国盟信息安全通报

2019 年 6 月 24 日第 195 期

国盟信息安全通报

（第 195 期）

国际信息安全学习联盟

2019 年 6 月 24 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 110 个、中危漏洞 162 个、低危漏洞 21 个。漏洞平均分值为 6.04。本周收录的漏洞中，涉及 0day 漏洞 185 个（占 63%），其中互联网上出现“RarmaRadio 'Server'拒绝服务漏洞、WordPress Antena_Ri Institute Themes 开放重定向漏洞”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 2883 个，与上周（1752 个）环比增长 65%。

主要内容

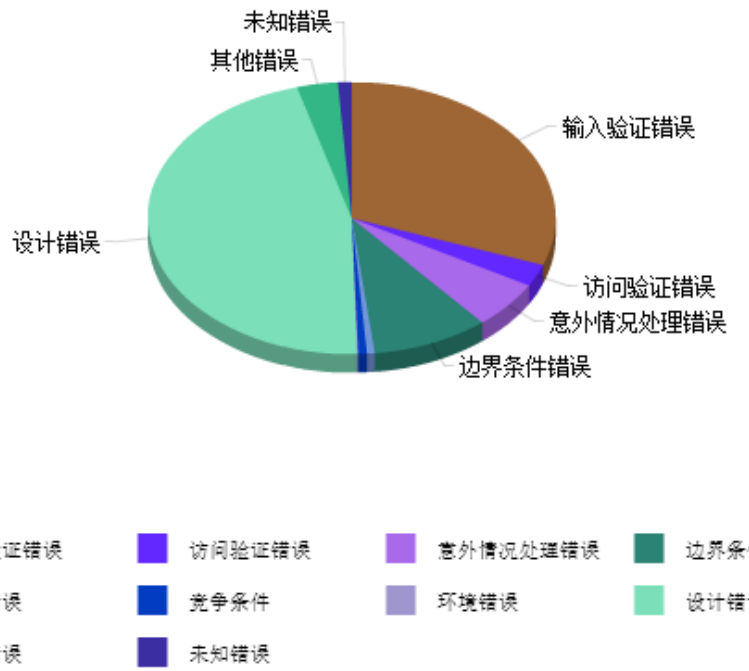
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

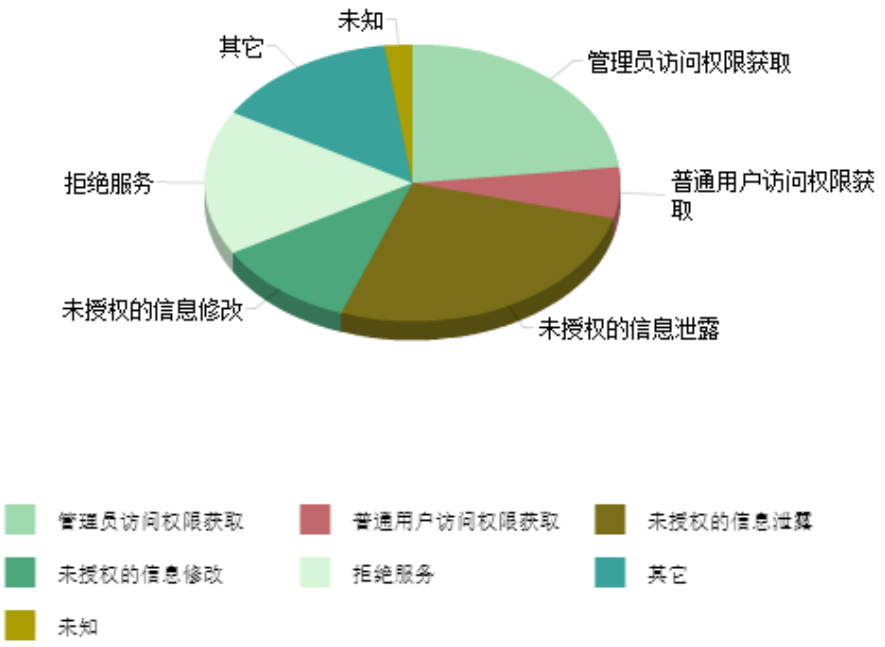
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 293 个，其中高危漏洞 110 个、中危漏洞 162 个、低危漏洞 21 个。漏洞平均分值为 6.04。本周收录的漏洞中，涉及 0day 漏洞 185 个（占 63%），其中互联网上出现“RarmaRadio 'Server'拒绝服务漏洞、WordPress Antena_Ri Institute Themes 开放重定向漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 2883 个，与上周（1752 个）环比增长 65%。

二、安全漏洞增长数量及种类分布情况

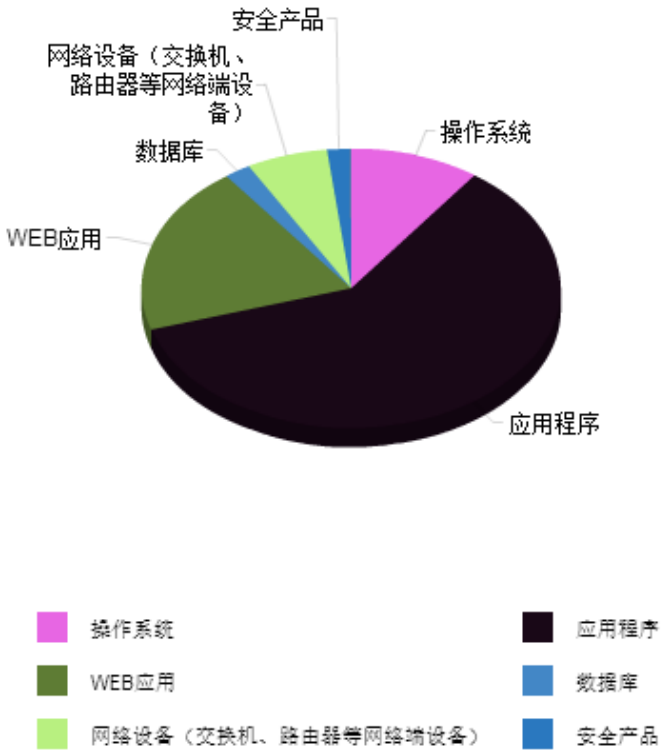
➢ 漏洞产生原因（2019 年 6 月 10 日—2019 年 6 月 24 日）



➢ 漏洞引发的威胁（2019 年 6 月 10 日—2019 年 6 月 24 日）



➢ 漏洞影响对象类型（2019 年 6 月 10 日—2019 年 6 月 24 日）



三、安全产业动态

➢ 加紧备战美国欲将全球拖入网络战争

去年，美国国防部发布的网络空间战略强调了“前沿防御（Defense forward）”理念。这被外界解读为美国军方将在他国而非美国本土实施网络攻防行动。此前，美国总统也赋予军方不受阻挠地部署先进网络武器的自由。作为网络战的始作俑者，美国正在通过积极网络备战，加速将全球拖入一场不会存在赢家的网络战争。

多年来，美国政客一直鼓吹其可能遭遇“网络珍珠港”攻击的风险，但全球首例使用网络武器攻击他国设施的行动却是由美国发起。作为网络战的始作俑者，美国不仅是网络战最强的国家，也是发动网络战最多的国家。

2004 年，美国发起网络攻击，导致利比亚国家顶级域名瘫痪。2010 年，美国和以色列联合制造的“震网”病毒攻击伊朗核设施，导致伊 1000 台离心机报废，致使伊朗核计划几乎“停滞”。2016 年，美国前国防部长卡特首次承认，美国使用网络手段攻击了叙利亚 ISIS 组织等，这是美国首次公开将网络攻击作为一种作战手段。2019 年 3 月初，委内瑞拉全国出现大规模停电，23 个州中有 18 个州受到影响，直接导致交通、医疗、通信及基础设施的瘫痪。委内瑞拉总统马杜罗指责美国策划了对该国电力系统的“网络攻击”，目的是通过全国范围的大停电，制造混乱，迫使政府下台。有分析认为，在无法进行直接和间接军事干预

情况下，对委内瑞拉发起网络攻击可能是美国的最佳选项。

美国在网络空间的备战计划从未停歇。2016 年底，美国进一步提升网络战的战略地位和作战价值，将原从属于美国战略司令部的网络战司令部提升为独立一级司令部，构成了总统—国防部长—作战司令部司令三级网络战指挥机制。目前，美军拥有 133 支网络战部队。2006—2016 年 10 年间，美军先后举行的大规模“网络风暴”演习或者网络太空战演习共 7 次，其中 3 次网络攻防作战行动专门针对中国。2018 年 8 月，美国总统特朗普签署命令，推翻了前总统奥巴马 2012 年签署的“第 20 号总统政策指令”（PPD—20），让军方更自由地部署先进网络武器，而不用受国务院和情报界阻挠。

对于美国的这些做法，哥伦比亚大学研究学者、网络安全专家杰森·希利（Jason Healey）十分忧虑，认为美国已经滑入永久的网络战，其中不会有真正的赢家。

这种担忧其实不无道理。美国不断加强自身网络战能力，给全球做出了恶劣的示范，如果其他国家或者美国的对手组织也效仿美国加强网络战能力建设和手段运用，美国绝不可能“独善其身”，倒是很可能是首当其冲的目标。靠互相攻击不可能实现网络安全，只会让网络空间走上一条对抗升级的不归路。（来源：人民日报）

➢ 《个人信息出境安全评估办法》解读

随着网络化和信息化的不断发展，我国已经成为世界上网民数量最多、网络数据生产量最大的国家之一，在我国数字经济领域高速发展的同时，频发的网络安全和数据泄露事件也在时刻提醒我们，对个人信息进行保护刻不容缓。

2019 年 6 月 13 日凌晨，国家互联网信息办公室发布了《个人信息出境安全评估办法（征求意见稿）》（以下简称“办法”），《办法》界定了个人信息出境的行为，明确了网络运营者和个人信息接收者的职责，细化了个人信息出境安全评估的内容。《办法》的出台对保障个人信息安全、规范个人信息出境依法有序的流动，具有重大的指导意义。

《办法》的出台，一方面是对我国已经出台的关于个人信息保护法律法规的进一步细化和延伸，如 2017 年开始实施的《网络安全法》第三十七条规定：“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估。”《办法》正是对个人信息出境进行安全评估的重要依据。

另一方面，针对国际范围内的数据流动，部分国家及国际组织出台了各自的法律和政策文件，来管理以个人信息为代表的跨境数据，如欧盟的《一般数据保护条例》（GDPR）、英国的《数据保护法案》、亚太经合组织的《跨境隐私规则体系》、日本的《个人信息保护法》等，以保障个人信息跨境流动的安全。我国是数据资源产出大国，亟需建立符合我国国情的个人信息出境管理办法，在数据跨境流动中切实保障个人信息安全。

《个人信息出境安全评估办法》作为一项“安全评估”办法，很多人关心的问题是，其安全评估的对象是谁？谁来进行安全评估？如何进行安全评估？《办法》的 22 个条款围绕这些问题给出了解答。

一是评估对象是谁？有人担心《办法》一旦实施，需要针对普通个人用户进行安全评估。其实不然，《办法》第二条明确指出“网络运营者向境外提供在中华人民共和国境内运营中收集的个人信息，应当按照《办法》进行安全评估”，可以看出，安全评估的对象是网络运营者，而不是个人用户。这里网络运营者，是指网络的所有者、管理者和网络服务提供者，普通的个人不在此范畴。

之所以将评估对象界定为“网络运营者”，是因为我国大量的个人信息，主要是被网络运营者所收集、持有和使用，管理好了这些拥有大量个人信息的网络运营者，就能在更大范围内保障个人信息安全。

二是谁来进行评估？安全评估工作由各省级网信部门负责，这是因为其担负着网络安全管理职能。具体来说，网络运营者向所在地省级网信部门申报个人信息出境安全评估，省

级网信部门组织专家或技术力量进行安全评估，经安全评估认定个人信息出境不会影响国家安全、损害公共利益，能够有效保障个人信息安全的，可以出境。

为了不影响网络运营者的正常业务，除复杂情况外，安全评估一般在 15 个工作日内完成。对安全评估结论存在异议的，网络运营者还可以向国家网信部门提出申诉。

三是评估内容是什么？有一种担心是，安全评估实施过程中，会不会引入个人信息泄露的风险？其实这一担心是完全不必要的。我们首先来看安全评估时网络运营者所需提供的材料有哪些，《办法》第四条指出，提供的材料包括申报书、网络运营者与接收者签订的合同、个人信息出境安全风险及安全保障措施分析报告等；再来看省级网信部门在安全评估时重点评估哪些内容，《办法》第六条指出，主要从是否符合法律法规、是否能保障个人信息主体合法权益等方面进行评估。可以看出，安全评估过程中并不需要提供具体的用户个人信息。

也就是说，评估的是网络运营者是否能够对拟出境的个人信息提供充分的安全保障，而非具体的个人信息本身。

四是个人信息出境后安全如何保障？个人信息流到境外后，由于数据持有者发生了变化，数据的保护能力、适用的法律法规也会发生改变，个人信息主体维护自身合法权益将面临一定的困难，《办法》充分考虑了这一难题，第十三至十五条要求境内网络运营者与境外个人信息接收者签订合同，明确对个人信息主体合法权益的保护，同时第十六条还对接收者将接收到的个人信息传输给第三方的行为进行了限定。

《个人信息出境安全评估办法》明确了网络运营者在个人信息出境方面的责任和义务，对网络运营者做好个人信息出境安全工作提出了更高的要求。这是针对个人信息脱离控制流向境外的情况，如何有效地保障个人信息主体的合法权益，所采取的一项有力的制度设计。

（来源：中国网信网　作者：邹潇湘　张奕欣）

➢ 国家工信安全中心：2019 年工业信息安全态势展望

一、2019 年工业信息安全形势判断

（一）针对工业企业的网络攻击呈现增势

2018 年，法国、俄罗斯等数百家工业企业成为网络钓鱼的攻击目标，涉及制造业、石油天然气、冶金等行业。2019 年，随着制造业转型升级持续推进，工业互联网发展速度加快，海量工业设备泛在连接、企业业务系统云化服务、网络化协调制造的趋势日益明显，工业生

产装备、传感器、工业控制系统等极易成为网络攻击的重点目标，工业企业受攻击风险进一步增大。

（二）工业数据面临严峻安全威胁

2018 年，100 余家汽车制造商的关键生产数据遭泄露事件，敲响了工业数据安全防护警钟。据《2018 年数据泄露调查报告》统计，全球制造业的数据泄露事件多达 536 起，行业排名第 6，其中涉及大型企业事件 375 起，行业排名居首位。2019 年，随着工业企业上云、工业 App 培育进程的推进，工艺参数、产能信息等关乎工业企业命脉的海量关键数据进一步向云平台汇聚，成为不法分子牟取利益的攻击窃密目标。

（三）勒索病毒攻击瞄准制造业

据国家工信安全中心统计，2017-2018 年，工业领域公开报道的勒索病毒攻击事件高达 17 起，其中制造业是攻击的重点目标。2019 年以来，针对制造业的勒索病毒攻击事件已发生 5 起，涉及多国知名化工、食品、汽车制造企业，直接造成了系统瘫痪、生产停滞、运营中断等严重后果。未来，随着制造业企业价值密度增大、网络依赖性提升，将愈发成为勒索者的“理想目标”。

（四）关键领域工控系统成为国家网络对抗攻击目标

在网络化、智能化的社会背景下，国家安全边界已经超越地理空间限制，延伸到了信息网络。以 2010 年攻击伊朗核设施的“震网”病毒为标志性事件，工业控制系统领域的网络对抗已经成为影响各国国防安全的重要元素。2018 年乌克兰氯气站遭 VPNFilter 恶意软件突袭、2019 年委内瑞拉停电等安全事件陆续被证实有国家力量的参与，工业控制系统正成为网络空间对抗的主战场。

二、2018-2019 年工业信息安全十大事件

序号	时间	事件
1	2018 年 2 月	加密采矿软件攻击致欧洲 废水处理设施瘫痪
2	2018 年 4 月	摩莎工业路由器曝 17 项安全漏洞
3	2018 年 7 月	100 余家汽车制造商 大量生产数据因平台漏洞遭泄露
4	2018 年 7 月	乌克兰氯气站遭 VPNFilter 恶意软件突袭
5	2018 年 8 月	勒索病毒导致台积电生产停摆
6	2018 年 11 月	中国台湾合晶科技遭 WannaCry 攻击
7	2018 年 12 月	美第三大报纸出版商 Tribune Publishing 遭勒索病毒攻击
8	2019 年 3 月	委内瑞拉电网工业控制系统遭攻击 导致全国大规模停电
9	2019 年 3 月	挪威铝业集团遭受勒索攻击
10	2019 年 4 月	德国制药和化工巨头拜耳公司 遭恶意软件入侵

三、工业信息安全现状分析

（一）工业控制系统漏洞情况

2018 年，国家工信安全中心收集研判工业控制系统、智能设备、物联网等领域的安全漏洞共计 432 个，主要分布于关键制造、能源、水务化学化工等领域。其中，高危漏洞 276 个，中危漏洞 151 个，中高危漏洞占比高达 99%。从漏洞类型来看，缓冲区溢出漏洞数量最多，占比 20%。排名前五的漏洞类型还有认证错误漏洞、权限控制漏洞、信息泄露漏洞、输入验证漏洞。从漏洞影响领域来看，排名前五的分别是关键制造、能源、水务、医疗健康、食品农业，共占比 74%。

（二）工业控制系统联网监测情况

据监测发现，我国在互联网上可辨识的工控系统、智能设备数量共计万余个，涉及全国 31 个省（区、市），其中广东、浙江、北京数量位居前列，占比 37%。暴露的联网系统和设备多用于市政、能源和智能制造领域，其中，SCADA 软件和 Modbus 设备数量最多。从已研判的案例统计，约 89%的设备及系统未采取有效的安全防护措施，被攻击风险较大。

（三）典型工业信息安全风险案例

自 2015 年起，国家工信安全中心常态化开展工控安全在线监测及风险预警工作，为全国重点省市提供工控安全监测服务。2018 年，共研判发现风险 82 个，其中，39%集中在电

力、热力、燃气及水生产和供应业， 28%来源于制造业。为地方主管部门提供风险监测报告共 12 期。2019 年，进一步强化风险研判水平，共研判发现风险 97 个，提供风险监测报告 8 期，帮助地方有效提升工控安全态势感知能力。

四、工业信息安全工作进展

一是欧美发达国家高度重视工业信息安全，继续强化战略部署。美国出台《能源行业网络安全多年计划》《2019 财年国防授权法案》《2018 年国防部网络战略》《国家网络战略》等文件，不断完善制造业、能源、电力、交通等关键信息基础设施领域政策法规体系；欧盟发布《工业 4.0 网络安全挑战和建议》明确工业 4.0 和工业物联网带来的安全挑战，并提出具体可行的建议。

二是我国工业信息安全顶层设计逐步加强，标准规范进一步完善。工信部发布的多份文件对工业互联网安全提出一系列要求，为我国工业互联网安全保障工作提供了强有力的政策支撑。国家能源局、公安部、水利部相继出台网络安全相关政策，进一步提升重点领域关键信息基础设施网络安全保障能力。同时，工控安全、工业互联网安全、电力系统安全检查等方面多份标准相继发布，安全标准体系持续完善。

三是国际知名安全企业聚焦工业信息安全，发布报告解读安全形势。2018-2019 年，美国国防和信息技术安全承包商帕森斯公司、全球知名网络威胁 AI 检测和响应企业威达、美国火眼公司、以色列工业网络安全公司 CyberX、卡巴斯基实验室、趋势科技等知名企业，在广泛采集其信息安全产品和服务监测数据、深入调研用户和客户的基础上，发布多份报告，加强工业信息安全风险分析和态势研判。

五、工业信息安全工作建议与展望

随着工业企业数字化、智能化程度进一步提高，工业信息安全风险威胁更加严峻，亟需多措并举，保障安全。

（一）加强工业企业安全防护：工业企业进一步贯彻落实《工业控制系统信息安全防护指南》要求，建立健全工控安全责任制，及时排查工控安全隐患，提升安全防护能力。

（二）强化工业数据安全保护：建立工业数据分类分级制度，规范不同级别工业数据的安全保护要求，指导工业企业做好重要数据备份，确保数据的完整性、可用性、保密性。

（三）提升安全监测预警能力：持续建设覆盖全国的工业信息安全态势感知网络，完善技术手段，实时感知安全威胁态势，有效研判预警安全风险。同时，重点工业企业建立工业信息安全监测系统，及时发现设备非法接入、恶意探测攻击等行为，强化风险感知能力。

展望未来，要在网络强国、制造强国战略的引领下，在“互联网+制造业”发展蓝图的

指导下，加强法规标准制定，提升安全防护能力，推动核心技术攻关，鼓励相关产业发展，培育壮大人才队伍，以工业信息安全整体能力护航制造业转型升级，以工业信息安全综合实力保障提升我国先进制造业国际竞争力，在国际格局变化和大国博弈较量中维护我国国家安全与利益。（来源：《中国信息安全》杂志 2019 年第 6 期）

➢ 美国网络安全人才队伍建设新举措

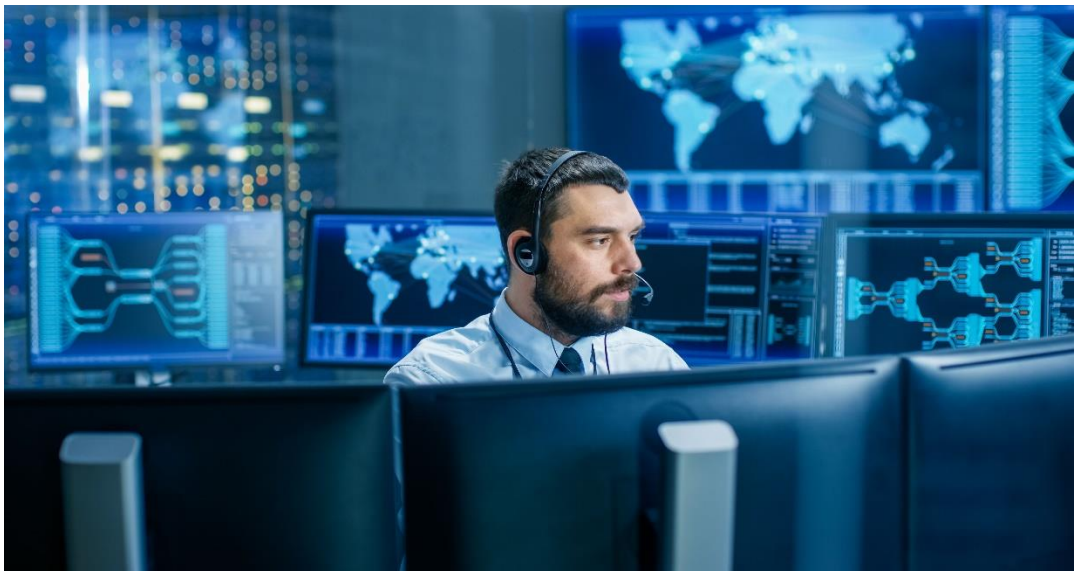
2019 年，美国通过“国家网络安全教育计划（NICE）”进行体系化的网络安全人才建设工作已进入第十个年头。5 月 2 日，美国总统特朗普签署《关于美国网络安全人才队伍的行政令》，要求在现有的网络安全教育培训工作“最大化”基础上，启动若干新的网络安全人才计划，以维持美国在网络空间的领先优势。其中最受关注的新计划包括设立联邦政府网络安全人才轮岗机制、开展“总统杯”网络安全竞赛，以及向优秀的网络安全人才颁发规格空前的“总统级”嘉奖等内容。这份最新指令显示，美国在网络安全人才队伍建设方面正在进入全面优化升级的新阶段。

一、美网络安全人才队伍建设重点新举措

最新发布的网络安全人才行政令正是特朗普针对此前提出的一系列网络安全人才相关战略、政令和表态所做的具体工作部署，其中的重点新举措主要包括以下几个方面。

1. 加强网络安全人才的流动配置力度

行政令要求，美国政府必须加强网络安全人员的流动性，以改进美国的国家网络安全。行政令称，“在网络安全从业人员的职业生涯中，他们将为不同的、多样的实体服务，承担多种角色。美国政府的政策必须促进网络安全从业人员在公共领域和私营领域之间的顺畅流动，充分发挥他们的技能、经验和才华，实现对国家贡献的最大化”。这种流动性将包括两个方面，一是在联邦政府各部门之间流动，二是在联邦政府内部和外部之间流动。在行政令发布 90 天之内，国土安全部部长应与管理预算办公室（OMB）主任和人事管理办公室（OPM）主任磋商，并向总统提交一份关于轮岗制的报告，就网络安全人员轮岗制度的计划方案、现有资源以及实施建议进行汇报。与此同时，一项关于联邦政府网络安全人员轮岗制度的法案也在参议院初步通过，其中规定网络安全专职人员可以申请派至其他部门执行为期 180 天到 1 年的临时任务。



加强人员流动性是美联邦政府为应对网络安全人才严重不足问题给出的最新解决方案。美国一直以来都在不断强调联邦政府自身网络安全人才队伍的重要性，但政府部门对网络安全人才的吸引力始终难以同私营领域竞争。网络安全人才缺口大、薪酬待遇有限、招聘流程冗长复杂、高端人才留不住等问题已成为美国网络安全人才发展工作中被诟病最多的痛点问题。在增量人才有限的情况下，美国转而在已经进入联邦政府工作的存量人才上做文章，通过轮岗使网络安全人才获得更多的练兵机会，同时使规模较小、网络安全实力有限的部门也能得到专业人士的支援。事实上，联邦政府各部门之间已经时有借调网络安全专家或团队处理网络风险管理、网络安全应急等工作的情况，未来通过行政命令和法律方式把这种轮岗制度固化后，预计将提高网络安全人才的效用，降低整体的用人成本。

2. 召开“总统杯”网络安全年度竞赛

行政令要求国土安全部部长应与国防部部长、科技政策办公室主任、OMB 主任，以及相关部门负责人磋商，制定一个针对联邦政府文职和军职雇员的“总统杯网络安全竞赛”计划。竞赛的目标是选拔、锻炼和奖励美国政府在网络安全攻、防两方面最优秀的网络安全从业人员和团队。首届竞赛应在 2019 年 12 月 31 日前举行，之后每年举行一次。按照行政令中要求开发的竞赛相关参数指标，未来的“总统杯网络安全竞赛”类别和项目都非常丰富，不仅包括个人和团体赛，还覆盖了软件逆向工程和利用、网络行动、取证、大数据分析、网络分析、网络防御、网络利用、安全编程、代码混淆、信息物理融合系统等各种竞赛项目。

开展网络安全竞赛是选拔和锻炼实战人才最直接、最有效的方法。美国军队内部有很多网络安全竞赛、网络演习、靶场等对抗演练活动。此次行政令中提出的“总统杯网络安全竞赛”独特之处在于，牵头规划的部门是国土安全部，参赛人员为来自联邦政府的各个部门军人和文职人员，包括联邦政府雇员、文职部门的军职人员，以及国防部的现役军职人员、文职人员，以及在武装部队预备役或国民警卫队中训练的预备人员，也可能会有联邦政府以外的人员直接参赛或到场观摩。该竞赛的具体方案还在规划之中，有可能会参考“全美大学生网络防御大赛”、大西洋协会“网络 9/12 战略挑战赛”等成熟竞赛的模式。如此看来，这项比赛的赛事规格、大赛规模和覆盖人群在美国公共领域都是空前的。

3. 向优秀人才颁发“总统级”嘉奖

为落实《国家网络战略》中“利用行政权重点突出和奖励人才”的要求，行政令提出“美国政府还必须对国家最优秀的从业人员和团队进行认可和奖励”。表彰和奖励的对象主要包括联邦政府内部和外部的网络安全优秀人才。对于联邦政府内的表彰，行政令要求政府各部门应确保在现有的军职和文职人员军功及奖励机制下，网络安全和网络行动领域的杰出表现也能够得到认可，包括依据 1957 年 1 月 10 日第 10694 号行政令（授权陆军、海军、空军部队的部长以美国总统之名向在行动中表现杰出的部队授奖）颁发嘉奖令，或提供同等级别的军功及奖励。在必要和适当情况下，各部门应创建新的军功及奖励，对网络安全和网络行动领域中的杰出表现和成就进行表彰。

上文中所提到的跨部门执行临时任务以及参加“总统杯网络安全竞赛”等也在网络安全嘉奖范围之内。行政令强调，总统的国家安全事务助理可向政府各部门推荐在国家安全危机、事件或工作中有重大突出表现的网络联合协调团队或类似的临时跨机构组织，提名其获得相应的军功及奖励。对于“总统杯”参赛人员，国土安全部部长正在按照行政令要求研究制定参赛激励手段，届时参赛者不仅可以获得不低于 25000 美元的现金奖励，政府各部门还将通

过颁发荣誉称号、现金奖励、休假奖励、破格晋升等方式鼓励人员积极参赛。对于联邦政府以外的奖励对象，行政令要求在 1 年之内设立一个“总统网络安全教育奖”，每年奖励小学和中学教育者各一人，并重点强调该奖项奖励的是教育者的教育成就，而非研究水平、学术水平或技术开发能力。

4. 网络安全教育培训最大化

在全国网络安全教育培训方面，行政令总的要求是要“实现网络安全人才和美国劳动者能力的最大化——尤其是在这些人才和能力有利于促进国家和经济安全的时候”，同时就几个方面进行了重点强调。一方面是强调了要优先填补国家安全和关键基础设施领域的网络安全人才缺口，“为加强国家发现和消减关键基础设施、防务系统，尤其是信息物理融合系统（其安全性和可靠性依赖于安全控制系统）中网络安全漏洞的能力”，国防部部长须牵头“确认并评估联邦政府和非联邦政府的网络安全人员技能缺口，特定关键基础设施行业、国防关键基础设施以及国防部信息技术平台的培训缺口”，并提出相关的培训建议和课程推荐。另一方面是强调了要建立最广泛的协商机制应对网络安全人才问题，“商务部部长和国土安全部部长应制定一项咨询性的工作机制，由联邦、州、属地和地方政府、学术界、私营领域利益相关方，以及其他相关方面共同就如何解决国家网络安全人才队伍需求、加强人才流动性等问题进行评估、提出对策建议”。

二、结语

特朗普政府自发布《国家网络战略》以来，明确了要“建设一支超群的网络安全人才队伍”的人才总要求。最新的人才行政令再次强调，“一支超群的网络安全人才队伍能促进美国的经济繁荣，维护和平稳定”，“无论是受雇于公共领域还是私营领域，他们都是我们国家和经济安全的卫士”。而为了建设这样一支队伍，行政令提出了多项引人关注的网络安全人才新举措。系列政令要求进一步加大已经开展的网络安全教育培训工作的力度，首先是体现了特朗普政府对前两届政府的网络安全人才工作整体继承的态度，这显示美国在涉及网络安全人才问题时政策比较统一，也少有党派争议，已经形成了很强的共识；其次是就一些长期以来尚未得到解决的人才痛点问题做出了新的部署，尤其是联邦政府部门网络安全人才缺口大、招聘难的问题，提出了“轮岗制”的要求，其实施效果值得关注；第三是就特朗普《国家网络战略》中关于加强人才奖励的要求快速响应，提出了要开展“总统杯”网络安全竞赛、颁发系列“总统级”嘉奖等要求，如此旗帜鲜明地对网络安全优秀人才进行表彰和奖励必然能极大地提升从事网络安全工作的荣誉感，具体能在多大程度上增加公共领域的人才吸引力同样值得关注。（来源:《中国信息安全》杂志 2019 年第 5 期）

四、政府之声

➢ 四部委联合开展互联网网站安全专项整治，将处罚并曝光违法违规网站

2019 年 6 月 11 日，中央网信办、工业和信息化部、公安部、市场监管总局四部门于 2019 年 5 月至 2019 年 12 月，联合开展全国范围的互联网网站安全专项整治工作，对未备案或备案信息不准确的网站进行清理，对攻击网站的违法犯罪行为进行严厉打击，对违法违规网站进行处罚和公开曝光。

此次专项整治的一大特点是加大对未履行网络安全义务，发生事件的网站开办者的处罚力度，督促其切实落实安全防护责任，加强网站安全管理和防护。各地通信管理局、公安机关将根据《网络安全法》，对落实网络安全义务不到位，发生网页篡改、被植入后门木马、大量公民个人信息被窃取等网络安全事件，以及存在非法获取、出售或提供个人信息等行为的网站，依据情节严重程度，采取约谈主要负责人、停业整顿、关闭网站、注销备案等措施并公开曝光，涉企行政处罚信息将依法纳入市场监管总局国家企业信用信息公示系统予以公示。专项整治期间，各地通信管理局、公安机关还将责令未按照有关规定进行 ICP 备案、联网备案或备案信息不准确的网站限期整改，对拒不整改的进行清理。公安机关将对非法入侵控制网站牟取利益或从事非法活动，非法提供入侵控制网站工具，买卖网站数据和控制权限，窃取买卖个人信息等违法犯罪活动和网络黑产行为，组织开展专项打击。各地网信部门统筹协调本地区专项整治工作。

对于当前互联网网站安全状况以及如何有效提升网站的防护水平，记者采访了有关专家。国家计算机网络应急技术处理协调中心（简称“CNCERT”）有关负责人介绍，近年来，攻击篡改、植入后门、数据窃取等危害互联网网站安全的行为呈现快速增长趋势。据 CNCERT 抽样监测发现，2019 年前 4 个月我境内被篡改的网站 8,213 个，同比增长 48.8%；被植入后门的网站 10,010 个，同比增长 22.5%。同时，近期发现由于运营者安全配置不当，很多数据库直接暴露在互联网上，导致大量用户个人信息泄露。造成这些事件很大原因是一些互联网网站运营者网络安全意识不强，特别是中小网站安全管理和防护能力较低，缺乏有效安全保障措施，成为网络攻击的重点目标和主要入口。

国家工业信息安全发展研究中心检查评估所副所长于盟介绍，采用云防护方式是当前有效快速提升网站防护能力的手段。云防护一般通过 DNS 流量牵引将网站访问引流到分布式的云防护清洗中心进行安全检测及拦截，再将安全流量回注到网站服务器，无需部署硬件设备、无需调整业务结构及网络拓扑，具有部署快速简便、及时防护最新漏洞、全网协同防御等特点，而且费用比较经济。国家信安标委组织制定了《信息安全技术网站安全云防护平台技术要求》等标准对云防护服务商进行规范引导。

专项整治期间，中央网信办将加强统筹协调，指导有关部门做好信息共享、协同配合。坚持依法依规，坚持防慑并举，促使网站运营者网络安全意识和防护能力有效提升，实现网站安全形势取得明显改观，迎接新中国成立 70 周年。（来源：网信中国）

➢ 国家互联网信息办公室发布《个人信息出境安全评估办法（征求意见稿）》

2019 年 6 月 13 日，为保障个人信息安全，维护网络空间主权、国家安全、社会公共利益，保护公民、法人的合法权益，依据《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有关部门起草了《个人信息出境安全评估办法（征求意见稿）》，现向社会公开征求意见。

根据《征求意见稿》，网络运营者向境外提供在中华人民共和国境内运营中收集的个人信息（以下称个人信息出境），应当按照本办法进行安全评估。经安全评估认定个人信息出境可能影响国家安全、损害公共利益，或者难以有效保障个人信息安全的，不得出境。（来源：国家互联网信息办公室）

- **《个人信息出境安全评估办法（征求意见稿）》**

- 全文：http://www.cac.gov.cn/2019-06/13/c_1124613618.htm

➢ 八部门发布《关于印发 2019 网络市场监管专项行动(网剑行动)方案的通知》

2019 年 6 月 17 日，市场监管总局、工信部等 8 部门发布《关于印发 2019 网络市场监管专项行动(网剑行动)方案的通知》。通知指出，严格海外代购行为监管，加大对跨境电商进出口环节整治力度。加强对网络销售禁止交易商品的监测监管工作，不断净化网络市场环境。

通知明确，充分发挥网络市场监管部际联席会议作用，严格贯彻落实《电子商务法》有关规定，严厉打击网络市场突出问题，营造公平竞争的市场秩序。坚持依法依规监管、审慎监管、智慧监管、综合监管和协同监管，强化信用约束，规范电子商务行为，净化交易环境，保护消费者和经营者合法权益，提升网络商品和服务质量，促进电子商务持续健康发展。

通知要求，着力规范电子商务主体资格，营造良好准入环境。依法查处电子商务经营者违反《电子商务法》第十五条规定的信息公示义务的行为。监督电子商务经营者依法办理市场主体登记，规范电子商务主体资格，加强对社交电商、跨境电商经营者的规范引导。督促电子商务平台经营者按照《电子商务法》等法律法规要求登记备案，对进入平台的经营者真实信息进行核验、登记，建立登记档案，监督电子商务经营者做好亮照、亮证、亮标工作。督促邮政企业、快递企业加强对电子商务企业协议客户经营范围的审查。规范电子商务经营主体，集中整治非法主体互联网应用(网站、APP 等)。

通知指出，严厉打击网上销售假冒伪劣产品、不安全食品及假药劣药，营造放心消费环境。以食品(含保健食品)、药品、电子产品、汽车配件、家具家装、家庭日用品、儿童用品、服装鞋帽以及劳动防护安全帽等社会反映集中、关系健康安全的消费品为重点，加强监管执

法和刑事司法，以大要案为突破口，组织开展集中打击，坚决守住人民生命健康和安全的底线。坚持线上线下治理相结合，加强流通销售餐饮环节食品等商品抽查，加强网络餐饮服务食品安全监管，加强风险监测，净化生产源头，依法查处利用互联网销售假冒伪劣商品违法犯罪活动。依法依规处置互联网侵权假冒有害信息。

通知提出，严厉打击不正当竞争行为，营造公平竞争的市场环境。按照《反不正当竞争法》《电子商务法》等相关规定，严厉打击网络虚假宣传、刷单炒信、违规促销、违法搭售等行为。严肃查处违规推销宣传婴幼儿配方食品的行为。严厉打击通过组织非法寄递空包裹等方式，帮助其他经营者进行刷单炒信等违法行为。督促电子商务平台经营者进一步加强对刷单炒信行为的监测监控，完善商品(服务)信用评价体系，配合执法工作开展。依法查处电子商务平台经营者限制平台内经营者参与其他第三方电子商务平台经营活动等行为。

通知明确，深入开展互联网广告整治工作，营造良好广告市场环境。以社会影响大、覆盖面广的门户网站、搜索引擎、电子商务平台为重点，突出移动客户端和新媒体账户等互联网媒介，针对医疗、药品、保健食品、房地产、金融投资理财等关系人民群众身体健康和财产安全的虚假违法广告，加大案件查处力度，查办一批大案要案。

通知指出，依法打击其他各类网络交易违法行为，有效净化网络市场环境。落实《电子商务法》《网络安全法》《消费者权益保护法》《价格法》《网络购买商品七日无理由退货暂行办法》等相关规定，畅通消费投诉举报渠道，保护消费者知情权和选择权，加大对不正当价格行为、不公平格式条款、不依法履行七日无理由退货义务等侵害消费者权益行为的打击力度。全方位多渠道加大个人信息保护力度，规范涉及个人信息的合同格式条款；严肃查处未经同意收集、使用、过度收集或泄露、非法出售、非法向他人提供个人信息行为，依法查处不履行个人信息保护义务、为网络违法犯罪提供支持帮助的网络平台；严厉打击侵犯公民个人信息犯罪，切实防范大数据技术对个人信息的滥用。依法严厉打击网络交易平台为违法出售、购买、利用野生动物及其制品或者禁止使用的猎捕工具提供交易服务的行为。密切协作配合，加强对手机 APP 端(网络交易平台、网络订餐平台、在线旅游平台、社交电商、跨境电商以及其他网络市场新模式新业态)违法犯罪行为的研判、监管和打击查处。加大对网络销售单用途商业预付卡违规行为的查处力度。严格海外代购行为监管，加大对跨境电商进出口环节整治力度。加强对网络销售禁止交易商品的监测监管工作，不断净化网络市场环境。

通知要求，强化网络交易信息监测和产品质量抽查，营造良好消费环境。不断强化监管技术应用，探索应用网络交易信息监测的新方式，完善监测监管流程，有效发现网络交易违法线索。重点关注网络集中促销期、节假日等重要时间节点，开展网络市场定向监测和产品

质量抽检，及时发现风险，发挥部门失信联合惩戒作用，实施全网警示。

通知提出，落实电子商务经营者责任，营造诚信守法经营环境。督促电子商务经营者特别是平台经营者履行法定责任和义务。监督电子商务经营者履行消费者权益、知识产权、个人信息保护等方面的义务，依法承担产品和服务质量责任，严格落实网络销售商品修理更换退货责任。指导和督促电子商务平台经营者加强对平台内经营者的资格审查、主体信息公示，落实知识产权保护“通知—删除”义务、显著标明竞价排名商品(服务)为“广告”义务；指导和督促网络餐饮服务平台加强分支机构、代理商、合作商管理，主动向监管部门报送平台入网餐饮服务提供者数据和平台分支机构、代理商、合作商等信息，加强餐食配送过程管理，逐步推动外卖餐食封签，确保食品配送过程不受污染。指导和督促配送、邮政、快递等企业完善实名制，拒绝接收、寄递侵权假冒商品，为执法部门核查违法犯罪线索提供支持。（来源：国家市场监管总局）

- **市场监管总局等部门关于印发 2019 网络市场监管专项行动（网剑行动）方案的通知**
- **全文：**http://gkml.samr.gov.cn/nsjg/wjs/201906/t20190620_302494.html

➢ 工信部公开征求《网络安全漏洞管理规定（征求意见稿）》

2019 年 6 月 18 日，工业和信息化部为贯彻落实《中华人民共和国网络安全法》，加强网络安全漏洞管理，工业和信息化部会同有关部门起草了《网络安全漏洞管理规定（征求意见稿）》（见附件），拟以规范性文件形式印发，现面向社会公开征求意见。

如有意见或建议，请于 2019 年 7 月 18 日前反馈。（来源：工业和信息化部网络安全管理局）

- **《网络安全漏洞管理规定（征求意见稿）》全文：**
- http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057724/n3057728/c7005976/content.html

五、本期重要漏洞实例

➢ IBM Tririga 应用平台未名信息泄露

发布日期：2019-06-21
更新日期：2019-06-21
受影响系统：
IBM Tririga Application Platform 3.6.0.2
IBM Tririga Application Platform 3.6.0.1
IBM Tririga Application Platform 3.6
IBM Tririga Application Platform 3.5.3.5
IBM Tririga Application Platform 3.5.3.3
IBM Tririga Application Platform 3.5.3
不受影响系统：
IBM Tririga Application Platform 3.6.0.3
IBM Tririga Application Platform 3.5.3.6
描述：

BUGTRAQ ID: 108843
CVE(CAN) ID: CVE-2018-2008
IBM TRIRIGA Application Platform 是美国 IBM 公司的一套用于部署 TRIRIGA 应用的技术平台。该平台提供了一组设计时和运行时组件，分别用于构建和运行其企业级应用，并支持客户特定的配置，而无需更改源代码。
IBM TRIRIGA Application Platform 3.5.3 和 3.6.0 可以向经过身份验证的用户披露敏感信息。
攻击者可以利用此问题获取对敏感信息的访问权限；这可能会导致进一步的攻击。
<*来源：思科
链接：https://www-01.ibm.com/support/docview.wss?uid=ibm10879463
建议：

厂商补丁：
IBM
IBM 已经为此发布了一个安全公告（IBM 10879463）以及相应补丁：
IBM 10879463：IBM TRIRIGA Application Platform could disclose sensitive information
链接：https://www-01.ibm.com/support/docview.wss?uid=ibm10879463

➢ Juniper Junos 远程拒绝服务漏洞

发布日期：2019-06-19
更新日期：2019-06-19
受影响系统：
Juniper Networks JUNOS 18.2R1

Juniper Networks JUNOS 18.2

不受影响系统：

Juniper Networks JUNOS 18.2R2

Juniper Networks JUNOS 18.2R1-S2

描述：

BUGTRAQ ID: 108490

CVE(CAN) ID: CVE-2019-0041

Junos OS 是 Juniper Networks 硬件路由器中使用的基于 FreeBSD 的操作系统。它是 Juniper 网络路由，交换和安全设备中使用的操作系统。

在应用了任何 lo0 过滤器的 EX4300-MP 系列设备上，传输网络流量可能通过环回接口（lo0）到达控制平面。设备可能无法转发此类流量。此问题影响到 18.2R1-S2 之前的 Juniper 网络公司 Junos OS 18.2 版本，EX4300-MP 系列的 18.2R2 版本。此问题不会影响任何其他 EX 系列设备。

攻击者可以利用此问题导致拒绝服务情况，从而有效地拒绝向合法用户提供服务。

<*来源：Juniper

链接：https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10933

*>

建议：

厂商补丁：Juniper Networks

Juniper Networks 已经为此发布了一个安全公告（JSA10933）以及相应补丁:

JSA10933：Junos OS: EX4300-MP Series: IP transit traffic can reach the control plane via loopback interface

链接：https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10933

➢ WordPress Mobile App Builder By Wappress 插件任意文件上传漏洞

发布日期：2019-06-19

更新日期：2019-06-19

受影响系统：

WordPress mobile-app-builder-by-wappress 1.05

描述：

BUGTRAQ ID: 96905

CVE(CAN) ID: CVE-2017-1002000/CVE-2017-1002001

WordPress 是一个以 PHP 和 MySQL 为平台的自由开源的博客软件和内容管理系统。

CVE-2017-1002000：wordpress 插件中的漏洞 mobile-friendly-app-builder-by-easytouch v3.0，文件中的代码./mobile-friendly-app-builder-by-easytouch/server/images.php 不需要身份验证或检查允许用户上传内容。

CVE-2017-1002001：wordpress 插件中的漏洞 mobile-app-builder-by-wappress v1.05，该插件包含来自 http://www.invedion.com 的未经许可的易受攻击的 CMS 软件。

攻击者可以利用此问题上载任意代码并在 Web 服务器进程的上下文中运行它。这可能有助于未经授权访

问该应用程序; 其他攻击也是可能的。
<*来源：Larry W. Cashdollar （lwc@vapid.dhs.org）
*>
建议：

厂商补丁：WordPress
目前厂商还没有提供补丁或者升级程序，我们建议使用此软件的用户随时关注厂商的主页以获取最新版本：
http://wordpress.org/

➢ Oracle 数据库服务器多个本地安全漏洞

发布日期：2019-06-12
更新日期：2019-06-18
受影响系统：
Oracle Database 18c
Oracle Database 12c Release 2 12.2.0.1
Oracle Database 12c Release 1 12.1 2
Oracle Database 11g Release 2 11.2.0.4
描述：

BUGTRAQ ID: 107940
CVE(CAN) ID: CVE-2019-2516/CVE-2019-2619
Oracle 数据库系统是美国 Oracle 公司（甲骨文）提供的以分布式数据库为核心的一组软件产品，是目前最流行的客户/服务器(CLIENT/SERVER)或 B/S（Browser/Server）体系结构的数据库之一。CVE-2019-2516：Oracle Database Server 的 Portable Clusterware 组件中的漏洞。受影响的受支持版本为 11.2.0.4,12.1.0.2,12.2.0.1 和 18c。易于利用的漏洞允许具有 Grid Infrastructure User 权限的高权限攻击者登录到 Portable Clusterware 执行的基础架构以破坏 Portable Clusterware。虽然此漏洞存在于 Portable Clusterware 中，但攻击可能会对其他产品产生重大影响。成功攻击此漏洞可能导致接管 Portable Clusterware。CVE-2019-2619：Oracle Database Server 的 Portable Clusterware 组件中的漏洞。受影响的受支持版本为 11.2.0.4,12.1.0.2,12.2.0.1 和 18c。易于利用的漏洞允许具有 Grid Infrastructure User 权限的高权限攻击者登录到 Portable Clusterware 执行的基础架构以破坏 Portable Clusterware。虽然此漏洞存在于 Portable Clusterware 中，但攻击可能会对其他产品产生重大影响。成功攻击此漏洞可能导致接管 Portable Clusterware。
<*来源：Oracle
链接：https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html
*>
建议：

厂商补丁：Oracle
Oracle 已经为此发布了一个安全公告（CVE-2019-2516/CVE-2019-2619）以及相应补丁:
CVE-2019-2516/CVE-2019-2619：Oracle Critical Patch Update Advisory - April 2019
链接：https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html

六、本期网络安全事件

➢ CBP 分包商出现重大数据泄露 5 万美国车牌信息在暗网出售

2019 年 6 月 18 日，援引美国有线电视新闻网（CNN）报道，美国海关和边境保护局（CBP）所雇佣的分包商 Perceptics 出现重大数据泄露事件，在对已经泄露的数据分析后发现至少有 5 万名美国车牌号码数据在暗网上被销售。更为重要的是，CBP 向 CNN 透露从未向该公司授权保留这些车主信息。

CBP 机构发言人表示：“CBP 并未授权承包商在非 CBP 系统上保留和持有车牌数据。”这项承认引发了一系列质疑，包括美国政府机构在雇佣承包商来监视公民的时候责任主体是谁？美国公民自由联盟的高级立法律师 Neema Singh Guliani 表示：“CBP 不断以隐私和公民自由的角度来收集更多信息，而且从安全的角度来看，他们已经证明了这些承包商没有能力可以保护好这些信息。”

CNN 对分包商 Perceptics 泄露的数据进行了分析，这些数据目前已经在暗网上进行出售。它显示了至少 5 万个独特的美国车牌号码记录。在特定情况下，CBP 承包商有权访问美国人的车牌图像以调整他们的系统，例如当州颁布新的车牌设计并且系统需要校准它时。但这些时期很短暂。 “这些数据确实必须删除，”CBP 发言人表示，尽管该机构没有澄清适用于 Perceptics 的政策细节。（来源：美国有线电视新闻网）

➢ 阿根廷因电力互联系统大规模故障全国大停电

2019 年 6 月 17 日，据《纽约时报》6 月 16 日报道，阿根廷和乌拉圭 16 日发生全国大停电，社交媒体用户称，巴西部分地区、巴拉圭和智利也受到波及。

当地时间 16 日 7 点 50 分，阿根廷电力公司 Edesur Argentina 在推特表示，“由于电力互联系统大规模故障，导致阿根廷和乌拉圭全境停电。”乌拉圭乌特电力公司表示，“阿根廷电网的一个故障影响了相连接的系统，导致整个国家以及邻国几个省份无法供电，该系统于当地时间早上 7 点 06 分发生故障。”

阿根廷能源国务秘书处发布公告称，目前约有 4800 万人受到停电影响，预计需要数小时的时间才能全面恢复供电。阿根廷民防副国务秘书处官员表示，目前阿根廷南部已有部分地区正在恢复供电。

6 月 16 日，在阿根廷布宜诺斯艾利斯，市民发动发电机以应对停电。6 月 16 日，在阿根廷布宜诺斯艾利斯，市民使用应急灯照明。 由于是周日，两国市民的生活并没有受到太大的影响。不过当天在阿根廷有四个省要进行省长选举，预计选举过程将会因此受到延误。阿根廷国内地铁、城铁等交通暂时停运。不过，布宜诺斯艾利斯市两大机场在停电后启用了备用电机，目前运转正常。

目前，两国的电力公司都已经开始了抢修工作。阿根廷电力公司表示，如此大规模的停电情况在历史上尚属首次，在 9 时 40 分左右首都布宜诺斯艾利斯以及周边地区已经开始逐渐恢复供电。乌拉圭电力公司也表示从 10 时 30 分开始，南部沿海和首都地区已经逐渐开始恢复供电，不过抢修的难度大，需要几个小时的时间，希望人们保持耐心。

6 月 16 日，在阿根廷布宜诺斯艾利斯，市民等待电力供应恢复。6 月 16 日，在阿根廷布宜诺斯艾利斯，市民点蜡烛应对停电。

有社交媒体用户称，这起停电也扩散到巴拉圭和巴西南部。一名阿根廷能源部官员表示，停电的影响范围和程度还不清楚，停电原因也仍待厘清。Edesur Argentina 公司简介显示，该公司有超过 2500 万名客户。巴西 2009 年也发生过大停电，当时巴西最大的伊泰普水电站 3 条输电线路故障，影响数千万人，也暴露了该国电力建设的脆弱。伊泰普水电站位于巴西和巴拉圭交界的巴拉那河上，是周边国家电力的重要来源。（来源：互联网综合整理）

➢ 黑客“撞库”破解抖音百万账户密码，两月获利上百万元

2019 年 6 月 21 日北京日报报道，撞库，是黑客圈的术语，即网络黑客将互联网上已泄露的账号密码，拿到其他网站批量登录，从而“撞出”其他网站的账号密码。由于许多网民习惯多个网站使用一个账号密码，所以“撞库”有着不低的成功率。海淀警方近日就抓获了一名利用撞库技术非法盗取网络用户信息进行牟利的嫌疑人汪某。

今年 2 月，海淀公安分局双榆树派出所接到辖区北京字节跳动公司报案，称其公司旗下抖音 APP 遭人恶意撞库达上千万账户密码，其中上百万账户密码被黑客撞出。为防止黑客利用撞出账户实施不法行为，公司通过安全系统对所有疑似被盗账号设置了二次登录验证。

接到报警后，警方立刻展开侦查，并迅速锁定了一名湖北籍男子汪某。5 月 22 日，民警远赴湖北将汪某抓获归案，并起获了其作案时使用的笔记本电脑。

经讯问，汪某交代，毕业后一直无业，便利用掌握的计算机技术，编写了大量撞库代码，对目前网络上比较热门的社交平台进行撞库，然后控制撞库获取的账户，在网上承接点赞刷量、发布广告等业务牟利，短短两个月的时间就获利上百万元。

目前，汪某因涉嫌非法获取计算机信息系统数据罪已被海淀警方依法刑事拘留，案件正在进一步审理中。

警方提示：“净网 2019”专项行动将侵犯公民个人信息、黑客攻击破坏等网络违法犯罪行为列为打击重点。互联网不是法外之地，警方将坚决打击网络违法犯罪活动，维护网络空间的清朗、安全、有序。同时，广大网民在使用互联网时要提高安全防范意识，加强个人信息保护，以防被不法分子窃取。（来源：北京日报）

➢ 夫妻联合百余黑客攻击国内公司敲诈解密费获利 700 余万

2019 年 6 月 21 日，记者从武汉市公安局江汉分局了解到，该局历经 3 个月的侦查，破获一起网络敲诈案，广东一对夫妻在深圳注册两家公司联合黑客攻击国内多家公司的电脑，以解密为由索利，先后获利 700 余万元。21 日，2 名犯罪嫌疑人被民警从深圳押解到武汉，目前案件正在进一步调查。

2019 年 3 月 23 日，武汉市公安局江汉公安分局王家墩派出所接到 CBD 商务区某科技

公司报案称，黑客攻击了该公司电脑，索要 25000 元解密费用。

江汉分局网安大队副大队长陈哲联手刑侦民警侦查。经与黑客在网上联系周旋，黑客在网上发来深圳某科技计算机服务公司的邮箱、手机等联系方式，民警拨通该公司电话后，接电话男子语气坚决，要求先支付钱款再帮解密。

民警进一步侦查得知，3 月 27 日湖南长沙某销售公司，也遭遇黑客攻击，被以同样的方式敲诈费用，支付给深圳某科技计算机公司 22000 元后，才得以解开密。江汉分局民警收集大量证据确认，两年中深圳这家公司与 100 余黑客签订了合作协议。

6 月 19 日，江汉分局刑警大队、网安大队、王家墩派出所联手武汉市网安支队 12 人赶赴深圳，设法摸清该公司详细地址和人员组成，并在该公司各个出入道口设哨布守后，进入公司将 2 名犯罪嫌疑人抓获。

据民警介绍，鲁正(化名)36 岁，妻子覃瑛(化名)32 岁，均系广东人。两年前，夫妻 2 人在深圳开了两家科技计算机服务公司，由黑客对客户实施网络攻击，并留下邮箱等联系方式。待客户与黑客联系后，黑客再将鲁正公司的邮箱、手机号码等联系方式发给对方，由鲁正等人负责解密并敲诈钱财。

民警称，鲁正与妻子覃瑛分工很明确，鲁正与客户签解密合同，并通过网络进行远程解密，其妻则负责收款。两年多来，他们共敲诈客户获利 700 余万元。目前，此案还在进一步调查中。（来源：新京报）

➢ 世界最大飞机零件供应商惨遭勒索病毒四个工厂停产

2019 年 6 月 13 日据报道：世界上最大的飞机零部件供应商 ASCO，由于其位于比利时扎芬特姆的工厂报告遭勒索软件感染，已停止在四个国家的工厂生产。由于被勒索软件感染导致 IT 系统瘫痪，该公司已将 1,400 名工人中的大约 1,000 人送回家带薪休假。

根据报告：感染于 6 月 7 日星期五生根，最初袭击了比利时公司的 Zaventem 工厂，但 ASCO 也关闭了德国，加拿大和美国的工厂。位于法国和巴西的非生产办事处未受影响。目前还不清楚该公司是否关闭其他工厂的运营，因为勒索软件可能具有横向传播功能，如果不是因为勒索软件具有内网传播功能，那么关闭工厂可能只是作为预防措施从而关闭。

ASCO 是世界上最重要的飞机零部件设计供应商之一。该公司的一些客户包括航空运输和军事领域的大腕，如空中客车公司，波音公司，庞巴迪公司和洛克希德马丁公司。ASCO 制造的零件用于 F-35 战斗机，空中客车 A400M 军用飞机，空中客车和波音商用客机以及阿丽亚娜太空发射火箭，仅举几例。感染该公司比利时工厂的勒索软件名称尚未公开。

目前还不清楚 ASCO 是否已支付赎金以恢复其系统的访问权限，从备份中恢复，或从头开始购买新系统和重建其计算机网络，就像过去一些其他被勒索攻击的公司所做的那样。这充分说明了，目前的飞机零件制造工厂，均是采用互联网智能化管理模式进行批量生产，往往是机器流水线，而人在其中是与自动化设备合作进行，因此两者缺一不可。

那么，在工业互联网时代，我们如何保障网络安全呢?目前来看智能化工厂安全以及设施设备保护将是制造商需要考虑的重要问题。具体问题如下：

一、工业互联网在生产过程中会生成大量的数据，这些数据基本是从机器和组件收集而来，并且通常可以远程访问和进行分析。

二、随着 IT 和 OT(运营技术)的结合渐密，工控系统因此更加容易受到攻击。

而目前，经过研究发现，攻击制造业主要有几个目的：

1、修改程序来破坏生产流程，导致系统停机，像本次攻击飞机零件供应商就是这一目的

2、获取私人专利数据

3、勒索钱财

4、国家级攻击

因此在工业互网时代，黑客可能恶意攻击工业控制系统以及可编程逻辑控制器，企业需要了解自身能力和系统的局限性，以形成全面的网络安全战略，从而确保数据、信息和知识产权得到正确的保护。例如，一些传统设备可能成为网络犯罪分子的目标，因为这些设备设计目的不是连接到互联网，增加网络连接意味会有安全隐患。

因此建议通过以下几点完善规章制度：

首先是评估工厂的数字化过程，了解所收集和存储的数据。在更新或升级系统时，必须考虑整个数据的封装，这包括核算任何个人设备，如智能手机、平板电脑和有权访问网络的笔记本电脑。其次，制造企业必须采取主动的网络安全措施。这包括安装有效的防火墙，进行网络监控等等。通过密切关注网络中的活动，将任何不寻常的活动标记为可疑，帮助更快地发现风险。

还有，公司应该考虑分割不同部门的网络，除非必要的情况下开放权限，其它不必要的就限制对网络的访问。因为连接点越多，风险就越大，所以分段网络可以限制数据泄露时的损害。（来源：互联网综合整理）

➢ 西太平洋银行支付平台 PayID 遭网络攻击十万客户信息泄露

2019 年 6 月 5 日，西太平洋银行(Westpac)的实时支付平台 PayID 系统遭网络攻击，近 10 万客户的私人信息泄露。这次袭击行为还会影响到其它银行的客户。计算机安全专家警告，这些被窃取的私人信息可能会被用于欺诈。

PayID 平台允许客户使用手机号码或电子邮件地址在银行之间进行即时转账。许多澳洲人并不知道，PayID 就像一本电话号码簿，任何人祇要输入手机号码或电子邮件地址，就能查出其相应银行账户持有人的姓名。这就让黑客有机会进行，安全专家称之为的“枚举攻

击”(即逐个列举)。在这种攻击下，黑客可以随机输入数字以查获成千上万澳洲人的姓名和手机电话号码。

安全专家表示，得到这些细节，黑客即可进行大规模的欺诈活动。西太平洋银行 3 日(周一)晚证实了这一事件，但没有透露有多少人受到影响。

西太平洋银行发言人说：“本银行可以证实，我们发现(新支付平台)PayID 的功能被滥用，我们采取了额外的预防措施，但不包括系统关闭。”“结果是没有客户的银行账号被泄露。”发言人说，“目前还没有发现进一步的不当活动。”根据悉尼晨锋报获得的一份机密备忘录，西太平洋银行向澳洲银行业和金融业披露了有关这次网攻事件的信息。其中说：“2019 年 5 月 22 日，西太平洋银行注意到，澳洲支付平台 PayID(NPPA PayID)的大量查询(约 60 万个)来自七个被泄露的西太平洋银行有效账户，约 9.8 万个查询成功解析了一个短名字，并暴露给了欺诈者。”

运营西太平洋银行新支付平台的澳洲支付平台公司的一位女发言人表示，“我们不能就个别银行及他们层次上的任何问题发表置评。”隐私专员不愿证实此事。其一位女发言人说：“根据我们的监管行动政策，我们一般不对具体事件发表评论。”

澳洲安全顾问亨特(Troy Hunt)表示:“PayID 平台的便利性是显而易见的，”“不太清楚的是，使用该平台的用户是否愿意以隐私为代价。我怀疑大多数人并没有意识到他们的个人信息已以这种方式被泄露。（来源：新浪科技）

信息安全意识产品免费大赠送

isa@spisec.com