时登录多个微信号，通过修改全球定位，伪装海淘假象等多种手段诱骗消费者购买产品。

记者调查：网售山寨微信已形成灰色产业链

记者调查发现，除了手机预装，目前网上还有一批兜售山寨微信及相关外挂的商家，通过层层分销代理的形式，与利益链顶端的软件开发者构成了一条灰色产业链，将山寨微信散布到网络各个角落。

记者在某网购平台发现一些销售山寨微信的店铺，软件叫价从几十元到上百元不等，不少商家都显示月销量上千。记者选择一家网店进行咨询，卖家提出要添加微信才能进一步沟通。该卖家称，购买软件的大多是微商，他们都有引流的需要，软件可以帮助他们制作 5 个分身同时登录，批量添加附近的人为好友，一键集赞等。目前该软件已经衍生到第二代，除了功能迭代之外更能保证稳定不被封号。

记者拿一款山寨微信软件进行测试，登录后发现山寨微信的好友数据和原来的一模一样，界面与正版微信几乎没有区别，只是左下角多了一个功能键，里面包含着“自动抢红包、一键转发朋友圈、自动打招呼”等 13 项正版微信没有的功能。

记者测试语音转发功能，录制“对，是我”等语音后转发给朋友，朋友听到语音后，马上信任了这是记者本人。如果有木马程序冒名操作，将会带来财产损失。而 “一键转发朋友圈”的功能，可以克隆目标好友发布的朋友圈，为生成微信假号偷梁换柱，假冒他人进行诈骗打开了方便之门。

山寨微信是违法恶意外挂，需多方合力避免蔓延

微信方面表示，山寨微信实际上是一种恶意外挂，功能虽然很多，但容易被“有心人”利用。同时，安装者本人也会因软件预留的“后门”及木马而受到信息泄露、账号被盗等威胁，具有极大安全风险。

北京市法律援助中心公职律师杨欣认为，目前来看山寨微信软件的来源大体上有两个，一个是山寨机预装，一个是消费者主动在网上购买山寨软件。对于第一种，监管部门可采取技术手段加大对山寨机的监管，减少消费者被动使用山寨软件的机会，工商行政部门也应当加大对销售山寨机商家的查处。对于第二种消费者主动购买行为，则需要销售平台配合电子商务监管部门加大监管和打击力度。

记者从微信方面了解到，微信成立了反外挂联合项目组，对使用以及售卖外挂行为的账号，根据违规程度按照阶梯性处罚原则，进行功能限制、账号封停等处罚。

“制作山寨微信的公司侵犯了正版微信所有人的软件著作权。企业应当加强对侵权者的赔偿责任追究，增加其违法成本。” 广州市南沙区知识产权发展促进会会长朱武说。

微信官方提醒：消费者要警惕手机里微信的异常情况，发现“李鬼”软件要及时投诉举报，搜索微信小程序“腾讯举报受理中心”投诉即可。同时，对于主动购买软件的消费者来说，要警惕个人信息泄露、被非法利用造成的法律风险。（来源：新华社）

信息安全意识产品免费大赠送

isa@spisec.com