国盟信息安全通报

2019 年 5 月 27 日第 193 期

国盟信息安全通报

（第 193 期）

国际信息安全学习联盟

2019 年 5 月 27 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 363 个，其中高危漏洞 111 个、中危漏洞 203 个、低危漏洞 49 个。漏洞平均分值为 5.77。本周收录的漏洞中，涉及 0day 漏洞 141 个（占 39%），其中互联网上出现“WordPress 插件 Form Maker SQL 注入漏洞、PHP-Fusion 'Edit Profile'远程代码执行漏洞”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 1672 与上周（3387 个）环比下降 51%。

主要内容

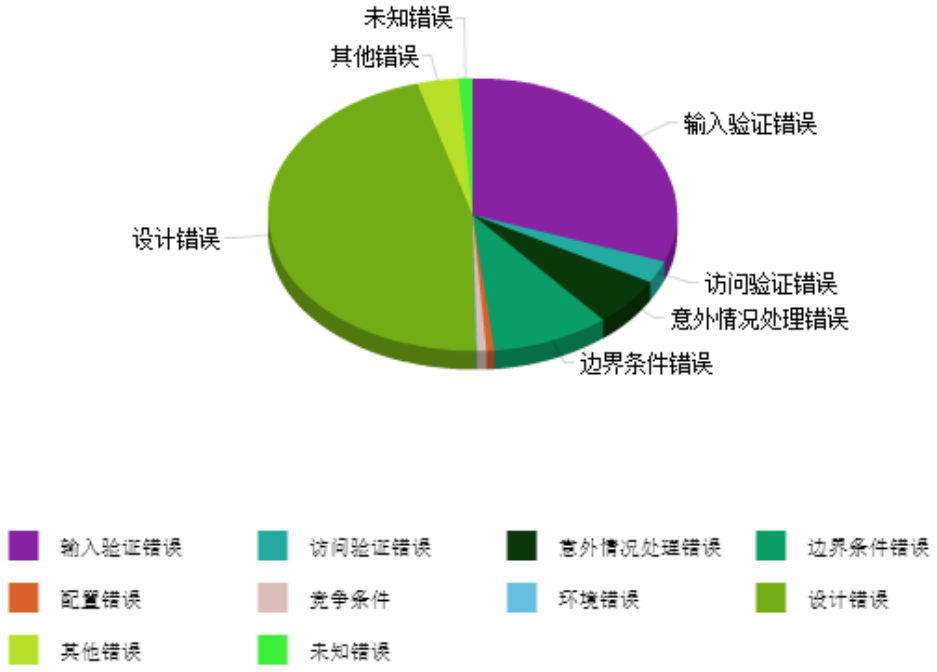
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

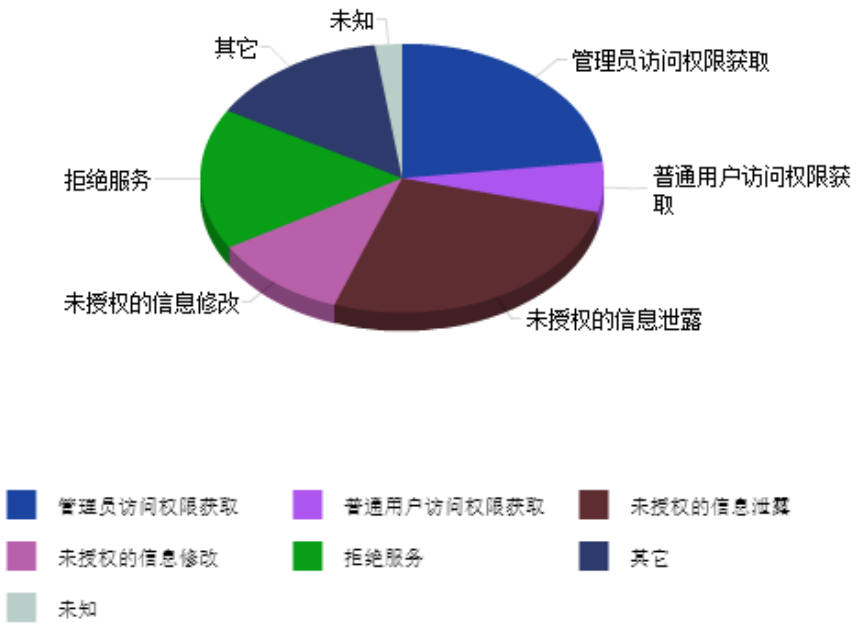
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 363 个，其中高危漏洞 111 个、中危漏洞 203 个、低危漏洞 49 个。漏洞平均分值为 5.77。本周收录的漏洞中，涉及 0day 漏洞 141 个（占 39%），其中互联网上出现“WordPress 插件 Form Maker SQL 注入漏洞、PHP-Fusion 'Edit Profile'远程代码执行漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 1672 与上周（3387 个）环比下降 51%。

二、安全漏洞增长数量及种类分布情况

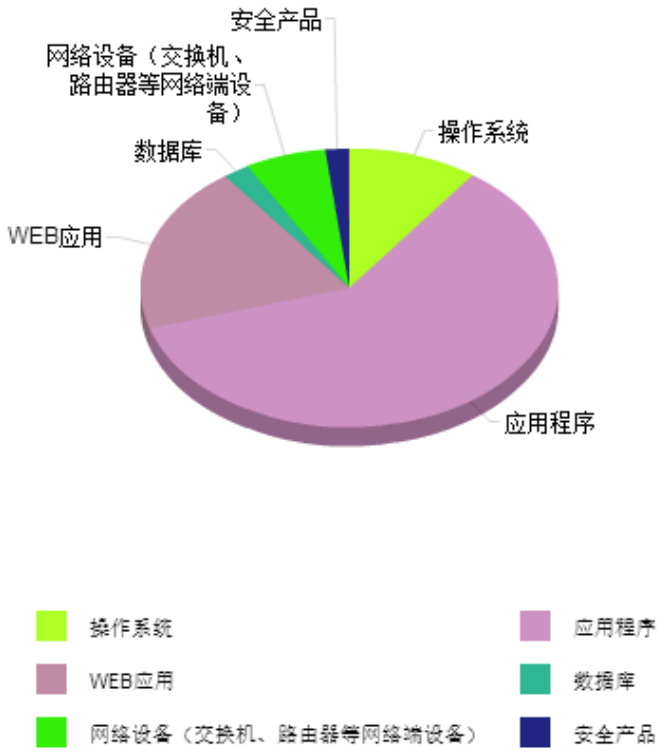
➢ 漏洞产生原因（2019 年 5 月 13 日—2019 年 5 月 27 日）



➢ 漏洞引发的威胁（2019 年 5 月 13 日—2019 年 5 月 27 日）



➢ 漏洞影响对象类型（2019 年 5 月 13 日—2019 年 5 月 27 日）



三、安全产业动态

➢ 构筑安全屏障，打牢国家网络安全的地基

没有网络安全就没有国家安全，筑牢安全屏障才能为发展保驾护航。

互联网是时代进步的加速器，但也给各行各业带来新的安全问题。党的十八大以来，以习近平同志为核心的党中央重视互联网、发展互联网、治理互联网，统筹协调涉及政治、经济、文化、社会、军事等领域信息化和网络安全重大问题，为推动我国网络安全保障体系的建立、树立正确的网络安全观指明了方向。在习近平总书记关于网络强国的重要思想的指引下，去年 3 月，中央网络安全和信息化领导小组改为中央网络安全和信息化委员会，负责这一领域重大工作的顶层设计、总体布局、统筹协调、整体推进、督促落实。一年来，从网络专项立法到网络安全制度建设，从保护用户隐私信息到加强网络安全审查，网络安全屏障日益牢固，网络安全地基不断夯实。

但同时要看到，当今社会，网络安全领域仍然面临诸多难题，网络安全形势依然复杂严峻。向内看，信息泄露、谣言传播等现象加深个人信息的安全担忧，虚假信息、不良信息影响国家社会和谐稳定；向外看，网络安全威胁和风险日益突出，并日益向政治、经济、文化、社会、生态、国防等领域传导渗透，网络安全防控能力薄弱，难以有效应对国家级、有组织的高强度网络攻击。这说明，网络安全是整体的、动态的、开放的、相对的、共同的，不是割裂的、静态的、封闭的、绝对的、孤立的。只有保持清醒头脑，树立正确的网络安全观，

防患于未然，才能切实维护网络安全。

网络安全为人民，也要靠人民。维护网络安全是全社会的共同责任，需要政府、企业、社会组织、广大网民共同参与，共筑网络安全防线。大到守护银行、电力等网络系统，小到帮助网民识别“钓鱼网站”，网络安全的战场覆盖生活工作的各个方面，网络安全意识需要贯穿始终。我们看到，过去一年，无论是严厉打击网络黑客、电信网络诈骗、侵犯公民个人隐私等违法犯罪行为，还是策划国际网络安全标准化论坛、国家网络安全宣传周，不管是上线中国互联网联合辟谣平台，还是加强预防中小学沉迷网络教育引导，网络安全知识技能宣传普及力度不断加大，广大人民群众网络安全意识和防护技能逐步提升，各方面齐抓共管的良好局面已经形成，网络安全的共治共建渐入佳境。

还要看到，互联网是人类的共同家园，让这个家园更美丽、更干净、更安全，是国际社会的共同责任。面对网络安全的共同挑战，尊重网络主权、构建网络空间命运共同体是必由之路。比如，在“一带一路”建设中，不少企业加强同沿线国家在数字经济、网络安全等方面的合作，推动建设 21 世纪数字丝绸之路。这启示我们，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。

安全是发展的前提，发展是安全的保障。时刻感知网络安全态势，做好网络风险防范，增强网络安全防御能力，我们就能让人民群众在信息化发展中有更多获得感、幸福感、安全感，推动网络安全和信息化工作再上新台阶。（来源：人民网）

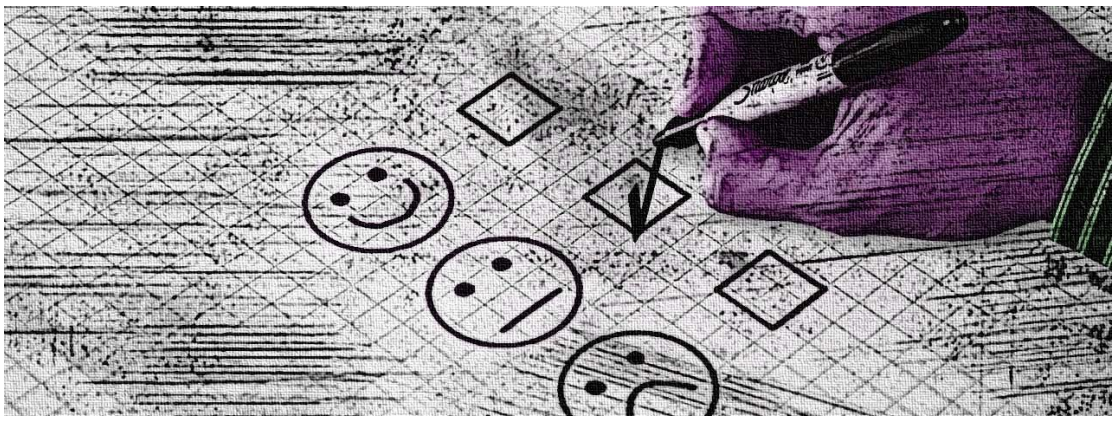
➢ 大数据时代的个人信息保护

大数据被称为未来“新石油”。据统计，截至 2018 年 12 月，我国网民规模 8.29 亿，普及率达 59.6%；网络购物用户规模 6.10 亿，年增长率为 14.4%。在大数据时代，如何实现网络服务提供者收集共享数据和个人信息保护的平衡，是一个亟待认真对待和解决的重要问题。

一、法律规制现状

构建了多层次法律体系。自 2000 年以来，我国各级国家机关陆续出台制度，规范收集使用个人信息行为。一是从立法主体来看，涵盖了全国人大及其常委会、国务院、工信部、国家质检总局、最高人民法院、最高人民检察院等，包括法律、行政法规、部门规章和司法

解释等。二是从部门法律来看，从民事、刑事、行政等领域强调了网络服务提供者义务。如《关于加强网络信息保护的决定》、消费者权益保护法、网络安全法要求收集使用公民个人电子信息时遵循合法、正当、必要原则，明示收集使用信息的目的、方式和范围。民法总则第一百一十一条规定自然人的个人信息受法律保护。侵权责任法第三十六条提出网络服务提供者利用网络侵害他人民事权益的，应承担侵权责任。刑法修正案（五）和刑法修正案（七）分别增设了窃取、收买、非法提供信用卡信息罪，出售、非法提供公民个人信息罪、非法获取公民个人信息罪。



强调知情同意。《关于加强网络信息保护的决定》首次强调了对个人信息的法律保护，要求网络服务提供者收集、使用个人信息应征得被收集人同意。这在消费者权益保护法、《征信业管理条例》和网络安全法中得到了坚持。在比较法上，经济合作与发展组织《金融消费者保护的高级原则》（2011 年）要求成员国建立机制确保消费者个人隐私安全，承认消费者的知情权。欧盟 2018 年《通用数据保护条例》将数据主体同意基于一项或多项目的对其个人数据进行处理作为合法性要件之一。

兼顾数据收集共享与个人信息保护。不少国家区分敏感和一般信息，禁止收集、处理和利用敏感信息，支持一般信息的合法流动。我国《征信业管理条例》第十四条将宗教信仰、基因、指纹、血型、疾病和病史信息作为禁止收集的个人敏感信息。德国 2002 年《联邦个人资料保护法》规定了种族血统、政治观点、宗教或哲学信仰、工会成员资格、健康或性生活等敏感信息。欧盟 2016 年《数据保护法规》列举了种族、民族出身、政治观点、宗教或哲学信仰、工会成员、基因等敏感信息。此外，欧盟 2015 年《金融服务监管中的数据保护指引》强调数据保护规则旨在实现信息在欧盟内部的自由流动，对个人权益进行保护。欧盟《通用数据保护条例》建立了个人信息的风险评估、数据保护认证（自愿将数据内容进行专业认证以表明处理合法性）、信息安全保障（采取匿名化方式或数据最小化原则减少数据泄露风险）。

二、我国数据共享与个人信息保护存在的问题

立法的统筹性和明确性有待提升。一是个人信息保护法律规范较零散，缺乏专门立法统一引领。二是民法总则第一百一十一条将“个人信息”作为法益，并未上升为个人信息权，造成了个人信息权利的归属、内容、个人可否支配等困惑。三是相近概念未明确区分。如民法总则规定了个人信息和隐私权，但两者的区分却未明确，影响了网络服务提供者收集共享数据的效率和个人法律救济。四是可穿戴设备、无人驾驶等数据共享新形式，在收集共享数据时难以及时征得个人同意，相关法律规范需予以明确。

法律规范可操作性有待加强。一是我国未从整体角度实现个人信息的类型划分，未建立不同类型信息的差异化保护规则，容易增加收集共享成本。二是现行立法采取知情同意，由于个人较之网络服务提供者属于“弱者”，面对授权条款时只能“接受或离开”，但立法对授权的具体方式、授权条款、授权范围和授权例外等未做明确，易生纠纷。三是特殊群体法律规则缺乏。纵观个人信息泄露致害、电信诈骗等案例，未成年人和老年人对信息收集共享的判断能力较弱，目前立法未建立特殊保护机制。

互联网企业的内部控制和风险管理机制有待加强。现阶段互联网技术缺陷、企业内部管理疏忽导致的“监守自盗”，是个人信息泄露的重要原因，互联网企业的内控和风险管理机制需完善。

三、大数据时代加强个人信息保护的建议

未来已来。在大数据时代，为强化优化个人信息保护，笔者提出如下建议：

制定统一规则。一是在评估各类现行规范及其效果基础上，制定个人信息保护统一规则，统筹规范各类信息收集共享行为。二是将个人信息升格为法定权利，明确个人信息权的内容，包括知情同意权、信息查阅权、信息安全维护权、信息更正权、信息删除权等。三是明确信息收集共享基本原则，包括合法、合理、最小化使用和利益平衡原则。一方面，网络服务提供者应严格控制收集范围，考量自身业务范围、需求、是否属于个人核心信息、是否已技术处理等因素，杜绝过度收集。另一方面，个人信息不应由个人排他享有。个人数据作为网络二进制基础上由 0 和 1 组成的比特形式，数据收集包含了网络服务提供者的劳动，正是海量数据而非单个信息使其产生经济价值，个人亦是个人数据的受益者，应鼓励合法收集和共享。

建立差异化保护机制。一是在类型划分方面，应根据个人信息和隐私、人格尊严的关联程度，区分敏感信息和非敏感信息，对于前者严格保护，对于后者支持便捷利用。个人敏感信息主要包括身份证号码、手机号码、种族、政治观点、宗教信仰、基因、指纹、性取向、性生活、银行账号密码、财产情况、病史等。二是在合理注意义务方面，应分析不同场景中

的信息处理行为能否为当事人合理预见，建立敏感、非敏感信息与合理注意义务之间的对应关系。对于敏感信息，个人对信息收集共享的容忍程度更低，网络服务提供商则应承担更高注意义务。三是在信息主体方面，研究制定收集共享特殊主体信息的保护规则。未成年人对信息收集共享缺乏独立判断能力，老年人对大数据收集运用场景缺乏足够了解，两类群体均易因信息泄露受骗致害。因此，建议收集共享未成年人所有信息均需经其法定监护人明示同意，收集共享 70 岁以上老年人敏感信息需经老年人及其赡养义务人明示同意，且共享未成年人和老年人上述信息须采取匿名化或加密处理，降低信息泄露风险。

完善授权同意规则。一是授权方式。尽管不同立法例对授权同意为明示或默示同意不尽相同，笔者认为，网络服务提供者收集共享个人敏感信息时应明示同意，彰显信息保护；收集共享个人非敏感信息时可采取默示同意，突出数据共享便捷。二是授权条款。应规范授权条款，如通过字体变化或字号加粗提示关注、行业组织提供条款模板，要求起草者充分解释等。三是授权范围。个人信息的收集共享均应得到授权，授权范围的表述应明确易懂。四是授权例外。基于国家利益、社会公共利益和个人紧急情况（如出行平台驾乘人员出现生命安全隐患时提供相关个人信息），明确无需个人同意即可收集信息的情形。

研究采取配套措施。一是加强企业内部控制和风险管理，细化信息收集共享风险评估，强化内部人员管理，完善数据加密和匿名化等网络安全技术。二是完善集团公司与下属子公司、子公司之间的信息共享机制，网络服务提供者应在授权同意环节明确信息共享的情形与范围，并采取技术保护措施。三是开发个人信息安全保险产品，由保险公司分担个人信息泄露所致财产损失，支持互联网产业发展。四是加强培训教育，增强个人及相关从业人员的信息安全意识。（来源：人民法院报，作者：刘曼，作者单位：人民法院新闻传媒总社）

➢ 《网络安全等级保护基本要求》GB/T22239-2019 标准解读

《信息安全技术信息系统安全等级保护基本要求》（GB/T 22239-2008）在我国推行信息安全等级保护制度的过程中起到了非常重要的作用，被广泛用于各行业或领域，指导用户开展信息系统安全等级保护的建设整改、等级测评等工作。随着信息技术的发展，已有 10 年历史的《GB/T 22239-2008》在时效性、易用性、可操作性上需要进一步完善。2017 年《中华人民共和国网络安全法》实施，为了配合国家落实网络安全等级保护制度，也需要修订《GB/T 22239-2008》。

2014 年，全国信息安全标准化技术委员会（以下简称安标委）下达了对《GB/T 22239-2008》进行修订的任务。标准修订主要承担单位为公安部第三研究所（公安部信息安全等级保护评估中心），20 多家企事业单位派人员参与了标准的修订工作。标准编制组于 2014 年成立，先后调研了国际和国内云计算平台、大数据应用、移动互联接入、物联网和工业控制系统等新技术、新应用的使用情况，分析并总结了新技术和新应用中的安全关注点和安全控制要素，完成了基本要求草案第一稿。

2015 年 2 月至 2016 年 7 月，标准编制组在草案第一稿的基础上，广泛征求行业用户单位、安全服务机构和各行业/领域专家的意见，并按照意见调整和完善标准草案，先后共形成 7 个版本的标准草案。2016 年 9 月，标准编制组参加了安标委 WG5 工作组在研标准推进会，按照专家及成员单位提出的修改建议，对草案进行了修改，形成了标准征求意见稿。2017 年 4 月，标准编制组再次参加了安标委 WG5 工作组在研标准推进会，根据征求意见稿收集的修改建议，对征求意见稿进行了修改，形成了标准送审稿。2017 年 10 月，标准编制组又一次参加了安标委 WG5 工作组在研标准推进会，在会上介绍了送审稿内容，并征求成员单位意见，根据收集的修改建议，对送审稿进行了修改完善，形成了标准报批稿。

2019 年《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）将正式实施。本文分析《GB/T 22239-2019》相较《GB/T 22239-2008》发生的主要变化，解读其安全通用要求和安全扩展要求的主要内容，以便于读者更好地了解和掌握《GB/T 22239-2019》的内容。

1、总体结构的变化

1.1 主要变化内容

《GB/T 22239-2019》相较于《GB/T 22239-2008》，无论是在总体结构方面还是在细节内容方面均发生了变化。**在总体结构方面的主要变化为：**

1）为适应网络安全法，配合落实网络安全等级保护制度，标准的名称由原来的《信息系统安全等级保护基本要求》改为《网络安全等级保护基本要求》。

2）等级保护对象由原来的信息系统调整为基础信息网络、信息系统（含采用移动互联技术的系统）、云计算平台/系统、大数据应用/平台/资源、物联网和工业控制系统等。

3）将原来各个级别的安全要求分为安全通用要求和安全扩展要求，安全扩展要求包括云计算安全扩展要求、移动互联安全扩展要求、物联网安全扩展要求以及工业控制系统安全扩展要求。安全通用要求是不管等级保护对象形态如何必须满足的要求；针对云计算、移动互联、物联网和工业控制系统提出的特殊要求称为安全扩展要求。

4）原来基本要求中各级技术要求的“ 物理安全” 、“ 网络安全” 、“ 主机安全” 、“ 应用安全” 和“ 数据安全和备份与恢复” 修订为“ 安全物理环境” 、“ 安全通信网络” 、“ 安全区域边界” 、“ 安全计算环境” 和“ 安全管理中心” ；原各级管理要求的“ 安全管理制度” 、“ 安全管理机构” 、“ 人员安全管理” 、“ 系统建设管理” 和“ 系统运维管理” 修订为“ 安全管理制度” 、“ 安全管理机构” 、“ 安全管理人员” 、“ 安全建设管理” 和“ 安全运维管理”。

5）云计算安全扩展要求针对云计算环境的特点提出。主要内容包括“ 基础设施的位置” 、“ 虚拟化安全保护” 、“ 镜像和快照保护” 、“ 云计算环境管理” 和“ 云服务商选择” 等。

6）移动互联安全扩展要求针对移动互联的特点提出。主要内容包括“ 无线接入点的物理位置” 、“ 移动终端管控” 、“ 移动应用管控” 、“ 移动应用软件采购” 和“ 移动应用软件开发” 等。

7）物联网安全扩展要求针对物联网的特点提出。主要内容包括“ 感知节点的物理防护” 、“ 感知节点设备安全” 、“ 网关节点设备安全” 、“ 感知节点的管理” 和“ 数据融合处理” 等。

8）工业控制系统安全扩展要求针对工业控制系统的特点提出。主要内容包括“ 室外控制设备防护” 、“ 工业控制系统网络架构安全” 、“ 拨号使用控制” 、“ 无线使用控制” 和“ 控制设备安全” 等。

9）取消了原来安全控制点的 S、A、G 标注，增加附录 A“ 关于安全通用要求和安全扩展要求的选择和使用”，描述等级保护对象的定级结果和安全要求之间的关系，说明如何根

据定级的 S、A 结果选择安全要求的相关条款，简化了标准正文部分的内容。

10）增加附录 C 描述等级保护安全框架和关键技术、附录 D 描述云计算应用场景、附录 E 描述移动互联应用场景、附录 F 描述物联网应用场景、附录 G 描述工业控制系统应用场景、附录 H 描述大数据应用场景。

1.2 变化的意义和作用

《GB/T 22239-2019》采用安全通用要求和安全扩展要求的划分使得标准的使用更加具有灵活性和针对性。不同等级保护对象由于采用的信息技术不同，所采用的保护措施也会不同。例如，传统的信息系统和云计算平台的保护措施有差异，云计算平台和工业控制系统的保护措施也有差异。为了体现不同对象的保护差异，《GB/T 22239-2019》将安全要求划分为安全通用要求和安全扩展要求。

安全通用要求针对共性化保护需求提出，无论等级保护对象以何种形式出现，需要根据安全保护等级实现相应级别的安全通用要求。安全扩展要求针对个性化保护需求提出，等级保护对象需要根据安全保护等级、使用的特定技术或特定的应用场景实现安全扩展要求。等级保护对象的安全保护措施需要同时实现安全通用要求和安全扩展要求，从而更加有效地保护等级保护对象。例如，传统的信息系统可能只需要采用安全通用要求提出的保护措施即可，而云计算平台不仅需要采用安全通用要求提出的保护措施，还要针对云计算平台的技术特点采用云计算安全扩展要求提出的保护措施；工业控制系统不仅需要采用安全通用要求提出的保护措施，还要针对工业控制系统的技术特点采用工业控制系统安全扩展要求提出的保护措施。

2、安全通用要求的内容

2.1 安全通用要求基本分类

《GB/T 22239-2019》规定了第一级到第四级等级保护对象的安全要求，每个级别的安全要求均由安全通用要求和安全扩展要求构成。例如，《GB/T 22239-2019》提出的第三级安全要求基本结构为：

8、第三级安全要求

8.1 安全通用要求

8.2 云计算安全扩展要求

8.3 移动互联安全扩展要求

8.4 物联网安全扩展要求

8.5 工业控制系统安全扩展要求

安全通用要求细分为技术要求和管理要求。其中技术要求包括“ 安全物理环境”、“ 安全通信网络”、“ 安全区域边界”、“ 安全计算环境” 和“ 安全管理中心”；管理要求包括“ 安全管理制度”、“ 安全管理机构”、“ 安全管理人员”、“ 安全建设管理” 和“ 安全运维管理” 。两者合计 10 大类，**如图 1 所示**。

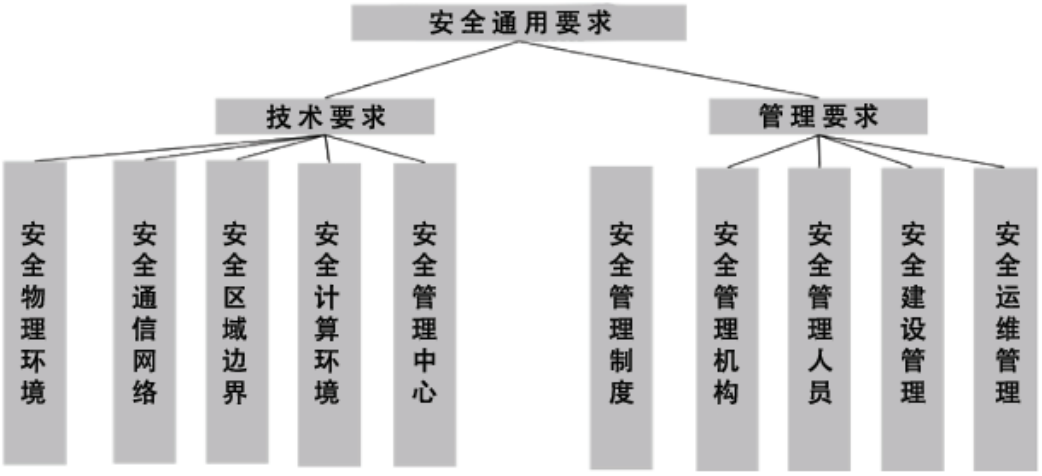


图 1：安全通用要求基本分类

2.2 技术要求

技术要求分类体现了从外部到内部的纵深防御思想。对等级保护对象的安全防护应考虑从通信网络到区域边界再到计算环境的从外到内的整体防护，同时考虑对其所处的物理环境的安全防护。对级别较高的等级保护对象还需要考虑对分布在整个系统中的安全功能或安全组件的集中技术管理手段。

1）安全物理环境

安全通用要求中的安全物理环境部分是针对物理机房提出的安全控制要求。主要对象为物理环境、物理设备和物理设施等；涉及的安全控制点包括物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护。

表 1 给出了安全物理环境控制点/要求项的逐级变化。

其中数字表示每个控制点下各个级别的要求项数量，级别越高，要求项越多。后续表中的数字均为此含义。

序号	控制点	一级	二级	三级	四级
1	物理位置的选择	0	2	2	2
2	物理访问控制	1	1	1	2
3	防盗窃和防破坏	1	2	3	3
4	防雷击	1	1	2	2
5	防火	1	2	3	3
6	防水和防潮	1	2	3	3
7	防静电	0	1	2	2
8	温湿度控制	1	1	1	1
9	电力供应	1	2	3	4
10	电磁防护	0	1	2	2

表 1 安全物理环境控制点/要求项的逐级变化

承载高级别系统的机房相对承载低级别系统的机房强化了物理访问控制、电力供应和电磁防护等方面的要求。例如，四级相比三级增设了“ 重要区域应配置第二道电子门禁系统”、“ 应提供应急供电设施” 、“ 应对关键区域实施电磁屏蔽” 等要求。

2）安全通信网络

安全通用要求中的安全通信网络部分是针对通信网络提出的安全控制要求。主要对象为广域网、城域网和局域网等；涉及的安全控制点包括网络架构、通信传输和可信验证。**表 2 给出了安全通信网络控制点/要求项的逐级变化。**

序号	控制点	一级	二级	三级	四级
1	网络架构	0	2	5	6
2	通信传输	1	1	2	4
3	可信验证	1	1	1	1

表 2 安全通信网络控制点/要求项的逐级变化

高级别系统的通信网络相对低级别系统的通信网络强化了优先带宽分配、设备接入认证、通信设备认证等方面的要求。例如，四级相比三级增设了“ 应可按照业务服务的重要程度分配带宽，优先保障重要业务” ，“ 应采用可信验证机制对接入网络中的设备进行可信验证，保证接入网络的设备真实可信” ，“ 应在通信前基于密码技术对通信双方进行验证或认证” 等要求。

3）安全区域边界

安全通用要求中的安全区域边界部分是针对网络边界提出的安全控制要求。主要对象为系统边界和区域边界等；涉及的安全控制点包括边界防护、访问控制、入侵防范、恶意代码防范、安全审计和可信验证。**表 3 给出了安全区域边界控制点/要求项的逐级变化。**

序号	控制点	一级	二级	三级	四级
1	边界防护	1	1	4	6
2	访问控制	3	4	5	5
3	入侵防范	0	1	4	4
4	恶意代码防范	0	1	2	2
5	安全审计	0	3	4	3
6	可信验证	1	1	1	1

表 3 安全区域边界控制点/要求项的逐级变化

高级别系统的网络边界相对低级别系统的网络边界强化了高强度隔离和非法接入阻断等方面的要求。例如，四级相比三级增设了“ 应在网络边界通过通信协议转换或通信协议隔离等方式进行数据交换”，“ 应能够在发现非授权设备私自联到内部网络的行为或内部用户非授权联到外部网络的行为时，对其进行有效阻断” 等要求。

4）安全计算环境

安全通用要求中的安全计算环境部分是针对边界内部提出的安全控制要求。主要对象为边界内部的所有对象，包括网络设备、安全设备、服务器设备、终端设备、应用系统、数据对象和其他设备等；涉及的安全控制点包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份与恢复、剩余信息保护和个人信息保护。**表 4 给出了安全计算环境控制点/要求项的逐级变化。**

序号	控制点	一级	二级	三级	四级
1	身份鉴别	2	3	4	4
2	访问控制	3	4	7	7
3	安全审计	0	3	4	4
4	入侵防范	2	5	6	6
5	恶意代码防范	1	1	1	1
6	可信验证	1	1	1	1
7	数据完整性	1	1	2	3
8	数据保密性	0	0	2	2
9	数据备份与恢复	1	2	3	4
10	剩余信息保护	0	1	2	2
11	个人信息保护	0	2	2	2

表 4 安全计算环境控制点/要求项的逐级变化

高级别系统的计算环境相对低级别系统的计算环境强化了身份鉴别、访问控制和程序完整性等方面的要求。例如，四级相比三级增设了“ 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现”，“ 应对主体、客体设置安全标记，并依据安全标记和强制访问控制规则确定

主体对客体的访问”，“ 应采用主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断” 等要求。

5）安全管理中心

安全通用要求中的安全管理中心部分是针对整个系统提出的安全管理方面的技术控制要求，通过技术手段实现集中管理。涉及的安全控制点包括系统管理、审计管理、安全管理和集中管控。**表 5 给出了安全管理中心控制点/要求项的逐级变化。**

序号	控制点	一级	二级	三级	四级
1	系统管理	2	2	2	2
2	审计管理	2	2	2	2
3	安全管理	0	2	2	2
4	集中管控	0	0	6	7

表 5 安全管理中心控制点/要求项的逐级变化

高级别系统的安全管理相对低级别系统的安全管理强化了采用技术手段进行集中管控等方面的要求。例如，三级相比二级增设了“ 应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控”，“ 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测”，“ 应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求”，“ 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理” 等要求。

2.3 管理要求

管理要求分类体现了从要素到活动的综合管理思想。安全管理需要的“ 机构”、“ 制度” 和“ 人员” 三要素缺一不可，同时还应对系统建设整改过程中和运行维护过程中的重要活动实施控制和管理。对级别较高的等级保护对象需要构建完备的安全管理体系。

1）安全管理制度

安全通用要求中的安全管理制度部分是针对整个管理制度体系提出的安全控制要求，涉及的安全控制点包括安全策略、管理制度、制定和发布以及评审和修订。**表 6 给出了安全管理制度控制点/要求项的逐级变化。**

序号	控制点	一级	二级	三级	四级
1	安全策略	0	1	1	1
2	管理制度	1	2	3	3
3	制定和发布	0	2	2	2
4	评审和修订	0	1	1	1

表 6 安全管理制度控制点/要求项的逐级变化

2）安全管理机构

安全通用要求中的安全管理机构部分是针对整个管理组织架构提出的安全控制要求，涉及的安全控制点包括岗位设置、人员配备、授权和审批、沟通和合作以及审核和检查。**表 7 给出了安全管理机构控制点/要求项的逐级变化。**

序号	控制点	一级	二级	三级	四级
1	岗位设置	1	2	3	3
2	人员配备	1	1	2	3
3	授权和审批	1	2	3	3
4	沟通和合作	0	3	3	3
5	审核和检查	0	1	3	3

表 7 安全管理机构控制点/要求项的逐级变化

3）安全管理人员

安全通用要求中的安全管理人员部分是针对人员管理模式提出的安全控制要求，涉及的安全控制点包括人员录用、人员离岗、安全意识教育和培训以及外部人员访问管理。**表 8 给出了安全管理人员控制点/要求项的逐级变化。**

序号	控制点	一级	二级	三级	四级
1	人员录用	1	2	3	4
2	人员离岗	1	1	2	2
3	安全意识教育和培训	1	1	3	3
4	外部人员访问管理	1	3	4	5

表 8 安全管理人员控制点/要求项的逐级变化

4）安全建设管理

安全通用要求中的安全建设管理部分是针对安全建设过程提出的安全控制要求，涉及的安全控制点包括定级和备案、安全方案设计、安全产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评和服务供应商管理。**表 9 给出了安全建设管理控制点/要求项的逐级变化。**

序号	控制点	一级	二级	三级	四级
1	定级和备案	1	4	4	4
2	安全方案设计	1	3	3	3
3	安全产品采购和使用	1	2	3	4
4	自行软件开发	0	2	7	7
5	外包软件开发	0	2	3	3
6	工程实施	1	2	3	3
7	测试验收	1	2	2	2
8	系统交付	2	3	3	3
9	等级测评	0	3	3	3
10	服务供应商管理	2	2	3	3

表 9 安全建设管理控制点/要求项的逐级变化

5）安全运维管理

安全通用要求中的安全运维管理部分是针对安全运维过程提出的安全控制要求，涉及的安全控制点包括环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理和外包运维管理。**表 10 给出了安全运维管理控制点/要求项的逐级变化。**

序号	控制点	一级	二级	三级	四级
1	环境管理	2	3	3	4
2	资产管理	0	1	3	3
3	介质管理	1	2	2	2
4	设备维护管理	1	2	4	4
5	漏洞和风险管理	1	1	2	2
6	网络和系统安全管理	2	5	10	10
7	恶意代码防范管理	2	3	2	2
8	配置管理	0	1	2	2
9	密码管理	0	2	2	3
10	变更管理	0	1	3	3
11	备份与恢复管理	2	3	3	3
12	安全事件处置	2	3	4	5
13	应急预案管理	0	2	4	5
14	外包运维管理	0	2	4	4

表 10 安全运维管理控制点/要求项的逐级变化

3、安全扩展要求的内容

安全扩展要求是采用特定技术或特定应用场景下的等级保护对象需要增加实现的安全要求。《GB/T 22239-2019》提出的安全扩展要求包括云计算安全扩展要求、移动互联安全扩展要求、物联网安全扩展要求和工业控制系统安全扩展要求。

3.1 云计算安全扩展要求

采用了云计算技术的信息系统通常称为云计算平台。云计算平台由设施、硬件、资源抽象控制层、虚拟化计算资源、软件平台和应用软件等组成。云计算平台中通常有云服务商和云服务客户/云租户两种角色。根据云服务商所提供服务的类型，云计算平台有软件即服务（SaaS）、平台即服务（PaaS）、基础设施即服务（IaaS）3 种基本的云计算服务模式。在不同的服务模式中，云服务商和云服务客户对资源拥有不同的控制范围，控制范围决定了安全责任的边界。

云计算安全扩展要求是针对云计算平台提出的安全通用要求之外额外需要实现的安全要求。云计算安全扩展要求涉及的控制点包括基础设施位置、网络架构、网络边界的访问控制、网络边界的入侵防范、网络边界的安全审计、集中管控、计算环境的身份鉴别、计算环境的访问控制、计算环境的入侵防范、镜像和快照保护、数据安全性、数据备份恢复、剩余信息保护、云服务商选择、供应链管理和云计算环境管理。**表 11 给出了云计算安全扩展要求控制点/要求项的逐级变化。**

序号	控制点	一级	二级	三级	四级
1	基础设施位置	1	1	1	1
2	网络架构	2	3	5	8
3	网络边界的访问控制	1	2	2	2
4	网络边界的入侵防范	0	3	4	4
5	网络边界的安全审计	0	2	2	2
6	集中管控	0	0	4	4
7	计算环境的身份鉴别	0	0	1	1
8	计算环境的访问控制	2	2	2	2
9	计算环境的入侵防范	0	0	3	3
10	镜像和快照保护	0	2	3	3
11	数据安全性	1	3	4	4
12	数据备份恢复	0	2	4	4
13	剩余信息保护	0	2	2	2
14	云服务商选择	3	4	5	5
15	供应链管理	1	2	3	3
16	云计算环境管理	0	1	1	1

表 11 云计算安全扩展要求控制点/要求项的逐级变化

3.2 移动互联安全扩展要求

采用移动互联技术的等级保护对象，其移动互联部分通常由移动终端、移动应用和无线网络 3 部分组成。移动终端通过无线通道连接无线接入设备接入有线网络；无线接入网关通

过访问控制策略限制移动终端的访问行为；后台的移动终端管理系统（如果配置）负责对移动终端的管理，包括向客户端软件发送移动设备管理、移动应用管理和移动内容管理策略等。

移动互联安全扩展要求是针对移动终端、移动应用和无线网络提出的特殊安全要求，它们与安全通用要求一起构成针对采用移动互联技术的等级保护对象的完整安全要求。移动互联安全扩展要求涉及的控制点包括无线接入点的物理位置、无线和有线网络之间的边界防护、无线和有线网络之间的访问控制、无线和有线网络之间的入侵防范，移动终端管控、移动应用管控、移动应用软件采购、移动应用软件开发和配置管理。**表 12 给出了移动互联安全扩展要求控制点/要求项的逐级变化。**

序号	控制点	一级	二级	三级	四级
1	无线接入点的物理位置	1	1	1	1
2	无线和有线网络之间的边界防护	1	1	1	1
3	无线和有线网络之间的访问控制	1	1	1	1
4	无线和有线网络之间的入侵防范	0	5	6	6
5	移动终端管控	0	0	2	3
6	移动应用管控	1	2	3	4
7	移动应用软件采购	1	2	2	2
8	移动应用软件开发	0	2	2	2
9	配置管理	0	0	1	1

表 12 移动互联安全扩展要求控制点/要求项的逐级变化

3.3 物联网安全扩展要求

物联网从架构上通常可分为 3 个逻辑层，即感知层、网络传输层和处理应用层。其中感知层包括传感器节点和传感网网关节点或 RFID 标签和 RFID 读写器，也包括感知设备与传感网网关之间、RFID 标签与 RFID 读写器之间的短距离通信（通常为无线）部分；网络传输层包括将感知数据远距离传输到处理中心的网络，如互联网、移动网或几种不同网络的融合；处理应用层包括对感知数据进行存储与智能处理的平台，并对业务应用终端提供服务。对大型物联网来说，处理应用层一般由云计算平台和业务应用终端构成。

对物联网的安全防护应包括感知层、网络传输层和处理应用层。由于网络传输层和处理应用层通常由计算机设备构成，因此这两部分按照安全通用要求提出的要求进行保护。物联网安全扩展要求是针对感知层提出的特殊安全要求，它们与安全通用要求一起构成针对物联网的完整安全要求。

物联网安全扩展要求涉及的控制点包括感知节点的物理防护、感知网的入侵防范、感知网的接入控制、感知节点设备安全、网关节点设备安全、抗数据重放、数据融合处理和感知

节点的管理。**表 13 给出了物联网安全扩展要求控制点/要求项的逐级变化。**

序号	控制点	一级	二级	三级	四级
1	感知节点的物理防护	2	2	4	4
2	感知网的入侵防范	0	2	2	2
3	感知网的接入控制	1	1	1	1
4	感知节点设备安全	0	0	3	3
5	网关节点设备安全	0	0	4	4
6	抗数据重放	0	0	2	2
7	数据融合处理	0	0	1	2
8	感知节点的管理	1	2	3	3

表 13 物联网安全扩展要求控制点/要求项的逐级变化

3.4 工业控制系统安全扩展要求

工业控制系统通常是可用性要求较高的等级保护对象。工业控制系统是各种控制系统的总称，典型的如数据采集与监视控制系统（SCADA）、集散控制系统（DCS）等。工业控制系统通常用于电力，水和污水处理，石油和天然气，化工，交通运输，制药，纸浆和造纸，食品和饮料以及离散制造（如汽车、航空航天和耐用品）等行业。

工业控制系统从上到下一般分为 5 个层级，依次为企业资源层、生产管理层、过程监控层、现场控制层和现场设备层，不同层级的实时性要求有所不同，对工业控制系统的安全防护应包括各个层级。由于企业资源层、生产管理层和过程监控层通常由计算机设备构成，因此这些层级按照安全通用要求提出的要求进行保护。

工业控制系统安全扩展要求是针对现场控制层和现场设备层提出的特殊安全要求，它们与安全通用要求一起构成针对工业控制系统的完整安全要求。工业控制系统安全扩展要求涉及的控制点包括室外控制设备防护、网络架构、通信传输、访问控制、拨号使用控制、无线使用控制、控制设备安全、产品采购和使用以及外包软件开发。**表 14 给出了工业控制系统安全扩展要求控制点/要求项的逐级变化。**

序号	控制点	一级	二级	三级	四级
1	室外控制设备防护	2	2	2	2
2	网络架构	2	3	3	3
3	通信传输	0	1	1	1
4	访问控制	1	2	2	2
5	拨号使用控制	0	1	2	3
6	无线使用控制	2	2	4	4
7	控制设备安全	2	2	5	5
8	产品采购和使用	0	1	1	1
9	外包软件开发	0	1	1	1

表 14 工业控制系统安全扩展要求控制点/要求项的逐级变化

4、结束语

《GB/T 22239-2019》在结构上和内容上相较于《GB/T 22239-2008》均发生了较大变化，这些变化给网络安全等级保护的建设整改、等级测评等工作均带来了一定的影响。如何基于新标准形成安全解决方案，如何基于新标准开展等级保护测评等，都需要仔细研读新标准，基于新标准找到开展网络安全等级保护工作的新思路和新方法。（来源：公安部信息安全等级保护评估中心　作者：马力，祝国邦，陆磊）

➢ 高素质网络空间安全人才特点及培养规律分析

引言：习近平总书记指出“网络空间的竞争，归根结底是人才竞争”。保障网络安全，维护网络空间主权、国家安全和社会公共利益，乃至建设网络强国，最根本的还是要有一支强大的网络安全人才队伍。

只有持续提高人才培养质量，才能涌现出更多的高素质人才。高素质网络安全人才作为网络安全队伍的领军人，是维护国家网络空间安全的核心力量，如何摸清高素质网络空间安全人才特点，把握其培育规律，建立有针对性的体系化人才培养机制，完善人才培养配套措施，从而打造素质过硬、战斗力强的人才队伍，已成为政府相关部门和院校的当务之急。

一、我国网络空间安全人才培养形势

党的十八大特别是中央网络安全和信息化领导小组成立以来，在国家政策引导和社会需求牵引下，我国网络安全人才培养工作明显加强，成效显著。但总的看来，网络安全人才培养与日趋严峻的网络安全形势仍不相适应，难以满足国家网络安全需求。

（一）网络空间安全专业人才缺口较大

高等院校是网络安全人才培养的主阵地。据不完全统计，在本科阶段，我国开设计算机专业的高校已经超过 1100 所，开设网络工程专业的接近 200 所。但网络安全专业每年培养的本科生和研究生人数不到 1 万人，大专毕业生人数约 2 万人，在校生约 0.7 万人。赛迪顾问预测，近 5 年我国网络安全行业每年还需增加约 2 万人，与每年 1 万人的本科以上毕业生相比，网络安全专业人才的缺口十分巨大。据教育部有关机构和专家预测，当前我国网络安全人才缺口达 70 万，到 2020 年将急剧增加到 140 万。

2016 年 4 月 19 日，习近平总书记主持召开网络安全和信息化工作座谈会并在讲话中对网信人才问题作出重要指示。

习近平总书记 4 •19 讲话中对网络安全和信息化人才问题做了重要论述。“要下大功夫、下大本钱，请优秀的老师，编优秀的教材，招优秀的学生，建一流的网络空间安全学院”。2015 年 6 月，网络空间安全被国务院学位委员会、教育部正式批准列为一级学科。2015 年 12 月，经学位办批准，我国 29 所高校设立网络空间安全一级学科博士点。2017 年 8 月，中央网信办、教育部印发的《一流网络安全学院建设示范项目管理办法》指出，我国在 2017 年-2027 年期间实施一流网络安全学院建设示范项目，形成 4-6 所世界一流的网络安全学院。首批共有 7 所高校入围一流网络安全学院建设示范项目。网络安全一级学科设立后，显著推动了高校网络安全学科专业和院系建设工作，多家高校整合资源新设了网络安全院系，加大了资源投入，扩大了招生规模。

（二）网络空间安全人才培养质量不容乐观

与网络安全人才缺口较大的问题相比，网络安全人才培养质量问题更亟待解决。从实际来看，目前一些高校人才培养效果难以满足网络安全实战需求。一方面由于我国网络安全教育起步较晚，高校网络安全实践型人才储备不足，缺乏精通尖端网络安全技术的专业教师队伍，师资力量亟待加强。另一方面，高校普遍缺乏网络安全实践场景，导致学生普遍理论功底强，实战能力弱，毕业后很难满足用人单位的要求。

2015 年，中央网信办等部门指导四川大学、西安电子科技大学、北京邮电大学、上海交通大学、解放军信息工程大学等高校开展网络安全人才培养基地建设，从而创新网络安全人

才培养模式，形成可复制、可推广的网络空间安全人才培养经验。5 所高校在教学方法改革、教材体系建设、企业教师队伍建设、实习基地建设、教师培训、网络安全竞赛等多个方面进行创新和探索。例如：四川大学与以色列多所大学签订合作协议，启动了网络安全本科生、研究生联合培养方案的协商和实施计划。武汉市积极响应中央关于创建一流网络安全学院的号召，创建国家网络安全人才与创新基地，与奇虎 360、武汉大学、易华录等单位就基地建设签订了一系列合作协议，充分调动社会资源，促进高校和行业企业、科研院所协同育人，提高网络安全人才培养质量。

（三）网络空间安全职业培训体系不完善

网络空间安全形势变化多端，从业人员需及时更新知识储备，持续提升安全技能。总体上看，我国网络安全职业培训体系还不完善，没有建立常态化的在职培训制度。

美国政府 2012 年发布了国家网络空间安全教育战略计划（简称 NICE 计划），该计划建立了从院校教育、从业人员培训及普通民众教育的人才培养体系，对全体网民进行网络安全意识培训，对专业人员进行系统的知识技能教育。其中的网络安全人才培训和职业发展模块，详细制定了国家网络安全人才所需的网络安全培训和职业发展过程。

我国信息安全认证中心分别面向从业人员推出了注册信息安全专业人员（CISP）认证、信息安全保障人员（CISAW）认证，长期组织或授权培训机构组织了相关培训，覆盖人数较多，取得很好的效果。部分网络安全企业及专业网络安全培训机构也面向社会开展了各种层次的培训。社会上的网络安全培训机构缺乏规范和监管，普遍存在规模小、师资缺、教材乱等问题，缺乏像美国(ISC)2 这样有国际影响力的认证培训机构，没有形成类似 CISSP、CISA 这样的知名认证品牌。

二、高素质网络空间安全人才特点

（一）政治素养过硬

当前，网络空间安全已经成为国家安全的核心组成部分，并在经济和社会发展的关键环节和基础保障方面发挥日益重要的作用。网络空间已成为陆、海、空、天之外，各国政治、经济、军事、文化实力角力的第五战场。

网络空间安全人才作为保卫国家网络疆场的安全员、战斗员，是国家网络空间战场的生力军，担负着意义非凡的使命与责任。对网络空间安全的捍卫者来讲，技术能力不是唯一的衡量标准，坚定的政治素养和无私的奉献意识往往决定着其能否堪当大任。上海交通大学网络空间安全学院院长李建华曾讲道：“技术是中性的，但技术服务的对象是有立场的。”技术能力出众的网安人才如果没有正确的政治立场，反而会对国家和社会造成严重危害。2013 年

爆发的“斯诺登”事件，不仅揭露了美国政府多个秘密情报监视项目，证实了网络空间斗争的严峻性，同时折射出网络安全从业者政治素养的重要性。

（二）技术和思维特点鲜明

1.快速学习能力强

网络攻击的日新月异，导致了网络安全知识需要实时更新。IT 领域也存在摩尔定律，计算机等 IT 产品的性能每 18 个月就会翻一番。受此影响，相关硬件、软件、知识技术的更新周期越来越短。这就对网络空间安全从业者提出了更高的要求，想要跟上技术更新的速度，就要不断地更新知识结构，追踪前沿知识，并在短时间内学习掌握新技术、新思想。此外，各类软件、硬件、系统的安全漏洞的生命周期较短，在短时间内学习其原理，发现漏洞并研究出漏洞利用的方法，也要求从业者必须具备快速学习和解决问题的能力。

网络空间安全具有实时性，高素质网络安全人才必须做好不断学习新知识的思想准备，时刻关注网络空间最新动态。网络空间实时性的特点，为不少“新人”提供了一展身手的好机会。网络安全的优秀人才越来越年轻化，许多天才黑客甚至只是中学生。这种情况在医学等经验性主导的领域是不可想象的，与医学人才“晚熟”的特点相比，网络安全人才往往越年轻越有活力,快速学习和接受新鲜事物的能力更强。

2.工程实践能力强

网络空间安全的实现不能只靠“纸上谈兵”，在具备一定的理论知识的基础上，将理论付诸实践也是网络安全人才的必备素质。

网络空间安全是典型的工科学科，除了掌握理论知识外，如何将理论应用于实际问题中，利用理论来进行安全技术的设计和实现，是网络安全工程师的基本功。安全系统、硬件产品从设计、建设到后期维护，都需要扎实的工程实践能力作支撑。工程实践能力的强弱一定程度上决定了网络安全人员的实战能力。

3.创新和批判性思维强

国内传统的教育导向以服从和尊重权威为主，培养出来的人才独立思考能力不足。网络安全人才恰恰需要打破固有的模式，以批判性思维向权威提出挑战，独立分析解决问题，从而突破传统的束缚，创造性的在网络空间展开攻击、防护、设计等工作。

乔布斯、扎克伯格等业界奇才，无一不是个性十足，勇于颠覆传统，不断追求创新和卓越的另类。只有具备独立思考能力，敢于另辟蹊径的创新性人才，才能走在网络空间技术浪潮的潮头，引领时代和技术潮流走向，成为该领域的大家。

（三）社会科学和人文素养兼备

1.法律和道德素养良好

进入 21 世纪以来，网络攻击、恶意软件入侵等网络犯罪行为愈演愈烈，严重威胁到网络空间安全和个人隐私安全，各国对网络空间进行必要的管理和控制方面已达成共识，加快了网络空间管控的立法速度。

在网络空间安全立法方面，美国一直走在全世界的最前面。自 2002 年以来，美国通过了近 50 部与网络空间安全有关的联邦法律，其中《网络安全研发法》、《电子政务法》、《联邦信息安全管理法》、《网络安全法案》等。我国于 2016 年发布《网络安全法》，此后又陆续发布《网络安全技术加强规范》、《关键信息基础设施安全保护条例》等法规条例，为国家网络空间安全建设和治理的实施工作提供了强大的法律法规后盾。

近年来，网络主权边界、网络数据利用和个人隐私保护的边界，越来越受到人们关注，相关立法和保护措施越来越明晰。这些都要求网络安全人员具备良好的法律和道德素养，从而厘清网络空间的边界、权利和义务，更好的规范自身在网络空间的行为方式，远离网络违法犯罪，同时避免网络行为所产生不必要的纠纷。

2.心理学和人文素养良好

随着各国网络空间安全防护意识和手段的不断提升，单靠技术手段完成网络入侵与攻击变得越来越困难。美国利用震网病毒摧毁伊朗核工业设施，就是在情报部门的配合下成功植入木马病毒，从而发挥其技术威力。

从历年来全世界发生的网络安全事件来看，多数问题远非技术问题，有学者认为 70%的网络安全事件本质上都是人的问题。高级的网络安全攻击通常是从技术人员本身下手，运用社会工程学、心理学等知识找到人在网络生态系统中的弱点，而后再用技术手段打开突破口。因此，网络安全人才需要具备社会公共管理科学知识、社会工学和心理学等领域的知识基础，而并非仅仅是技术天才。

三、网络空间安全人才培养规律

（一）学科的交叉性

网络空间安全学科不仅综合了计算机科学与技术、信息与通信工程、软件工程、数学等相近的理工类一级学科，还涵盖了管理、法律、社会等自然及人文学科的内容，是高度交叉融合的学科。网络空间安全作为一个整体，并不是将各自学科安全问题进行简单集合，而是以跨学科凝练的安全基本理论体系和方法论体系，来指导各个学科内的安全问题的研究。

在人才培养的过程中只注重单独某一学科的安全问题，或将网络空间安全问题当作各学科安全问题的简单集合，都会造成人才培养的局限性。另一方面，一旦忽视社会科学、人文

素养以及政治立场的塑造，培养出来的学生只具备专项技术能力，在解决现实问题时往往捉襟见肘。网络空间安全需要的是具有从全面的视角来发现、分析和解决安全问题能力的人才。

（二）渠道的协同性

人才培养是一项系统性工程，网络安全领域对人才的理论、实践、创新能力都有很高的要求，单靠院校一方努力，难以达成人才培养的目标。

首先，院校的主渠道作用需要社会和企业的有力支撑。搭建院校与行业和产业间的桥梁，为院校人才培养提供实践平台，把高校的教学培养和企业实践有机结合起来,实现高校与企业、社会的综合培养。促进政府机构、科研院校和企业形成伙伴关系，形成涵盖网络空间教育、培训和产业研发的健全生态系统，从而有效拓宽人才培养渠道。

其次，健全的职业培训体系将为人才培养开辟更多渠道。企业在“掐尖”院校毕业人才的同时，要为人才的继续教育和培训创造条件，利用自身的实践平台优势，在用人的同时继续育人。在职业技能培训和认证方面，建立政府、认证机构、培训机构、高校及研究院所、企业多方协作的认证和培训模式，规范和统一培训资质，从而使行业培训、认证更加权威和规范。

（三）导向的实践性

工程实践能力是网络安全人才的核心素质。在人才培养过程中突出实践性导向尤为重要。

首先，在课程体系设计上，加大实验和实践课程的比重，提高实践环节的考核要求。其次，采用产学研相结合的教育模式，企业利用自身优势，把培训学生当作对人才的长期投资，企业职员定期到院校学习深造并与老师一起对学生进行指导。再次，网络空间安全的学习实践，需要大量最新的仿真环境，国家需加强基础设施和平台的建设力度。

（四）生源的多样性

网络空间变化快，知识和技术更新周期短的特点决定了网络空间安全人才选拔和发现的模式与其他领域有所区别。批判性思维和实践能力强的人才往往是一些具有“极客”精神的“偏才”“奇才”和“怪才”，也是人才培养的重要生源之一。

网络空间安全的“奇才”和“怪才”对网络空间安全技术有着强烈的兴趣和热情，他们一般非科班出身，实践经验丰富，实战成果丰硕，在对抗中解决实际安全问题的能力强，“剑走偏锋”的技术往往成为网络空间安全对抗中的杀手锏。

综上所述，国家需从顶层设计角度，打破人才选拔方面的限制，扩大人才选拔的来源，加快我国网络空间安全人才队伍培养步伐，支撑网络强国建设。（来源：《网信军民融合》杂志 2019 年 4 月刊）

四、政府之声

➢ 《网络安全审查办法（征求意见稿）》公开征求意见的通知

2019 年 5 月 21 日，为提高关键信息基础设施安全可控水平，维护国家安全，依据《中华人民共和国国家安全法》《中华人民共和国网络安全法》等法律法规，国家互联网信息办公室会同国家发展和改革委员会、工业和信息化部、公安部、国家安全部、商务部、财政部、中国人民银行、国家市场监督管理总局、国家广播电视总局、国家保密局、国家密码管理局联合起草了《网络安全审查办法（征求意见稿）》，现向社会公开征求意见。

征求意见稿称，对于申报网络安全审查的采购活动，运营者应通过采购文件、合同或其他有约束力的手段要求产品和服务提供者配合网络安全审查，并与产品和服务提供者约定网络安全审查通过后合同方可生效。

征求意见稿称，网络安全审查重点评估采购活动可能带来的国家安全风险，主要考虑的因素有：对关键信息基础设施持续安全稳定运行的影响，包括关键信息基础设施被控制、被干扰和业务连续性被损害的可能性；导致大量个人信息和重要数据泄露、丢失、毁损、出境等的可能性；产品和服务的可控性、透明性以及供应链安全，包括因为政治、外交、贸易等非技术因素导致产品和服务供应中断的可能性等，共七项考虑因素。（来源：国家互联网信息办公室）

- **《网络安全审查办法（征求意见稿）》**
- **全文：**http://www.cac.gov.cn/2019-05/24/c_1124532846.htm

➢ 工信部通报: 2019 年第一季度信息通信行业网络安全监管情况

2019 年 5 月 22 日，为贯彻落实《网络安全法》，进一步强化信息通信行业网络安全监管，落实企业网络安全责任，现将 2019 年第一季度信息通信行业网络安全监管有关情况通报如下：

一、网络安全总体态势

(一)公共互联网安全保护形势依旧严峻。一季度，恶意程序、各类钓鱼和欺诈网站仍不断出现，全行业共处置网络安全威胁约 967 万余个，包括恶意 IP 地址、恶意域名等恶意网络资源近 170 万个，木马、僵尸程序、病毒等恶意程序约 698 万余个，网络安全漏洞等安全隐患约 4.8 万个，主机受控、数据泄露、网页篡改等安全事件约 93.5 万个。

(二)工业互联网安全风险居高不下。一季度，对 98 个工业互联网平台、近 4800 个平台 IP 域名、46.7 万个工业互联网联网设备进行安全监测，发现疑似风险 2466 个，其中高、中危漏洞分别占比 33.4%，49.4%。相较 2018 年第四季度，中高危漏洞占比下降近 10 个百分点，但仍然维持在高位。

(三)移动通信转售企业电话用户实名登记工作成效持续巩固。一季度，抽查 16 家移动通信转售企业 6300 万条电话用户登记信息，实名登记准确率达 99%以上，用户人证一致率为 98.7%，与 2018 年第四季度基本持平。

二、网络安全监管情况

(一)加强网络数据安全事件监测跟踪和执法调查。一季度，组织对媒体曝光及用户投诉数据安全问题较为集中的 7 家企业进行了问询约谈，要求企业及时自查整改问题。针对国内多起因 MongoDB 数据库配置不当引发的数据泄露事件，组织开展技术排查和风险研判，指导各地通信管理部门督促属地相关单位完善安全配置，部署防护措施。联合中央网信办、公安部、市场监管总局积极推进 APP 违法违规收集使用个人信息专项治理工作，组织对用户举报较为集中的百余款 App 进行安全评估，及时通报问题严重的 APP 进行整改。

(二)持续深化电信网络诈骗治理。一季度，联合公安部对重点地区开展专项督导检查，进一步加强对诈骗电话、诈骗短信等的预警分析和联动处置，日均处置诈骗电话 247 万次。

先后下发电信网络诈骗举报通报 2 期，责令 8 家企业对电话用户入网登记、代理渠道、物流配送等方面的管理薄弱环节进行严肃整改。从一季度态势看，受理涉嫌通讯信息诈骗用户举报 1 万余件次，环比下降 42%;处置国际来源诈骗电话 81 万余次，环比下降 70%。

(三)开展移动通信转售企业行业卡安全管理抽查。一季度，对 6 家移动通信转售企业的行业卡安全管理情况进行抽查，针对检查发现的部分销售渠道不合规、合同模板不规范、安全评估审核不严、功能限制落实不力、监测技术手段薄弱等问题，通报相关企业整改，并就进一步做好行业卡安全管理提出具体工作要求。

(四)地方通信管理局全面部署推进网络安全工作。一季度，按照部统一工作部署和网络安全管理局 2019 年工作要点，各地通信管理局结合工作实际，积极组织部署 2019 年网络安全工作，有序推进各项重点任务落实。在重大活动保障方面，北京市通信管理局圆满完成全国“两会”网络安全保障任务，组织完成第二届“一带一路”国际合作高峰论坛保障准备工作;湖北省通信管理局有序组织部署“2019 年第七届世界军人运动会”网络安全保障工作。在治理电信网络诈骗工作方面，河南省通信管理局在全国率先建成电话用户管理系统并上线运行。在数据安全执法方面，江苏、宁夏、浙江、广东、上海等省市通信管理局针对数据安全和个人信息保护开展工作调研和执法检查。在工业互联网安全监测方面，湖南、广东、河南等省通信管理局初步形成与国家工业互联网安全监测平台的数据联动能力。

三、安全指引及风险提示

(一)安全指引

移动通信转售企业要严格落实《关于加强源头治理 进一步做好移动通信转售企业行业卡安全管理的通知》(工信厅网安〔2018〕75 号)要求，切实履行企业主体责任，规范行业卡入网流程，强化行业卡安全管理。

(二)风险提示

1.广大用户要提高数据安全意识。不要轻易向他人提供个人信息，勿将本人手机卡或本人身份证随意提供和转卖给他人使用，杜绝不法分子可乘之机;不要随意蹭网，随意点击短信、微信、邮件上不明来路的链接，或下载来历不明的邮件等。

2.广大用户要谨防短信诈骗。近期，冒充“航空公司客服”、“信用卡服务”、“贷款业务服务”等境外诈骗短信问题较为突出，此类短信多利用用户个人信息进行精准诈骗，迷惑性较强，请广大用户加强防范。（来源：中华人民共和国工业和信息化部网络安全管理局 ）

➢ 我国网络内生安全试验场正式开通上线

2019 年 5 月 22 日，基于我国科学家原创理论和技术研发的网络内生安全试验场，在江苏南京紫金山实验室举行开通仪式。

此次上线的网络内生安全试验场（NEST），是全球首个永久在线、面向全球开放的网络内生安全防御技术试验场。中国工程院院士、国家数字交换系统工程技术研究中心主任邬江兴及其研究团队，针对网络空间漏洞、后门无法避免等问题提出一整套独创的、具有内生性安全效应的拟态防御理论，成为这一试验场的核心支撑。

近年来，我国网络空间拟态防御技术在理论提出、原理验证、技术突破、设备研制等方面取得全方位进展。2016 年，拟态防御原理验证系统通过国家级测试评估；2018 年，全球首例基于拟态构造的系列化网络设备，在中国联通等单位投入线上运行。同年，成功举办首届“强网”拟态防御国际精英挑战赛，在真实网络场景下验证了拟态防御抵御基于未知漏洞的后门攻击能力。

据悉，该试验场将向全球提供技术验证、安全比赛、能力评价、人员培训等多项服务，打造成全球网络安全新高地，孵化出多样化的领先技术产品，用创新技术和实践成果推动网络空间命运共同体建设不断取得新进展。

“开放共享是网络空间的基本属性，我们愿意本着开放共享原则，用技术方案解决当前网络空间的安全顽疾。”在邬江兴院士看来，网络空间不应成为全球化进程中的壁垒和障碍。他表示，该试验场上线后将保持永久在线模式，随时欢迎来自全球任何个人和组织的攻击挑战。（来源：国防部）

➢ 工业和信息化部发布：2019 年智能网联汽车标准化工作要点

2019 年 5 月 18 日，为深入贯彻落实党中央、国务院关于建设制造强国的战略部署，积极创新、探索标准化工作新模式，动态完善、统筹推进标准体系建设，加快重点领域关键急需标准制定，加强国际标准法规协调与产业协作，工业和信息化部装备工业司组织全国汽标委编制了 2019 年智能网联汽车标准化工作要点。主要内容如下：

一、落实标准体系建设指南，动态完善标准体系

1.贯彻落实《国家车联网产业标准体系建设指南（智能网联汽车）》，加快基础通用和行业急需标准制定，加强标准关键技术研究和试验验证工作，及时开展标准宣贯与实施，确保各类标准项目有序推进。

2.开展标准体系建设工作总结和绩效评估，及时总结标准体系建设成果、经验及问题，持续优化完善标准体系，适时调整标准项目优先级及工作安排，确保标准体系建设持续支撑产业发展。

3.切实贯彻《C-V2X 标准合作框架协议》，按照“友好合作、专业分工、优势互补、协同推进”原则，研究制定汽车通信应用层相关标准，配合做好道路基础设施、智能交通管理平台等相关标准制定，协同推进车联网标准体系建设。

二、系统布局技术领域，加快重点标准制修订

1.稳步推动先进驾驶辅助系统（ADAS）标准制定。完成乘用车和商用车自动紧急制动（AEB）、商用车电子稳定性控制系统（ESC）等标准制定，组织开展先进驾驶辅助系统术语及定义、盲区监测、车道保持辅助等标准的研制工作，积极推动全景影像监测、夜视系统、信号提示优先度等标准立项，全面推进全速自适应巡航、交通拥堵辅助控制及自动紧急转向

等自动控制系统标准的预研工作。

2.全面开展自动驾驶相关标准研制。完成驾驶自动化分级等基础通用类标准的制定，组织开展特定条件下自动驾驶功能测试方法及要求等标准的立项，启动自动驾驶数据记录、驾驶员接管能力识别及驾驶任务接管等行业急需标准的预研，积极组织开展商用车辆列队跟驰等重要标准的测试验证，组织编制智能网联汽车功能和性能评价指南等指导性文件。

3.有序推进汽车信息安全标准制定。完成汽车信息安全通用技术、车载网关、信息交互系统、电动汽车远程管理与服务、电动汽车充电等基础通用及行业急需标准的制定，研究提出汽车软件升级、信息安全风险评估等应用类标准的立项，系统开展汽车整车及零部件信息安全测试评价体系研究，启动车载硬件环境及操作系统相关标准体系规划及预研。

4.协同开展汽车网联相关标准制定。完成网联车辆方法论标准制定工作，推动智能网联汽车无线通信应用层技术要求、信息交互系统技术要求等标准立项，启动交叉路口碰撞预警等系统应用类标准的预研，完成智能网联汽车通信需求、自动驾驶高精地图标准化需求等研究项目，提出智能网联汽车相关基础设施与服务标准项目建议。

三、履行国际协调职责，加强标准交流与合作

1.深入参与联合国智能网联汽车国际法规协调。切实履行联合国 WP29 框架下自动驾驶车辆工作组副主席职责，加强智能网联汽车国际法规协调专家队伍及支撑体系建设，积极推动联合国自动驾驶法规相关框架文件制定及实施，主动承担重点法规项目的组织、协调及研究任务，积极承办相关法规制定工作会议。

2.继续加大国际标准的参与广度与深度。系统跟踪国际标准化组织道路车辆委员会（ISO/TC22）动态，积极参与自动驾驶特别工作组（ADAG）项目规划，深入参与预期功能安全、信息安全等重点标准制定；认真履行自动驾驶测试场景工作组（SC33/WG9）召集人职责，积极承担测试场景通用要求等国际标准制定。

3.持续加强和扩大国际交流与合作。依托政府间多双边对话合作机制，巩固与欧盟、德国、法国、日本等的交流与合作，逐步建立“一带一路”沿线国家的交流合作机制，支持全国汽标委及相关组织与国外对应机构建立合作关系，形成多方参与、多层协作的智能网联汽车标准法规国际交流合作机制。（来源：工业和信息化部 ）

五、本期重要漏洞实例

➢ 关于 Microsoft 远程桌面服务存在远程代码执行漏洞的安全公告

发布日期：2019-05-15
更新日期：2019-05-15
受影响系统：
Windows 7 for 32-bit Systems Service Pack 1
Windows 7 for x64-based Systems ServicePack 1
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2008 for x64-based SystemsService Pack 2
Windows Server 2008 for x64-based SystemsService Pack 2 (Server Core installation)
Windows Server 2008 R2 for Itanium-BasedSystems Service Pack 1
Windows Server 2008 R2 for x64-basedSystems Service Pack 1
Windows Server 2008 R2 for x64-basedSystems Service Pack 1 (Server Core installation)
Windows XP SP3 x86
Windows XP SP2 x64
Windows XP Embedded SP3 x86
Windows Server 2003 SP2 x86
Windows Server 2003 SP2 x64
描述：

CNTA-2019-0017
CNVD-2019-14264
2019 年 5 月 15 日，国家信息安全漏洞共享平台（CNVD）收录了 Microsoft 远程桌面服务远程代码执行漏洞（CNVD-2019-14264）。攻击者利用该漏洞，可在未授权的情况下远程执行代码。目前，漏洞细节虽未公开，但已引起社会高度关注，微软公司已发布官方补丁。
Microsoft Windows 是美国微软公司发布的视窗操作系统。远程桌面连接是微软从 Windows 2000 Server 开始提供的组件。
2019 年 5 月 14 日，微软发布了本月安全更新补丁，其中修复了远程桌面协议（RDP）远程代码执行漏洞。未经身份验证的攻击者利用该漏洞，向目标 Windows 主机发送恶意构造请求，可以在目标系统上执行任意代码。由于该漏洞存在于 RDP 协议的预身份验证阶段，因此漏洞利用无需进行用户交互操作，存在被不法分子利用进行蠕虫攻击的可能。
CNVD 对该漏洞的综合评级为“高危”。
<*来源：微软
建议：

厂商补丁：
目前，微软官方已发布补丁修复此漏洞，CNVD 建议用户立即升级至最新版本：
链接：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

链接：https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/

另可采取下列临时防护措施：

1、禁用远程桌面服务。

2、通过主机防火墙对远程桌面服务端口进行阻断（默认为 TCP 3389）。

3、启用网络级认证（NLA），此方案适用于 Windows 7、Windows Server 2008 和 Windows Server 2008 R2。启用 NLA 后，攻击者首先需要使用目标系统上的有效帐户对远程桌面服务进行身份验证，然后才能利用此漏洞。

附：参考链接：

链接：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
链接：https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/

➢ Cisco 多款产品本地安全绕过漏洞

发布日期：2019-05-15
更新日期：2019-05-22
受影响系统：
Cisco NX-OS Software for UCS 6300 Fabric Interconne
Cisco NX-OS Software for UCS 6300 Fabric Interconne
Cisco NX-OS Software for UCS 6200 Fabric Interconne
Cisco NX-OS Software for UCS 6200 Fabric Interconne
Cisco NX-OS Software for Nexus 7700 Series 8.2
Cisco NX-OS Software for Nexus 7700 Series 8.1
Cisco NX-OS Software for Nexus 7700 Series 8.0
Cisco NX-OS Software for Nexus 7700 Series 7.3
Cisco NX-OS Software for Nexus 7700 Series 7.2
Cisco NX-OS Software for Nexus 7000 Series 8.2
Cisco NX-OS Software for Nexus 7000 Series 8.1
Cisco NX-OS Software for Nexus 7000 Series 8.0
Cisco NX-OS Software for Nexus 7000 Series 7.3
Cisco NX-OS Software for Nexus 7000 Series 7.2
Cisco NX-OS Software for MDS 9700 Series 8.2
Cisco NX-OS Software for MDS 9700 Series 8.1
Cisco NX-OS Software for MDS 9700 Series 7.3
不受影响系统：
Cisco NX-OS Software for UCS 6300 Fabric Interconne
Cisco NX-OS Software for UCS 6200 Fabric Interconne
Cisco NX-OS Software for Nexus 7700 Series 8.2(3)
Cisco NX-OS Software for Nexus 7700 Series 7.3(3)D1

Cisco NX-OS Software for Nexus 7000 Series 8.2(3)
Cisco NX-OS Software for Nexus 7000 Series 7.3(3)D1
Cisco NX-OS Software for MDS 9700 Series 8.3(1)
Cisco NX-OS Software for MDS 9700 Series 8.1(1a)
描述：

BUGTRAQ ID: 108375
CVE(CAN) ID: CVE-2019-1809
Cisco NX-OS Software 是美国思科（Cisco）公司的一套交换机使用的数据中心级操作系统软件。
Cisco NX-OS Software 的映像签名验证功能存在一个漏洞，允许经过身份验证的本地攻击者使用管理员级别凭据在受影响设备上安装恶意软件补丁。
该漏洞产生原因是对补丁图像的数字签名的不正确验证。通过制作未签名的软件修复补丁来绕过签名检查并将其加载到受影响的设备上，攻击者可利用此漏洞，启动恶意软件补丁映像。
如果以下 Cisco 产品运行含有漏洞的 Cisco NX-OS Software 版本，则会受此漏洞影响：
-MDS 9700 Series Multilayer Directors
-Nexus 7000 Series Switches
-Nexus 7700 Series Switches
-UCS 6200 Series Fabric Interconnects
-UCS 6300 Series Fabric Interconnects
<*来源：Cisco
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190515-nxos-psvb
*>
建议：

厂商补丁：
Cisco
Cisco 已经为此发布了一个安全公告（cisco-sa-20190515-nxos-psvb）以及相应补丁：
cisco-sa-20190515-nxos-psvb： Cisco NX-OS Software Patch Signature Verification Bypass Vulnerability
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190515-nxos-psvb

➢ Linux Kernel 本地信息泄露漏洞

发布日期：2019-05-17
更新日期：2019-05-21
受影响系统：
Linux kernel <= 5.1.2
描述：

BUGTRAQ ID: 108380
CVE(CAN) ID: CVE-2018-7191

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 4.13.14 及之前版本的 tun 子系统中，在 register_netdevice 之前不调用 dev_get_valid_name。这允许本地用户通过带有包含/字符的 dev 名称的 ioctl（TUNSETIFF）调用来导致拒绝服务（NULL 指针解除引用和恐慌）
<*来源：Linux
链接：
https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=0ad646c81b2182f7fa67ec
*>
建议：

厂商补丁：
Linux
Linux 已经为此发布了一个安全公告以及相应补丁:
tun: call dev_get_valid_name() before register_netdevice()
链接：
https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=0ad646c81b2182f7fa67ec

➢ Symantec Messaging Gateway 本地信息泄露漏洞

发布日期：2019-05-15
更新日期：2019-05-21
受影响系统：
Symantec Messaging Gateway < 10.7.0
不受影响系统：
Symantec Messaging Gateway 10.7.0
描述：

BUGTRAQ ID: 108303
CVE(CAN) ID: CVE-2019-9699
Symantec Messaging Gateway 是美国赛门铁克（Symantec）公司的一套垃圾邮件过滤器。该产品具有反垃圾邮件、防病毒、高级内容过滤和数据泄露防护等功能。
Symantec Messaging Gateway 10.7.0 之前版本存在一个信息泄露漏洞，允许攻击者未经授权访问数据。
<*来源：Muhammad Nafees
链接：https://support.symantec.com/en_US/article.SYMSA1482.html
建议：

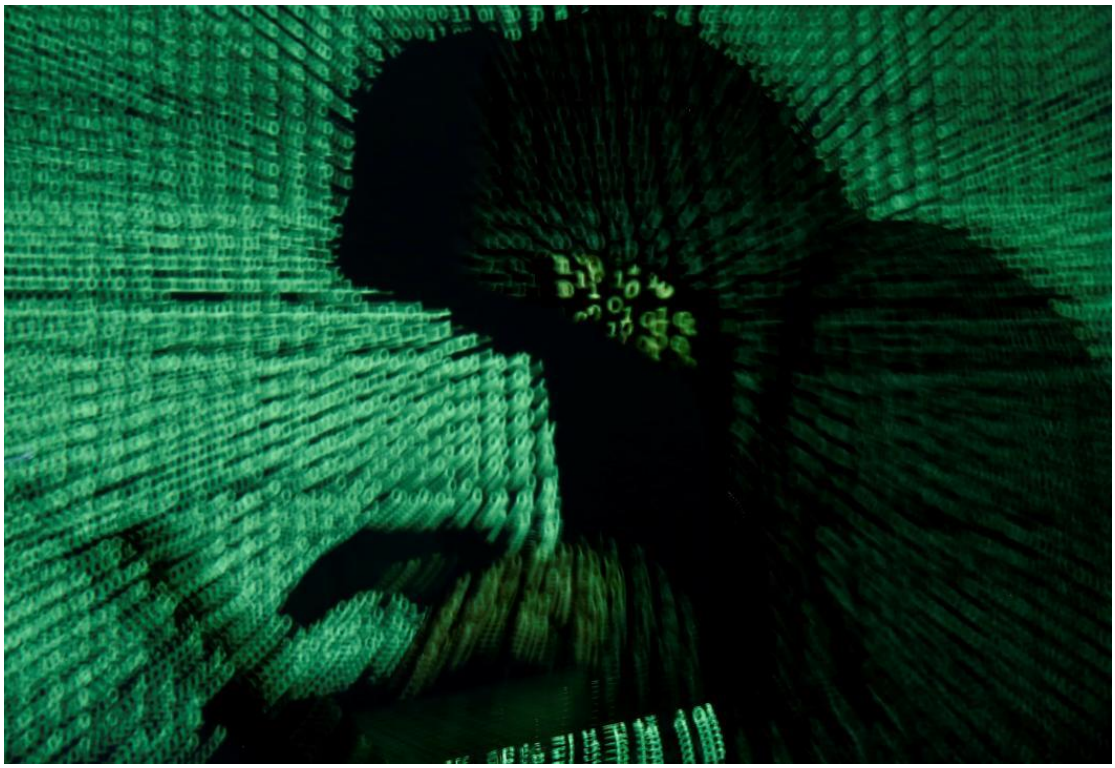
厂商补丁：
Symantec
Symantec 已经为此发布了一个安全公告（SYMSA1482）以及相应补丁:
SYMSA1482：Symantec Messaging Gateway Information Disclosure
链接：https://support.symantec.com/en_US/article.SYMSA1482.html

六、本期网络安全事件

➢ 重庆破涉外黑客案，涉案 2000 万黑客月入 30 万

2019 年 5 月 23 日消息：日前，在“净网 2019”专项行动中，荣昌区公安局在重庆市公安局网安总队的指导下，成功破获系列网络黑客案件。

2018 年 3 月，荣昌警方接上级公安机关线索：荣昌籍黑客许某涉嫌在国外通过网络入侵我国境内网站服务器，以获取服务器权限并出售获利。在市公安局网安总队的指导下，荣昌区公安局迅速成立专案组，展开案侦工作。由于许某长期在菲律宾一带活动，境外侦查难度重重。经过近一年的侦查，专案民警确定了以许某、张某、李某、郭某为骨干的网络黑客犯罪团伙。



2018 年 12 月，该团伙成员陆续回到国内。为防止其成员再次出境从事违法犯罪活动，2019 年 2 月 27 日，重庆市公安局网安总队、荣昌区公安局调集警力 70 余名，分赴重庆、湖北荆州、福建厦门三地实施抓捕。2 月 28 日，三地同时行动，迅速抓捕，将该团伙骨干及成员共 12 人全部抓获。目前,10 人已采取强制措施，正移送起诉中。

经审讯，该网络黑客团伙作案地主要分布于东南亚国家和国内重庆、湖北、福建、山东一带，且有非中国籍人员参与其中，团伙内部又设有若干子团伙，组织分工严密，非法侵入、

控制境内网站数量巨大，仅许某参与的黑客犯罪团伙入侵的国家事务网站就达 200 余个，非法控制网站 500 余个，涉案金额高达 2 千余万元，该团伙成员平均月获利 10 万元到 30 万元不等。

其中，以许某为骨干的菲律宾黑客团伙主要攻击入侵国内的新闻、学校、政府机关网站，通过寻找此类网站漏洞，植入木马病毒，控制网站服务器，加挂黑链自动链接博彩网站，或把境外博彩公司链接地址保存在搜索引擎内，当用户访问网站时，网站会自动跳转至境外博彩公司网页；用搜索引擎搜索“时时彩、博彩”等关键字时，就会优先显示境外博彩公司地址，以达到加大博彩公司访问量，吸引更多人参与赌博的目的。同时，团伙成员还会对被控制的网站服务器定期维护，防止被其他黑客入侵。经审讯，该团伙入侵控制的网站有河南、浙江、江西、辽宁等政府机关、高校在内的网站 700 余个。重庆地区黑客犯罪团伙则以非法入侵计算机信息系统、入侵传销网站为主，获取网站数据库系统权限，以买分卖分方式，获利 20 余万元。

近年来，国内“网络黑客”赴东南亚国家作案日益增加，呈团伙化、集团化发展趋势。此案中，犯罪嫌疑人主要分布在菲律宾、柬埔寨等东南亚国家，涉案人数众多，涉及资金巨大，对境内机关、企事业单位网站大肆攻击，造成我国政治、经济损失重大。

互联网信息技术的发展催生出各类网络安全隐患，犯罪手段也在变换和更新。对此，警方提醒，要树立信息安全意识，加强网站安全管理，从源头上遏制风险隐患，合力筑牢安全防火墙，不给犯罪分子留下可乘之机。（来源：央广网）

➢ 高薪 IT 男为“炫技”窃取母校 4 万余条学生信息 被警方刑拘

2019 年 5 月 20 日，据平安鹤城报道，高薪 IT 人员周某为在学弟学妹面前炫技，竟用黑客手段窃取母校 4 万多条个人信息，目前其已被刑事拘留。

“我真没想到这触犯了法律”周某做梦也没有想到，因为自己一时炫技竟惹上了牢狱之灾。5 月 15 日晚，怀化市公安局鹤城分局网安大队民警将涉嫌侵犯公民个人信息及破坏计算机信息系统的违法犯罪嫌疑人周某从深圳带回怀化。周某因涉嫌窃取怀化市某高校学生信息数据 46767 条，目前已被刑事拘留。

今年 3 月 18 日，怀化市公安局网警在对全市高校进行例行网络安全现场检查时发现某高校教务系统有安全漏洞，并检查出其教务系统于 2 月 13 日被黑客利用漏洞窃取 2007 级

至 2018 级所有学生数据共计 46767 条。发现该情况后，市局网警部门将案情通报给了鹤城分局网警。怀化市公安局鹤城分局立即成立了由网安、刑侦和辖区派出所精干力量组成的联合专案组，共同开展侦查研判及抓捕工作。在上级公安机关的大力支持下，通过分析黑客的攻击手段及目的，还原网上攻击手段，民警很快锁定了人在深圳的犯罪嫌疑人周某。5 月 12 日专案组民警赶往深圳市，并于 13 日上午将犯罪嫌疑人周某抓获归案。由于破案及时，被窃取的信息未发生二次扩散。

在民警们审讯周某时发现，他竟然是该高校的毕业生，并且还是国内一知名数码电子产品公司的高薪聘请人员，拥有高超的电脑技术，可以说是走上了人生巅峰。然而如此“优秀”的人为什么会走上犯罪的道路呢?原因竟是自己虚荣心作祟，想在学弟学妹面前显摆一把而已。周某从母校毕业多年，年初时无意找到当年学校贴吧的账号。心血来潮的他就登陆上去看了一会，如今事业小有成就的他突然虚荣心作祟，想在学弟学妹面前炫一把技，并且还在学校贴吧发帖扬言只要发一张照片，他就能说出这个人的名字。今年 2 月 13 日，周某通过网络攻击窃取并下载了学校 2007 年至 2018 年学生信息共计 46767 条，严重触犯了相关法律，等待他的将是法律的制裁。

民警提醒：刑法第二百五十三条之一规定的“公民个人信息”,是指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身份或者反映特定自然人活动情况

的各种信息，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。非法获取公民个人信息罪是指以窃取或者其他方法非法获取国家机关或者金融、电信、交通、教育、医疗等单位在履行职责或者提供服务过程中获得的公民个人信息，出售或者非法提供给他人，情节严重的行为。根据刑法规定，犯本罪的，处三年以下有期徒刑或者拘役，并处或者单处罚金。（来源：平安鹤城）

➢ 美金融集团被指泄露数亿份产权保险记录：最早可追溯至 2003 年

2019 年 5 月 23 日，据外媒报道，财富 500 强房地产产权保险巨头公司 First American Financial Corp.的网站从 2003 年开始对外泄露了数亿份与抵押贷款交易有关的文件，直到本周才得到来自网络安全公司 KrebsOnSecurity 的通知。

这些数字化的记录--包括银行账号和对账单、抵押贷款和税务记录、社会安全号码、电汇收据和驾照图像--无需任何网络浏览器的认证就可以获取到。

这家总部位于加州圣安娜的 First American 是房地产和抵押贷款行业产权保险和结算服务的领先服务供应商。该公司总共雇佣了 1.8 万名员工，2018 年的收入超过了 57 亿美元。

本周早些时候，一位房地产开发商联系了 KrebsOnSecurity。据这位开放商披露，firstam.com 的信息泄漏如果说没有达到数亿级别起码也有数千万级别。他称，任何知道网站上有效文档 URL 的人都可以通过修改链接中的一个数字来查看其他文档。这可能包括任何曾被 First American 通过电子邮件发送过文档链接的人。

KrebsOnSecurity 证实了该开发商提供的线索，这意味着 First American 的网站泄露了约 8.85 亿份文件，泄露最早可追溯到 16 年前。阅读这些文档不需要身份验证。

许多被曝光的文件则是银行帐号的电汇交易记录以及来自房屋或房产买卖双方的其他信息。向 KrebsOnSecurity 上报了这一数据泄露的开发者 Ben Shoval 称，First American 是房地产产权保险和房地产交易中使用最广泛的公司之一，而买卖双方在交易过程中需要签署一堆的法律文件。

据了解，产权保险代理机构需要从买家和卖家那里收集各种各样的文件，包括社会保险号、驾照、账户对账单，如果是一家小企业，产权保险代理甚至还会收集公司内部文件。很显然，无论是卖家还是买家都希望自己的信息能够得到很好的保护。

Seller Information

Escrow No.

Seller 1 Name: [redacted] **SSN:** [redacted]

Seller 2 Name: **SSN:**

Current Marital Status: Divorced

Telephone Number(s):
Seller 1: [redacted] Home / Work / Cell / Fax (circle one)

Seller 2: Home / Work / Cell / Fax (circle one)

Email address:
Seller 1: [redacted]

Seller 2:

Current Mailing Address: [redacted]
Street Address
Scottsdale AZ 85266
City State Zip

Forwarding Address:
(After Sale of Property)
Street Address
City State Zip

Please complete the following information and return as soon as possible:
(Be sure to include pool loans, water softener loans, & equity credit lines)

1st Mortgage: Lender Name: SLS
Address: 8742 Lucent Blvd Suite 300 Highlands Ranch, CO 80129
Loan No: [redacted] Phone No. 800 315 4757

2nd Mortgage: Lender Name:
Or EQUITY Address:
CREDIT LINE Loan No: Phone No.

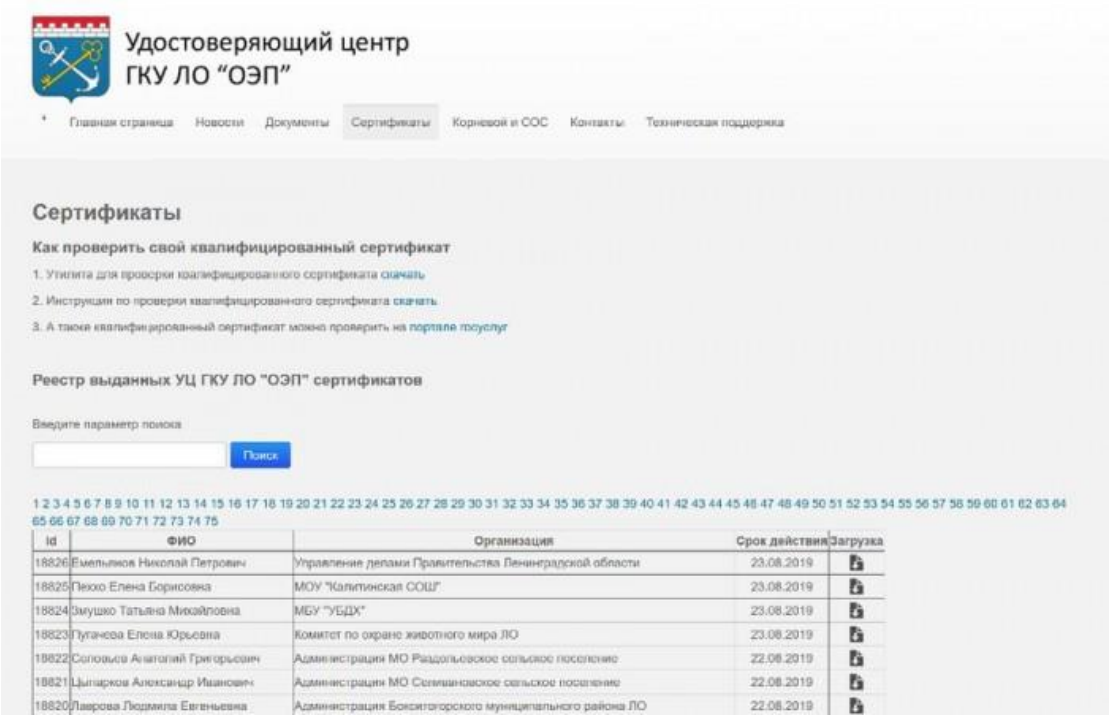
针对这一事件，First American 方面不愿就其网站上可能曝光的总记录数量或这些记录被公开的时间长短做出评论。不过这家公司的发言人倒是发布了一份声明：“First American 了解到一个应用上存在的设计缺陷，这使得其可能未经授权就能访问客户数据。在 First American 内部，安全、隐私和保密都是放在首位的，我们致力于保护客户的信息。公司已经立即采取行动解决了这一问题并关闭了对该应用的外部访问端口。我们目前正在评估这对客户信息安全造成的影响。在我们的内部审查完成之前，我们不会发表进一步评论。”

尽管如此，First American 曝光的信息对所谓的商业电子邮件妥协(BEC)诈骗的钓鱼者和诈骗者来说将是一座虚拟金矿。BEC 骗局通常会模仿房地产经纪人、产权公司、托管公司等诱使买房者把钱汇给骗子。（来源：cnBeta）

➢ 俄罗斯政府网站被爆泄露 225 万用户社保和护照等信息

2019 年 5 月 17 日，多家俄罗斯政府网站泄露了超过 225 万公民、公务员和高层政治家的私人和护照信息。俄罗斯非政府组织 Informational Culture 的联合创始人 Ivan Begtin 最先发现并公开了本次严重的数据泄露事件。由三篇博文组成的系列报道中，Begtin 表示他对政府在线认证中心、50 家政府门户网站以及政府机构使用的电子投标平台进行了调查。

调查结果发现有 23 家网站泄露个人保险信息（SNILS，相当于社保卡号码），14 家网站泄露护照信息。Begtin 表示通过这些网站总共有超过 225 万条俄罗斯公民的信息数据，而且任何人都可以进行下载。从这些网站泄露的数据包括全名、职称、工作地点、电子邮件和税号。



虽然一些网站泄漏的数据难以识别并且需要 Begtin 从数字签名文件中提取元数据，但可以使用谷歌搜索政府网站上的开放网络目录找到一些数据。在今天的 Facebook 帖子中，研究人员说八个月前他联系了负责数据隐私的俄罗斯政府机构 Roskomnadzor。

在接受外媒 ZDNet 采访的时候，Begtin 表示多次通知俄罗斯政府监管机构，但是该机构并没有采取措施来增强这些网站的安全防护，目前依然可以访问这些数据。在去年 4 月希望通过博文方式吸引公众和监管机构注意之后，今天 Begtin 通过俄罗斯新闻网站 RBC 公布了他的发现，而且该网站发布了一篇详细的深入报道。（来源：新华社）

➢ 湖北首例入侵物联网系统案告破，竞争对手使坏致十万设备离线

2019 年 5 月 16 日从湖北武汉市公安局获悉，当地警方经过 50 余天侦查，成功破获湖北省首例入侵物联网破坏计算机信息系统的刑事案件，13 日，武汉市公安局网安支队会同武汉东湖高新技术开发区公安分局抓获两名犯罪嫌疑人。

据警方介绍，3 月 21 日至 22 日，位于光谷总部国际的“微锋”(化名)科技有限公司的多台物联网终端设备出现故障：自助洗衣机、自助充电桩、自助吹风机、按摩椅、摇摇车、抓娃娃机等均脱网无法正常运行。经统计，共 100 余台设备被恶意升级无法使用、10 万台设备离线，造成了重大经济损失。

接报案后，网警通过对故障设备的源代码进行解密，对公司服务器日志进行取证分析。

原来从 3 月 21 日 20 时开始，公司服务器收到了大量的伪造离线报文，通过溯源分析，网警发现“微天地”科技公司谢某、王某有重大作案嫌疑。

5 月 13 日，民警在位于东湖新技术开发区精工科技园的“微天地”科技公司抓获谢某、王某。经审查核实，谢某系“微锋”公司前员工，2018 年初离职时带走了该公司产品的设计源代码，后与王某共同成立了“微天地”科技公司，成为“微锋”公司的行业竞争对手。谢某、王某为提高自己公司产品的市场占有率，破解了“微锋”公司的物联网服务器，利用系统漏洞将终端设备恶意升级，导致 100 余台设备系统损坏，无法正常工作;同时模拟终端设备，以每秒 3 至 4 千条的速度给服务器发送伪造离线报文，导致 10 万台设备离线。

目前，武汉东湖高新技术开发区公安分局依法以涉嫌破坏计算机信息系统罪将谢某、王某刑事拘留，案件在进一步深挖中。（来源：澎湃新闻）

➢ 46 万名客户信息遭泄露优衣库回应:不涉及中国网站

2019 年 5 月 13 日，优衣库母公司日本迅销(Fast Retailing)发布公告称，4 月 23 日至 5 月 10 日期间，其日本在线购物网站遭到黑客攻击，黑客在“未经授权”的情况下进行了 46.11 万次登录，这意味着超过 46 万名顾客的信息可能遭到了泄露。这些账户包含的信息包括客户姓名、地址、电话号码、电子邮件、生日、收件地址以及部分信用卡信息。该公司承认，虽然信用卡密码“不存在泄露的可能性”，但黑客可能已经“浏览过部分信用卡的信息”。日本迅销称，目前已经向受影响的账户单独发送了电子邮件，要求他们重置账号密码。

2019 年 5 月 14 日下午日本迅销发布声明说，旗下品牌优衣库、GU 销售网站逾 46 万名客户个人信息遭未授权访问，可能造成信息泄露。优衣库方面当天表示，经调查，此次事件不涉及中国的网站及信息平台。

目前还没有相关信息为第三方使用的报告。迅销公司说，已经给相关程序漏洞打“补丁”，作废了受影响账户的登录密码，并要求受影响客户重新设置线上店登录密码。迅销公司为此次事件向客户致歉，承诺将防止同类事情再次发生。5 月 14 日，该公司股价单日内下跌 2.54%。

优衣库方面表示：关于近日迅销集团旗下日本电商网站账户遭黑客攻击事件，经调查，此次事件不涉及中国的网站及信息平台。在中国，优衣库一直以来严格遵守国家的各项法律法规，并通过严格的管理流程和技术手段保护消费者的个人信息及消费数据。优衣库将一如既往地严格遵守国家有关法律法规，为消费者提供安全的购物环境。（来源：安全学习那些事）