奇安信
新一代网络安全领军者

2021 工业互联网安全发展与实践分析报告

工业控制系统安全国家地方联合工程实验室

奇安信行业安全研究中心

2021 年 4 月

主要观点

- ✧ 工业系统安全漏洞数量增长显著放缓，但超高危漏洞数量却大幅增加。统计显示，2021年，国内外四大漏洞平台共计新收录工业系统安全漏洞636个，较2020年的804个下降了20.9%。但新增超高危漏洞多达16个，比2020年的6个，大幅增长了166.7%。

- ✧ 被新报告安全漏洞数量最多的 10 家工业系统供应商均为国外企业。其中，仅西门子（Siemens）一家就被报告新增安全漏洞193个，占到全年新增工业系统安全漏洞总量的30.3%。国外供应商对国内工业互联网安全的影响仍然十分巨大。

- ✧ 在与工业互联网相关的各个行业中，制造业面临的网络安全风险最大：88.7%的新增工业系统安全漏洞会对制造业产生影响；奇安信安服团队全年处置的90起与工业互联网安全相关的应急响应事件中，46.7%发生在制造业。工业网络软件的安全漏洞、勒索病毒等，对制造业的网络安全威胁最大。

- ✧ 勒索软件仍然是工业互联网网络安全的最大威胁，国内、国外工业机构都深受其害。工业勒索事件占到了奇安信安服团队全年处置工业互联网安全应急响应事件的57.6%。此外，数据安全问题也是困扰工业互联网发展的重要威胁，42.1%的工业系统网络安全应急响应事件与数据安全问题密切相关。

- ✧ 2021年，从中央到地方，密集出台了多项涉及工业互联网安全的政策法规及安全标准，工业互联网安全监管体系不断完善。

- ✧ 2021年智能网联汽车发展迅速，车联网安全关注度显著增加。同时，5G+工业互联网应用的广度和深度不断拓展，安全风险也随之增多。5G+工业互联网安全能力亟需提升。

摘　　要

- 2021 年，四大漏洞平台共收录工业系统安全漏洞 636 个，较 2020 年的 804 个下降了 20.9%；收录工业系统超高危漏洞 16 个，较 2020 年（6 个）增长了 166.7%，占年度四大漏洞平台收录工业系统漏洞总数的 2.51%。
- 工业控制系统安全漏洞多数分布在制造业、能源、水务、商业设施、石化、医疗、交通、农业、信息技术、航空等关键基础设施行业。其中，有 564 个漏洞涉及到制造业。
- 2021 年，奇安信安服团队共处置国内的网络安全事件多达 1097 起，与工业互联网相关的安全事件 90 起，占比 8.2%。从行业来看，制造业 42 次，交通运输 29 次，能源行业 13 次，化学工业 3 次。其中，57.6%的事件为工业勒索事件，42.1%的事件与工业数据安全相关。
- 2021 年工业互联网安全政策法规标准体系不断完善，出台 9 个相关的政策法律法规文件。
- 2021 年智能网联汽车发展迅速，车联网安全关注度显著增加。
- 5G+工业互联网安全能力亟需提升，表现在技术融合带来新风险、安全运营能力不足、数据采集难度增加、供应链安全能力不足、国产化进程需加快等多个方面。

关键词：安全漏洞、制造业、勒索攻击、工业数据、车联网、5G+工业互联网

目　　录

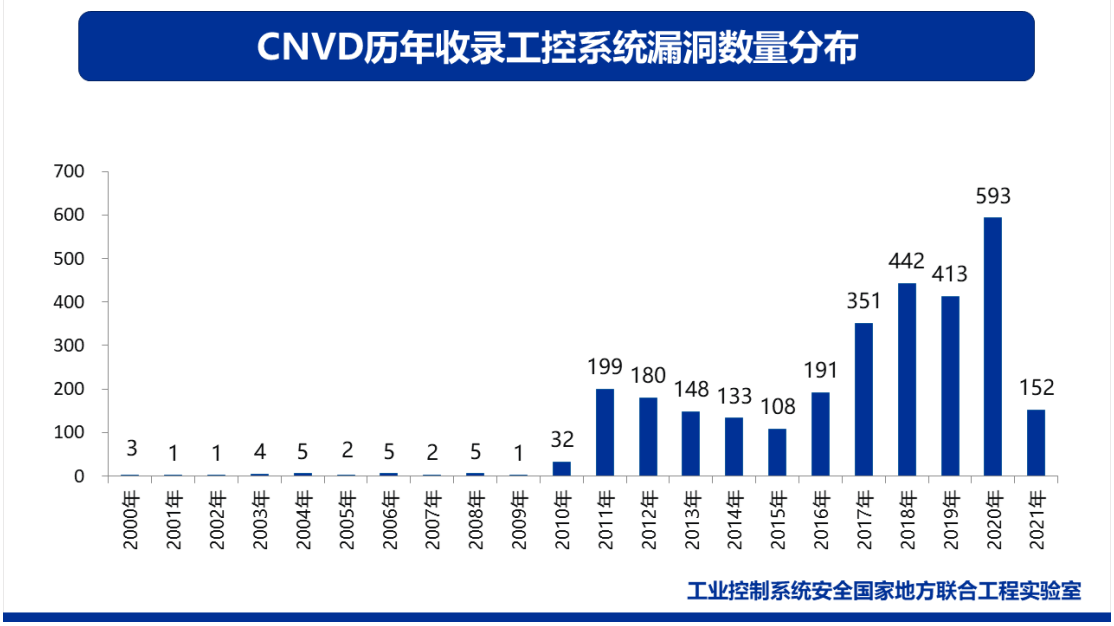
第一章　工业互联网安全态势

本章内容主要以工业控制系统安全国家地方联合工程实验室（以下简称：联合实验室）漏洞库收录的工业控制系统相关的漏洞信息和奇安信安服团队处理的工业安全应急事件统计数据为基础，从工控漏洞的年度变化趋势、等级危害、漏洞类型、漏洞涉及行业、漏洞设备类型等方面和工业应急处理事件的行业分布、事件类型、损失类型等方面分析工业互联网的安全威胁态势、脆弱性以及发展变化趋势。

一、　安全漏洞形势分析

（一） 工业互联网安全漏洞总体态势

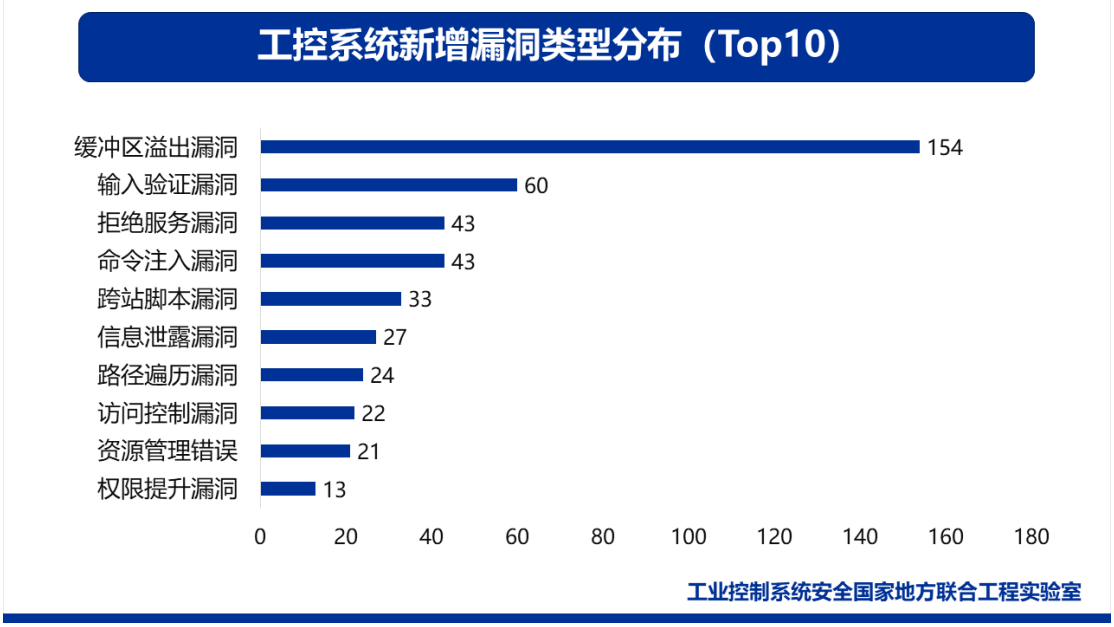
根据中国国家信息安全漏洞共享平台最新统计，截止到 2021 年底，CNVD 收录的与工业控制系统相关的漏洞高达 3103 个，2021 年新增的工业控制系统漏洞数量达到 152 个，较 2020 年 593 个下降 74.4%。2000-2021 年 CNVD 工控新增漏洞年度分布如下所示：



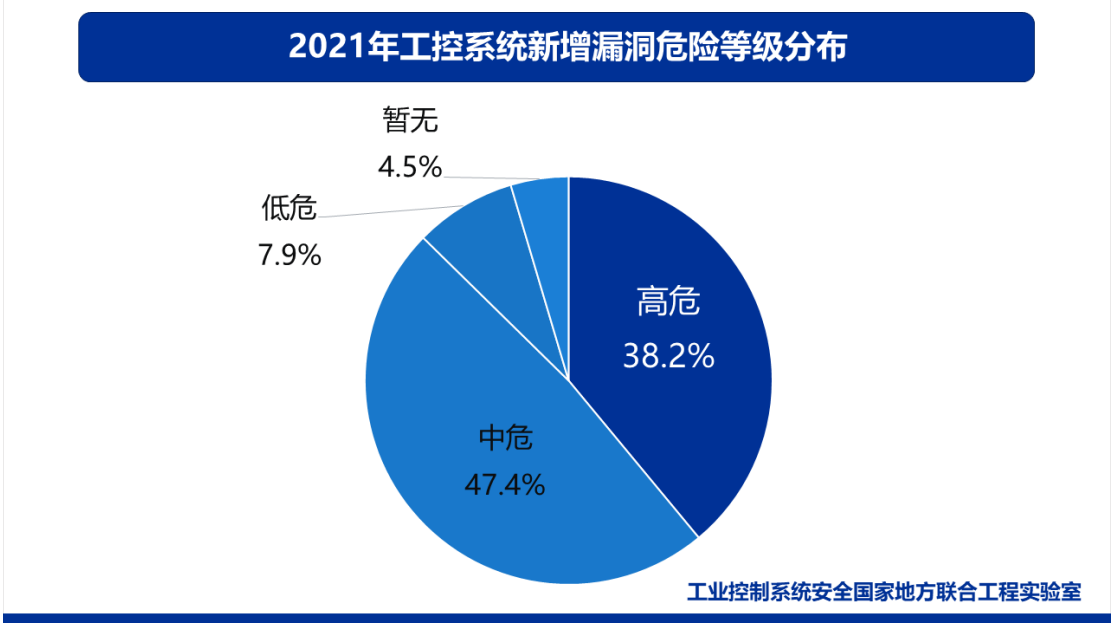
综合参考了 Common Vulnerabilities & Exposures（CVE）、National Vulnerability Database（NVD）、中国国家信息安全漏洞共享平台（CNVD）及国家信息安全漏洞库（CNNVD）（以下简称“四大漏洞平台”）所发布的漏洞信息来看， 2021 年，四大漏洞平台共收录的工业系统安全漏洞 636 个，较 2020 年的 804 个下降了 20.9%。

新增工业系统安全漏洞的成因多样化特征依然明显，技术类型多达 30 种以上。其中，

缓冲区溢出漏洞（154）、输入验证漏洞（60）和拒绝服务漏洞（43）数量最多。2021 年工控系统新增漏洞类型分布如下：

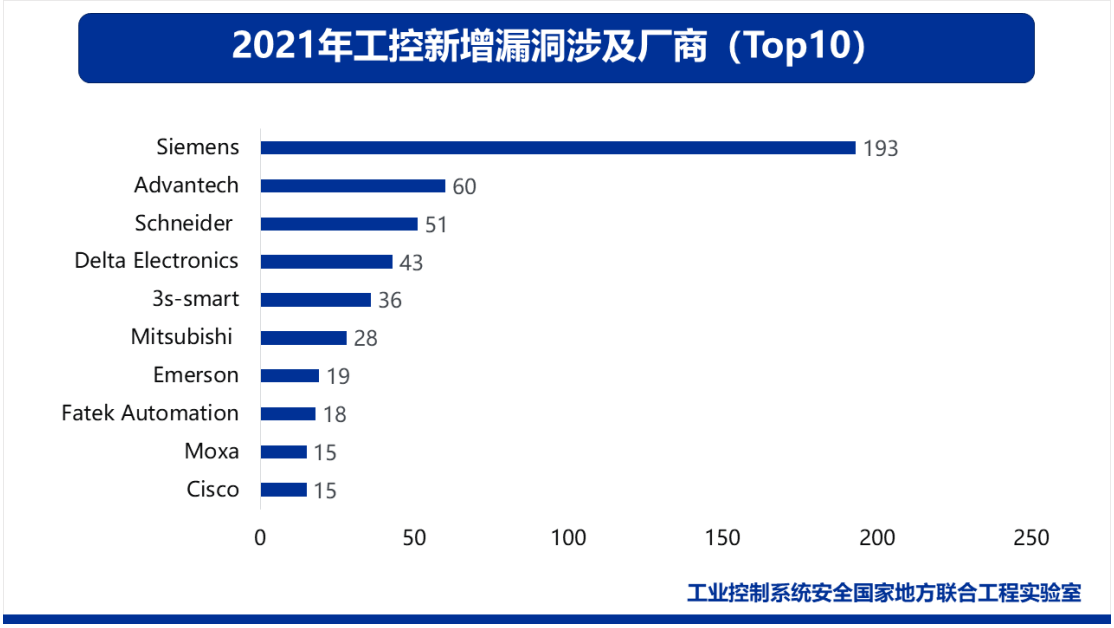


在四大漏洞平台收录的工业系统漏洞中，高危漏洞占比 38.2%，中危漏洞占比为 47.4%，中高危漏洞占比高达 85.6%。工业控制系统多应用于国家关键基础设施，一旦遭受网络攻击，会造成较为严重的损失。2021 年工控系统新增漏洞危险等级分布如下：



在收录的工业控制系统漏洞中，涉及到的前十大工控厂商分别为西门子（Siemens）、研华（Advantech）、施耐德（Schneider）、台达电子（Delta Electronics）、3S-Smart、三菱（Mitsubishi）、艾默生（Emerson）、永宏电机（Fatek Automation）、摩莎（Moxa）和思科

（Cisco）。2021 年工控新增漏洞涉及主要厂商情况如下图所示：

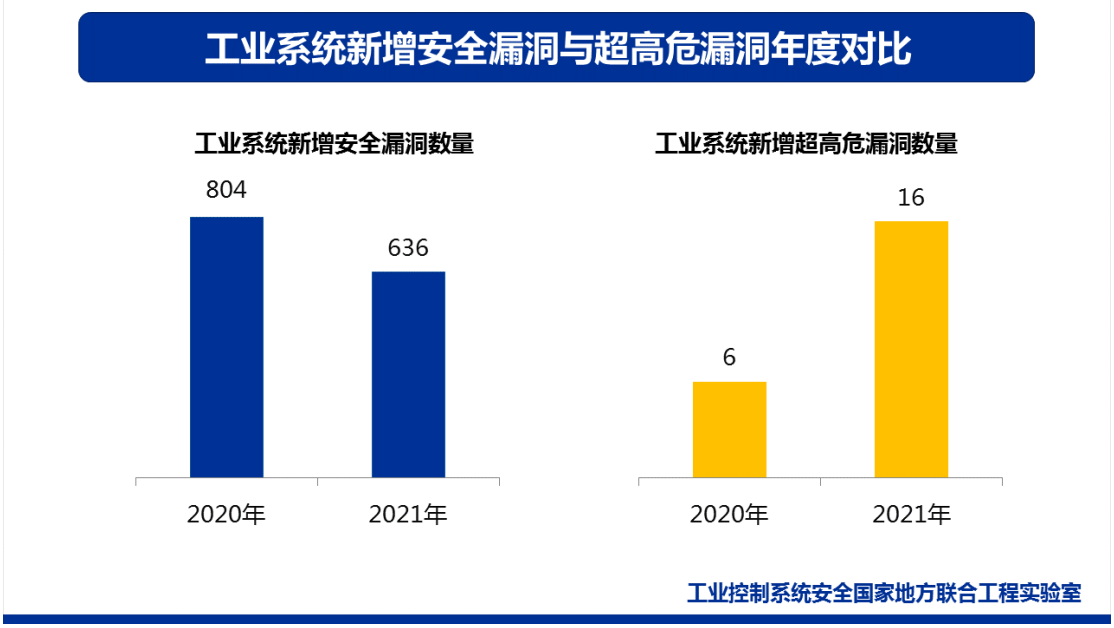


需要说明的是，虽然安全漏洞在一定程度上反映了工控系统的脆弱性，但不能仅通过被报告的厂商安全漏洞数量来片面判断比较厂商产品的安全性。因为一般来说，一个厂商的产品越是使用广泛，越会受到更多安全研究者的关注，因此被发现安全漏洞的可能性也越大。某种程度上来说，安全漏洞报告的厂商分布，更多程度上反映的是研究者的关注度。

（二） 工业超高危漏洞明显增加

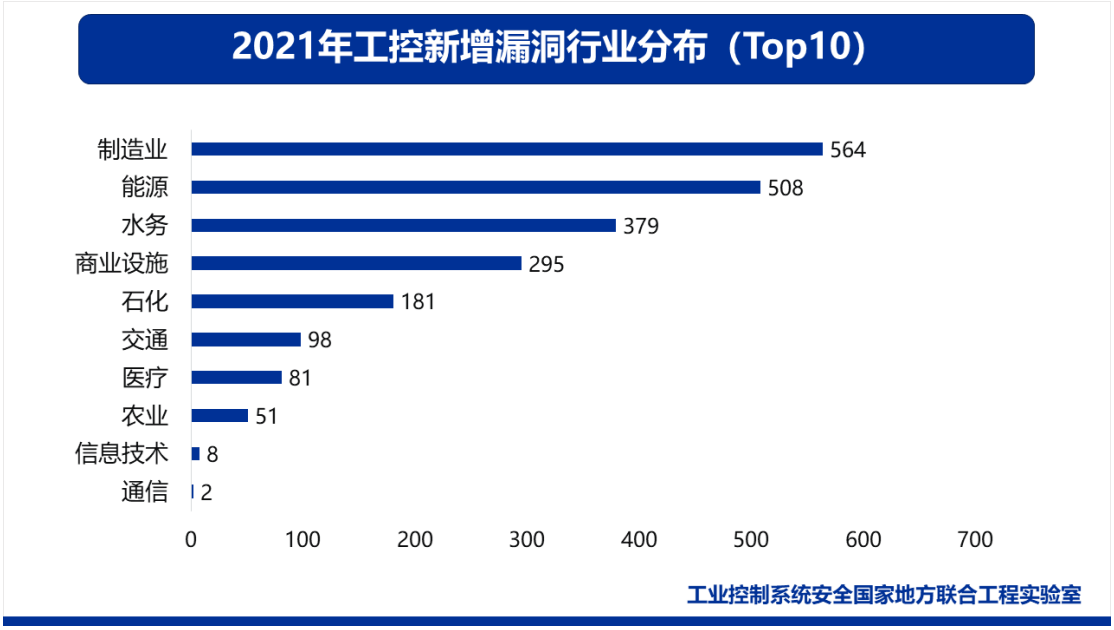
漏洞库平台根据 CVSS 分级标准对漏洞进行 0 至 10 之间的数字评分，10 分为最高分，表示该漏洞的严重程度最高，我们称之为超高危漏洞，一旦被攻击者利用，就可能造成的重大损失和严重后果。

尽管 2021 年新增工业系统安全漏洞的总数较 2020 有明显下降，但超高危漏洞的数量却显著上升。统计显示，2021 年四大漏洞平台共收录工业系统超高危漏洞 16 个，较 2020 年（6 个）增长了 166.7%，占年度四大漏洞平台收录工业系统漏洞总数的 2.51%。2021 年新收录的超高危漏洞详细信息见附录二。



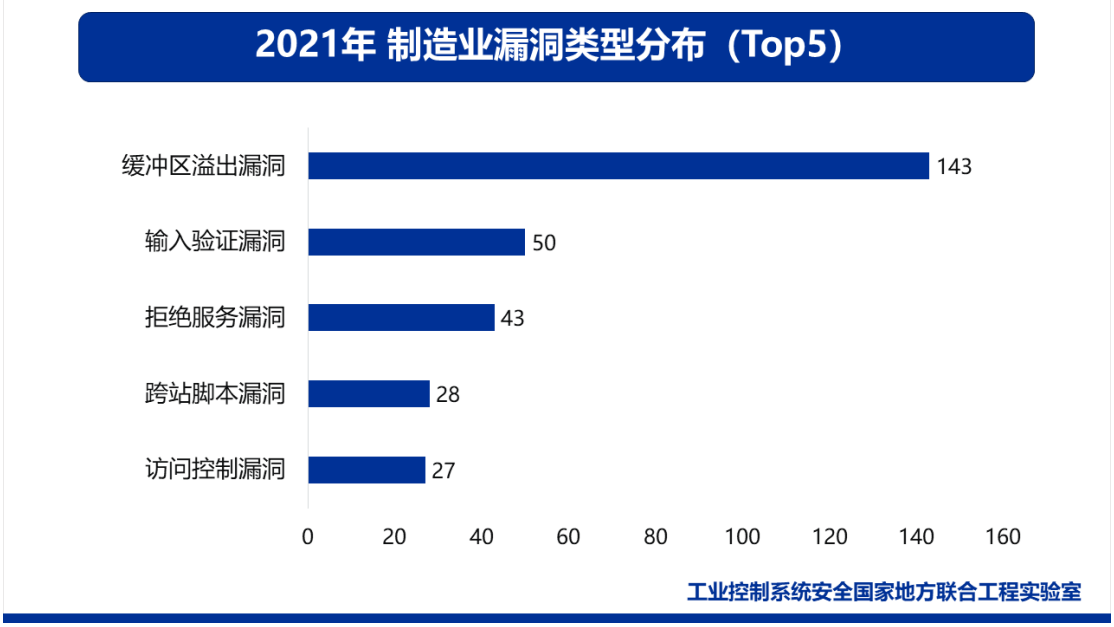
（三） 涉及制造业的漏洞仍然最多

四大漏洞平台收录的工业控制系统安全漏洞多数分布在制造业、能源、水务、商业设施、石化、医疗、交通、农业、信息技术、航空等关键基础设施行业。一个漏洞可能涉及多个行业，在 636 个漏洞中，有 564 个漏洞涉及到制造业，也是占比最高的行业。涉及到的能源行业漏洞数量高达 508 个。对比 2020 年的数据，依然是制造业和能源行业工控漏洞较多，应持续加强这两个行业工业安全建设。2021 年工控新增漏洞行业分布图如下：

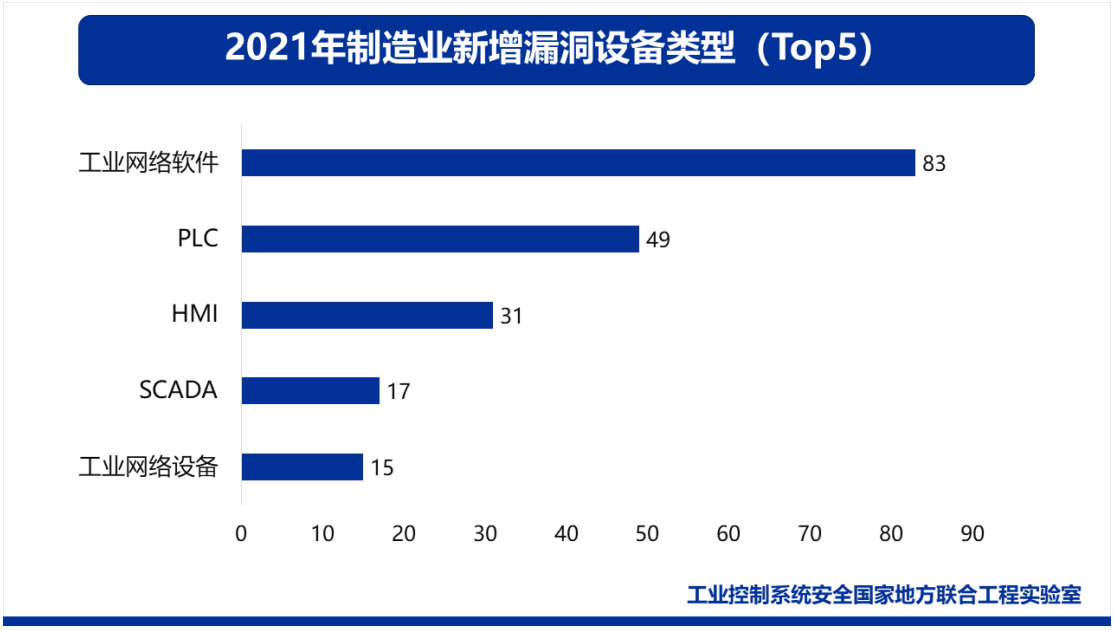


对 2021 年新增的与制造业相关的安全漏洞做进一步统计分析发现，缓冲区溢出漏洞

（143 个）、输入验证漏洞（50 个）、拒绝服务漏洞（43 个）、跨站脚本漏洞（28 个）、访问控制漏洞（27 个）最为常见。2021 年制造业新增漏洞类型分布如下：



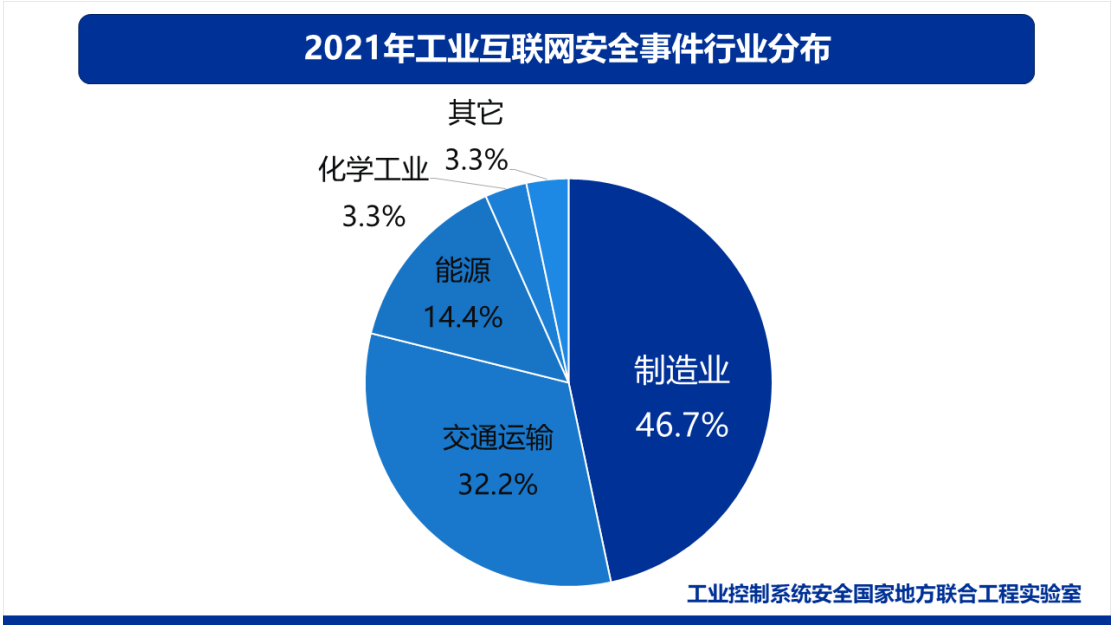
针对制造业控制系统设备，按照 PLC、SCADA、RTU、HMI、工业网络设备、工业网络软件、普通软件、其他进行设备分类，涉及到的前五大设备漏洞中，工业网络软件最多，数量为 83 个，PLC 设备（49 个）、HMI（31 个）、SCADA（17 个）、工业网络设备（15 个）。制造业新增漏洞设备类型数据如下：



二、 应急响应形势分析

（一） 应急响应事件行业分析

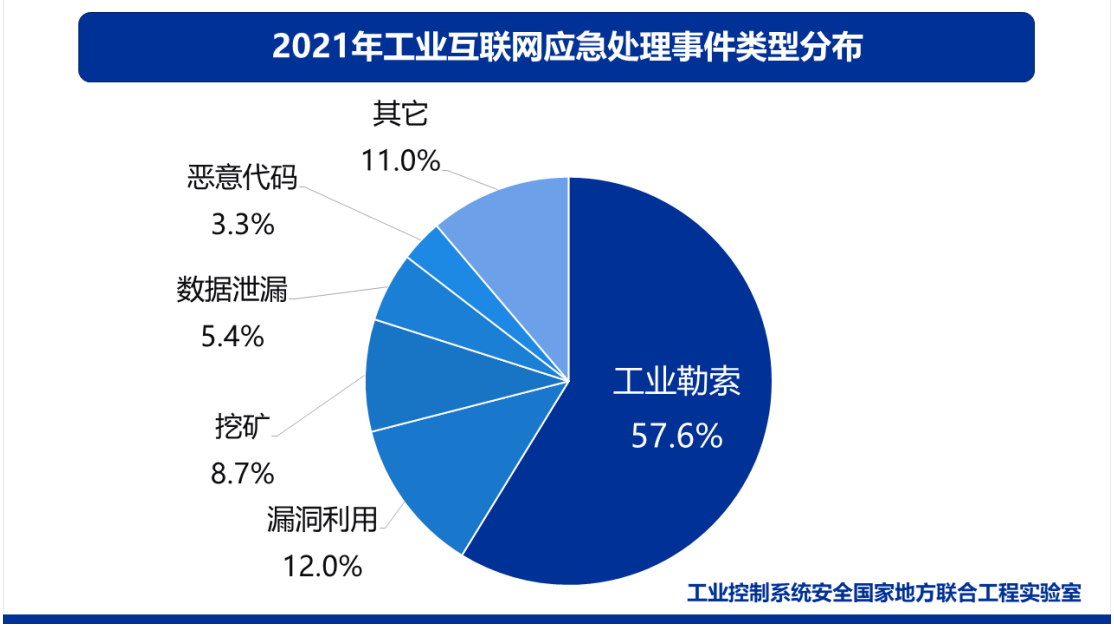
2021 年，奇安信安服团队共处置国内的网络安全事件多达 1097 起，与工业互联网相关的安全事件 90 起，占比 8.2%。统计这些工业互联网安全事件的行业分布，其中制造业 42 次，交通运输 29 次，能源行业 13 次，化学工业 3 次。工业互联网安全事件行业分布如下图所示：



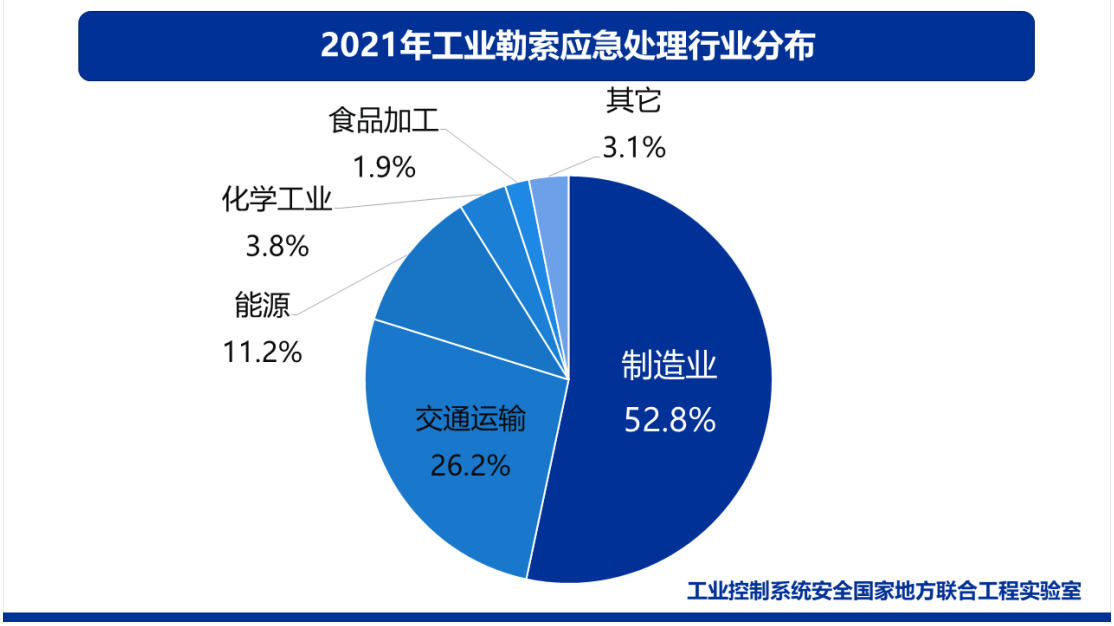
从这些安全事件的统计数据表明中国工业互联网安全形势依然严峻，特别是制造业的安全防护能力薄弱，安全事件高发。需要提高整个行业的安全防范意识，加强日常安全巡检制度，定期对系统配置、网络设备及安全策略进行检查，主动发现目前系统、应用存在的安全隐患，保障工业互联网的安全稳健运行。

（二） 工业勒索成制造业最大威胁

从攻击类型上看，在 2021 年奇安信安服团队处置的 90 起应急响应事件中，勒索事件占比最高，达到了 57.6%，如下图所示。由此可见，针对工业系统的勒索攻击是当前国内工业企业最大的网络安全威胁。

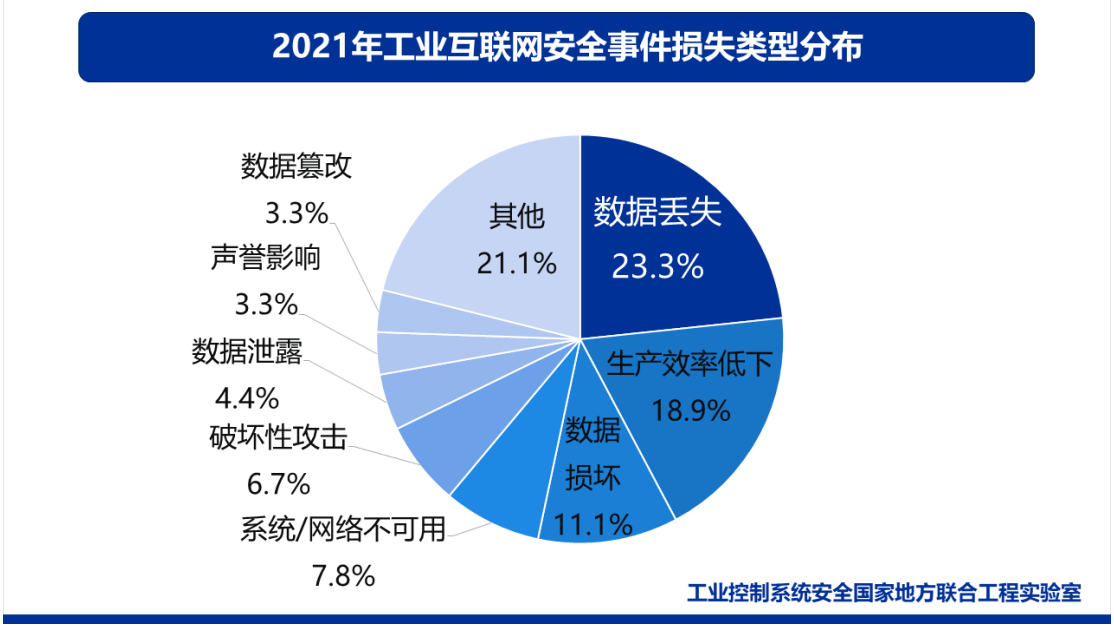


针对所有勒索攻击引发的工业互联网应急响应事件进行行业分析发现，制造业仍然占比最高，达到了 52.8%，如下图所示。



（三） 数据安全成工业互联网新痛点

从应急响应事件的损失类型来看，直接与工业数据相关的事件占比达到了 42.1%，包括数据丢失（23.3%）、数据损坏（11.1%）、数据泄漏（4.4%）、数据篡改（3.3%）。另外，系统/网络不可用（7.8%）和破坏性攻击（6.7%）也会间接导致工业数据的安全问题。具体分布如下图所示：



数据安全问题，不仅困扰着国内工业企业，从公开报道上来看，国外企业也深受其害。

2021 年 3 月 16 日，能源巨头壳牌公司（Shell）遭遇黑客攻击。攻击者利用了安全厂商 Accellion 的文件传输程序 FTA 的零日漏洞，访问了一些个人数据以及属于壳牌利益相关方和子公司的数据，导致严重的数据泄漏。

2021 年 5 月，大众汽车集团美国公司（VWGoA）披露了一起数据泄露事件，表示他们的一家供应商曾在 2019 年 8 月至 2021 年 5 月期间在互联网上泄露大量未受保护的客户数据。这批泄露的数据主要影响到美国及加拿大多家奥迪与大众授权经销商的 330 万购车客户。

2021 年 7 月，ZeroX 恶意团伙从沙特阿美石油公司盗窃 1TB 专有数据，开价 500 万美元在暗网上出售。

2021 年 10 月 26 日，伊朗油气系统遭到严重的网络攻击。网络攻击引起的软件故障扰乱了伊朗全国各地的加油站，导致加油站的加油系统中断，并且破坏了加油泵屏幕和天然气价格广告牌，在广告牌上显示与政治相关的内容。这次攻击影响了 NIOPDC 的 IT 网络，而 NIOPDC 是伊朗一家管理着 3500 多个加油站的国有天然气分销公司。攻击涉及使用一种前所未见的可重复使用的数据擦除恶意软件“Meteor”。

第二章　政策法规建设与发展

自 2017 年 12 月，工业互联网创新发展战略实施以来，我国工业互联网创新发展战略稳步推进，成效显著。2021 年是“十四五”开局之年，我国工业互联网创新发展新格局加速构建，政策法规和技术标准体系进一步健全完善，展现出新型工业化进程的强劲动力和壮阔前景。

一、　工业互联网安全政策体系不断完善

（一） 工业互联网创新发展行动计划（2021-2023 年）

2021 年 1 月，为深入实施工业互联网创新发展战略，推动工业化和信息化在更广范围、更深程度、更高水平上融合发展，工信部工业互联网专项工作组制定《工业互联网创新发展行动计划（2021-2023 年）》。

行动计划中明确安全发展目标：安全保障能力进一步增强。工业互联网企业网络安全分类分级管理有效实施，聚焦重点工业领域打造 200 家贯标示范企业和 100 个优秀解决方案。培育一批综合实力强的安全服务龙头企业，打造一批工业互联网安全创新示范园区。基本建成覆盖全网、多方联动、运行高效的工业互联网安全技术监测服务体系。

（二） 工业互联网企业网络安全分类分级管理指南（试行）

2021 年 1 月，为进一步加强工业互联网网络安全管理，提升工业互联网企业网络安全水平，工信部开展工业互联网企业网络安全分类分级试点工作，发布《工业互联网企业网络安全分类分级管理指南（试行）》。

通过试点，进一步完善工业互联网企业网络安全分类分级规则标准、定级流程以及工业互联网安全系列防护规范的科学性、有效性和可操作性，加快构建工业互联网企业网络安全分类分级管理制度；进一步落实试点企业网络安全主体责任，形成可复制可推广的工业互联网网络安全分类分级管理模式；总结一批工业互联网网络安全典型解决方案，选拔一批优秀示范企业、培育一批专业服务机构。

（三） 工业互联网标识管理办法

2021 年 1 月 19 日，工信部发布《工业互联网标识管理办法》（工信部信管〔2020〕204 号）。《办法》要求标识服务机构应当落实网络与信息安全保障措施，具备相应的技术、服务和网络安全保障能力和专业人员，并明确专门的责任部门与责任人。还应当建立网络安全防护技术手段，依法记录并留存相关日志记录，保障标识服务系统安全。

（四） 中华人民共和国数据安全法

2021 年 6 月 10 日，《中华人民共和国数据安全法》由中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议正式表决通过，2021 年 9 月 1 日正式实施，标志我国在数据安全领域有法可依，为各行业数据安全提供监管依据。《数据安全法》的出台，我国在网络与信息安全领域的法律法规体系得到了进一步的完善。按照总体国家安全观的要求，《数据安全法》明确数据安全主管机构的监管职责，建立健全数据安全协同治理体系，提高数据安全保障能力，促进数据出境安全和自由流动，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益，让数据安全有法可依、有章可循，为数字化经济的安全健康发展提供了有力支撑。该法律的公布施行，为工业互联网领域的数据安全防护提供了直接有力的法律依据。

（五） 关键信息基础设施安全保护条例

2021 年 8 月 17 日，《关键信息基础设施安全保护条例》（以下简称“条例”）正式发布，2021 年 9 月 1 日起施行。条例详细阐明了关键信息基础设施的范围、运营者应履行的职责以及对产品和服务的要求。明确公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等属于基础设施范围。条例旨在通过配套立法进一步明确关键信息基础设施安全保护的具体要求，保障国家关键信息基础设施安全。

（六） 物联网新型基础设施建设三年行动计划（2021-2023 年）

2021 年 9 月 27 日，工信部、网信办等八部委联合发布《物联网新型基础设施建设三年行动计划（2021-2023 年）》（工信部联科〔2021〕130 号）。《行动计划》要求加快物联网安全监测、预警分析和应对处置技术手段建设，加快物联网领域商用密码技术和产品的应用推广，开展物联网基础安全“百企千款”产品培育计划，建设安全公共服务平台，开展安全能力评估，加速推进全面感知、泛在连接、安全可信的物联网新型基础设施建设。

（七） 物联网基础安全标准体系建设指南（2021 版）

2021 年 10 月 25 日，工信部发布《物联网基础安全标准体系建设指南（2021 版）》（工信厅科〔2021〕34 号）。《指南》要求，围绕物联网基础设施和重点行业应用，加快推进基础通用、关键技术、试验方法等重点和急需标准制定，及时满足物联网产业的安全需求。提出了物联网基础安全标准体系包括总体安全、终端安全、网关安全、平台安全、安全管理等五大类标准。

（八） 工业领域数据安全管理试点

2021 年 12 月 14 日，工信部发布关于组织开展工业领域数据安全管理试点工作的通知。该试点工作是贯彻落实《中华人民共和国数据安全法》《中华人民共和国网络安全法》等法律法规在工业领域的具体落实，目标是指导省级工业和信息化主管部门组织开展数据安全管理试点，督促企业落实数据安全主体责任，加强数据分类分级管理、安全防护、安全评估、安全监测等工作，提升数据安全防护能力。加强试点成果转化应用，完善工业领域数据安全制度规范和工作机制，遴选一批示范企业、优秀产品和典型解决方案，形成可复制可推广的管理模式，促进提升行业数据安全保护水平。

（九） 工业互联网综合标准化体系建设指南（2021 版）

2021 年 12 月 24 日，工信部、国家标准化管理委员会联合发布《工业互联网综合标准化体系建设指南（2021 版）》（工信部联科〔2021〕291 号）。《指南》从工业互联网技术与产业发展现状出发，提出了进一步建立健全，加快构建统一、融合、开放的工业互联网标准体系的总体要求，明确了工业互联网标准体系包括基础共性、网络、边缘计算、平台、安全、应用等六大部分，并分别给出了具体的标准建设内容。

二、 工业互联网安全标准体系不断健全

建立健全的工业互联网安全标准体系对网络安全建设具有重要的指导意义。通过工业互联网安全标准体系的建设，可有效提高对工业网络安全风险的管控能力，通过与等级保护等工作接续起来，使得工业网络安全管理更加科学有效。同时，网络安全标准体系的建立将使得企业安全实施水平与国际先进水平接轨，从而加快工业网络安全的落实。2021 年新发布了多项与工业互联网安全相关的国家标准。

2021 年 10 月，国家标准**《信息安全技术 安全处理器技术要求》**发布，标准号：GB/T 40653-2021，归口单位为全国信息安全标准化技术委员会。本标准规定了安全处理器的安全功能要求和安全保障要求。本标准适用于安全处理器设计、生产和应用。

2021 年 10 月，国家标准**《信息安全技术 恶意软件事件预防和处理指南》**发布，标准号：GB/T 40652-2021，归口单位为全国信息安全标准化技术委员会。本标准在 GB/T 20985.1—2017 和 GB/T 20985.2—2020 的基础之上，针对恶意软件事件的预防和处理过程给出了进一步指南。本标准适用于计算机系统管理人员、网络管理人员、安全事件响应小组等预防和处理恶意软件事件。

2021 年 10 月，国家标准**《信息安全技术 工业控制系统安全防护技术要求和测试评价**

方法》发布，标准号：GB/T 40813-2021，归口单位为全国信息安全标准化技术委员会。本标准规定了工业控制系统安全防护技术要求、保障要求和测试评价方法。本标准适用于工业控制系统建设、运营、维护等。

2021 年 10 月，国家标准**《工业自动化和控制系统安全 IACS 服务提供商的安全程序要求》**发布，标准号：GB/T 40682-2021，归口单位全国工业过程测量控制和自动化标准化技术委员会。本标准定义了在自动化解决方案的集成和维护活动中 IACS 服务提供商可以向资产所有者提供的安全能力的一系列综合要求。

2021 年 5 月，国家标准**《工业通信网络 网络和系统安全 术语、概念和模型》**发布，标准号：GB/T 40211-2021，归口单位全国工业过程测量控制和自动化标准化技术委员会。本标准关注工业自动化和控制系统的安全，“工业自动化和控制系统”（IACS）包括了用于制造业和流程工业的控制系统、楼宇控制系统、地理上分散的操作诸如公共设施（例如:电力天然气和供水）管道和石油生产及分配设施、其他工业和应用如交通运输网络,那些使用自动化的或远程被控制或监视的资产。本标准中的术语“安全”是指防止非法或有害的渗透,有意或无意的妨碍正常的和预期的运行、或不适宜的访问 IACS 的保密信息。

2021 年 5 月，国家标准**《工业通信网络 网络和系统安全 工业自动化和控制系统信息安全技术》**发布，标准号：GB/T 40218-2021，归口单位全国工业过程测量控制和自动化标准化技术委员会。大部分的电子安全技术和计算机入侵防范措施都适用于 IACS 环境。本标准列举了几类计算机信息安全技术和防范措施并针对每一类具体讨论其所处理的脆弱性部署的建议及其已知的优点和弱点。另外，本标准提供了对当前许多类型的电子计算机安全技术、缓解措施和工具的评价和评估，这些用于保护 IACS 环境以防不利的计算机入侵和攻击。本标准中的网络安全指南是通用一般性的视人员知识在工业自动化系统中的应用而定，并且应根据适用的、特定的工业自动化系统人员知识正确适用于每一个控制系统和网络。

2021 年 3 月，国家标准**《信息技术 安全技术 网络安全 第 5 部分：使用虚拟专用网的跨网通信安全保护》**发布，标准号：GB/T 25068.5-2021，归口单位全国信息安全标准化技术委员会。本标准规定了使用虚拟专用网（VPN）连接到互联网和将远程用户连接到网络上的安全要求，以及在使用 VPN 提供网络安全时所必需的控制技术的选择、实施和监控指南。本部分适用于在使用 VPN 时负责选择和实施提供网络安全所必须的技术控制人员，以及负责随后的 VPN 安全的网络监督人员。

2021 年 2 月，国家标准**《网络关键设备安全通用要求》**发布，标准号：GB 40050-2021，归口单位工业和信息化部。本标准规定了网络关键设备的通用安全功能要求和安全保障要

求。本标准适用于网络关键设备，为网络运营者采购网络关键设备时提供依据，还适用于指导网络关键设备的研发、测试、服务等工作。

第三章　工业互联网应急响应典型案例

本章节选取 2021 年奇安信安服团队处理过的众多工业互联网安全应急响应事件中具有代表性的几个案例。

一、　某地铁公司遭蠕虫病毒攻击

2021 年 10 月 31 日，某一线城市地铁运营公司发现多台主机终端中病毒无法上传文件，紧急向奇安信安服团队求助，希望尽快排查并溯源。

应急响应中心专家通过对受害主机进行上机排查，经过对受害主机中提取的病毒样本以及对既往处置过案例的案例中，研究发现本次病毒事件系中永恒之蓝下载器的变种木马之一。排查系统日志，发现受害主机被内网其他受害主机攻击，但因客户处存在还原盘等设置，会删除过往日志，导致部分受害主机无法追溯到攻击者，溯源工作无法继续推进。

通过对本次永恒之蓝下载器变种木马进行处置分析，造成安全事件的原因主要包括以下几点：

1) 系统无防病毒软件；

2) 系统存在弱口令；

3) 网络缺乏有效的隔离机制；

4) 系统开放无用的 SMB 共享端口；

二、　某汽车制造企业遭勒索病毒攻击

2021 年 10 月 4 日，奇安信安服团队接到某汽车制造企业的应急求助，其内网发现大量服务器中勒索病毒，导致业务系统无法正常运行。

应急响应中心专家通过对受害主机进行上机排查，发现勒索病毒最早由 VPN 线路进入内网，攻击者在最初的目标留下勒索信后不满足于成功又攻击了域控获取了域内的权限进行了更大范围的勒索病毒扩散，最终在 9 月 29 日 5 点 10 分发布勒索信。因为大部分主机的日志已被清除，且无流量监控设备和主机监控设备，进一步溯源被限制。

三、　某半导体材料企业遭受挖矿病毒攻击

2021 年 9 月 9 日，某半导体材料企业自行发现入侵迹象，及时断开互联网连接，自行通过赛门铁克对中毒机器进行杀毒，但大部分机器已无法运行赛门铁克；2021 年 9 月 10 日上午奇安信安服团队接到应急请求，经现场排查发现是中了蠕虫挖矿病毒范围 400 台左右。

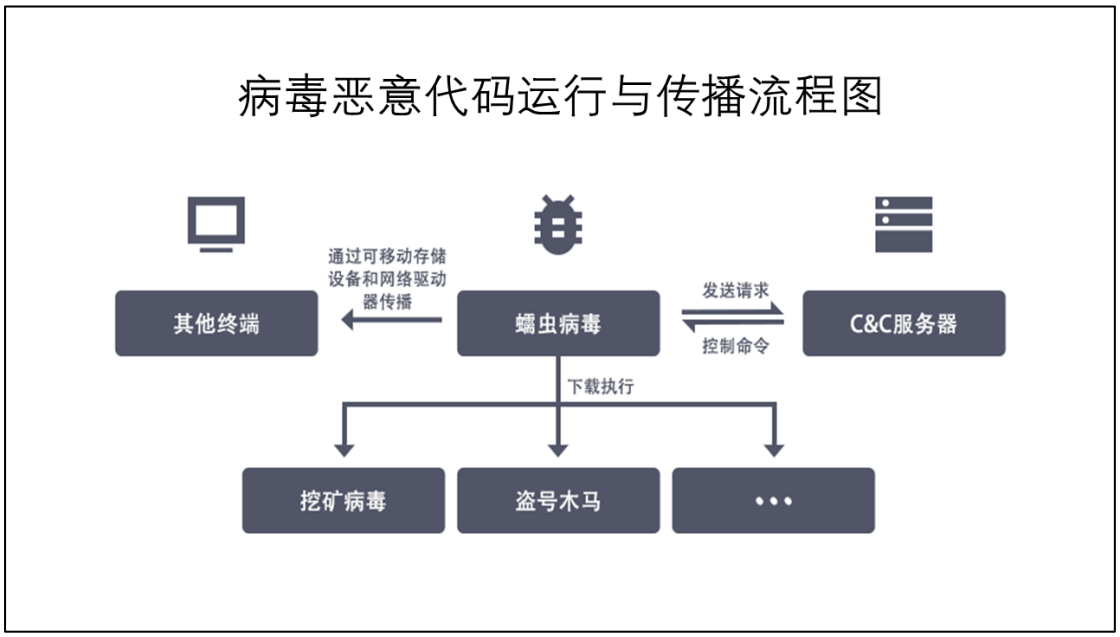
排查多台服务器，发现恶意程序和运行日志，发现域管密码泄露，内网网络互通未做隔离，全局机器开放 445 端口，且均未安装 17-010 漏洞补丁；将部分恶意样本取出分析，发现存在定时任务，恶意程序自我服务，请求恶意挖矿域名；从 PLM-TEST 主机上确定最早入侵时间在 8 月 24 号之前，且内网无全流量设备，主机系统日志已被覆盖，无法准确找到入侵入口和确切入侵时间。

应急响应中心专家通过调查发现，病毒在内网潜伏时间已久，大量主机安装 office 破解、驱动人生、KMS、大白菜等大量破解软件极大地增加了安全风险；内网未做网络隔离，导致病毒传播速度极快；内网无日志审计、流量审计等安全设备，导致无法及时发现潜伏的恶意程序；几乎所有的 windows 系统都未安装漏洞补丁。

四、 某铁路机车企业遭恶意代码攻击

2021 年 3 月 26 日，奇安信安服团队接到某铁路机车企业应急求助，生产内网存储服务器文件出现异常，需要进行应急处置。通过奇安信工程师现场排查，成功从客户 U 盘中提取到病毒样本文件，通过对样本文件进行分析，发现样本特征和客户内网病毒传播特征匹配。

该病毒通过可移动存储设备（U 盘、移动硬盘等）和网络驱动器等方式进行传播。被该蠕虫病毒感染后，病毒会将移动设备、网络驱动器内的原有文件隐藏起来，并创建了一个与磁盘名称、图标完全相同的快捷方式，诱导用户点击。用户一旦点击，病毒会立即运行。病毒恶意代码运行与传播流程图，如下图所示：



该病毒会将自身拷贝到可移动存储设备和网络驱动器中，病毒程序及脚本分别名为

DeviceConfigManager.exe 和 DeviceConfigManager.vbs。被释放的病毒文件及文件描述，如下表所示：

病毒文件名	文件描述
DeviceConfigManager.exe	蠕虫病毒
DeviceConfigManager.vbs	用于启动蠕虫病毒，关闭当前资源管理器窗口并打开目录
与磁盘同名的快捷方式	启动 DeviceConfigManager.vbs
autorun.inf	通过系统设备自动播放功能启动 DeviceConfigManager.exe

该病毒整体逻辑分为两个部分，分别为传播和后门逻辑。该病毒的传播只针对可移动存储设备和网络驱动器，被感染后的可移动存储设备或网络驱动器根目录中会被释放一组病毒文件，并通过诱导用户点击或利用系统自动播放功能进行启动。

通过奇安信威胁情报中心进行分析，从 2018 年开始，该病毒在国内呈现出迅速爆发的威胁态势，并且近期还在不断传播。病毒运行后，首先会通过 C&C 远程返回的控制命令，将其感染的电脑进行分组，再针对性的获取相应的病毒模块，执行盗号、挖矿等破坏行为。病毒作者十分谨慎，将蠕虫病毒及其下载的全部病毒模块，都使用了混淆器，很难被安全软件查杀。同时，其下载的挖矿病毒只会在用户电脑空闲时进行挖矿，并且占用 CPU 资源很低，隐蔽性非常强。

不仅如此，该病毒还会删除被感染设备或网络驱动器根目录中的可疑文件，以保证只有自身会进入用户电脑。由此可见，该病毒以长期占据用户电脑来牟利为目的，日后不排除会远程派发其他恶性病毒（如勒索病毒）的可能。

第四章　工业互联网安全发展趋势

2021 年，工业互联网的发展延续了近几年来的趋势，正处在创新活跃期、战略窗口期和关键发展期。工业互联网创新发展在基础设施建设、融合应用发展、创新能力提升和产业生态培育等方面正持续深化，前进的步伐更加坚实。与此同时，工业互联网安全面临的挑战也日益严峻。结合奇安信在工业互联网安全研究、建设和服务实践中掌握的漏洞、安全威胁以及应急事件等信息分析，我们对工业互联网安全发展趋势有如下判断。

一、　工业数据安全风险日益高涨

随着越来越多的工业控制系统与互联网连接，传统相对封闭的工业生产环境被打破，勒索、病毒等威胁从网络端渗透蔓延至内网系统，存在内网大范围感染恶意软件、高危木马等潜在安全隐患，黑客可从网络端攻击工业控制系统，甚至通过攻击外网服务器和办公网实现数据窃取。

首先，针对数据层面的攻击方式类型多样。以暴力破解凭证、勒索攻击、撞库攻击、漏洞攻击等方式威胁数据安全的网络攻击日益增多，成为工业互联网数据安全的重大威胁。例如，2021 年 7 月 9 日，伊朗铁路系统遭遇网络攻击，攻击者在全国各地车站的显示屏上大肆发布关于火车延误或取消的虚假信息。

其次，工业主机、数据库、App 等存在的端口开放、漏洞未修复、接口未认证等问题，都成为黑客便捷入侵的攻击点，可造成重要工业数据泄露、财产损失等严重后果。同时，数据全生命周期各环节的安全防护面临挑战。

最后，新一代信息技术应用带来新的数据安全风险。云环境下越来越多的工业控制系统、设备直接或间接与云平台连接，网络攻击面显著扩大，单点数据一旦被感染，就可能从局部性风险演变成系统性风险。信息技术与制造业融合发展，推动工业数据急剧增长，海量工业数据的安全管理和防护面临挑战。人工智能、5G、数字孪生、虚拟现实等新技术应用都会引入新的数据安全风险。

二、　车联网安全关注度显著增加

车联网是新一代网络通信技术与汽车、电子、道路交通运输等领域深度融合的新兴产业形态。在产业快速发展的同时，车联网安全风险日益凸显，车联网安全保障体系亟须健全完善。

早在 2015 年，克莱斯勒的 JEEP 车型娱乐芯片漏洞就曾被黑客远程攻破；2016 年，特斯拉车载系统遭无接触远程破解，黑客可以在车辆行驶过程中打开汽车后备箱甚至让车辆突然刹车。知名汽车网络安全公司 Upstream Security 发布的《2021 汽车网络安全报告》显示，自 2016 年以来，汽车网络安全事件的数量成倍增长。过去十年，前三大攻击媒介分别是无钥匙进入系统（30%）、后端服务器（27%）和移动应用程序（13%）；安全事件造成的后果位列前三的分别是汽车盗窃/入侵（31%）、对汽车系统的控制（27%），以及数据/隐私泄露（23%）。

2021 年 8 月 12 日发生的国内某品牌汽车自动驾驶致人死亡的事件引发社会对智能网联汽车安全风险的高度关注。车联网若遭受安全攻击，轻则泄露出行轨迹、习惯、语音、视频等个人隐私，重则酿成车毁人亡的惨剧，甚至被控制的汽车可能成为恐怖分子的工具。电影《速度与激情 8》网络恐怖分子攻击周边几公里范围内的汽车，把这些受遥控的‘僵尸车’作为攻击武器的场景就可能在现实中出现。

在车联网时代，安全问题将由单一车辆财产安全向威胁个人安全、公共安全蔓延，安全事件影响面逐渐扩大。个人安全方面，车联网对其的威胁主要体现在三个方面：一是个人信息泄露。车联网实现了用户线上和线下生活的有机结合，相关数据既涵盖了与车辆安全运行关联的数据，也包括了用户数据、车联网应用服务相关的数据，这些数据信息相结合，几乎涵盖个人生活相关的所有关键数据，而以上数据一旦泄露将对个人造成很大的威胁。二是非法操控。车辆或车联网平台一旦被黑客非法入侵，可能面临车辆被远程解锁、远程开车门、启动，甚至是转向系统、动力系统等被非法控制，造成车辆被盗取甚至车辆行驶安全事故。三是拒绝服务。黑客对平台端的服务器发起网络攻击，造成平台网联功能（如车辆信息上传、远程控制以及请求服务等）受限或无法使用；对车辆端发起攻击而发送大量垃圾数据造成 CAN 总线过载和通信受阻，导致车辆运行异常。公共安全方面，车联网对其的威胁主要体现在：车联网在极大增强车联网应用功能、改善用户业务体验、促进智慧城市和智能交通管理的同时，使得车辆、基础设施或服务平台可能会受到网络攻击或基于漏洞的网络攻击而面临拒绝服务或控制权被恶意拦截、替换等威胁，进而造成大面积交通混乱或瘫痪，威胁公共安全。

奇安信成立了专注车联网安全的星舆实验室，实验室致力于新四化（智能、网联、电动、共享）汽车安全研究，漏洞挖掘，渗透测试，攻防演练等工作，研究范围包括车辆的信息安全和数据安全，汽车云端控制，近场通讯，车端内部 CAN 总线通讯，车路协同，自动驾驶，充电桩等。星舆实验室出色的车联网安全研究能力，入选中汽中心“车联网漏洞分析专家工

作组”专家成员，并成为中汽中心“车联网安全重点支撑单位”。

2021 年星舆实验室在研究中发现了大量的车联网安全问题，包括：（1）发现特斯拉安全问题，两名安全研究员进驻特斯拉安全名人堂，获奖金 3133.7 美金。（2）发现施耐德充电桩安全漏洞，获特施耐德官方致谢。（3）发现某汽车人脸识别漏洞，并获中汽中心 CNNVD 漏洞平台原创漏洞证书。

三、 5G+工业互联网安全能力亟需提升

“5G+工业互联网”是指利用以 5G 为代表的新一代信息通信技术，构建与工业经济深度融合的新型基础设施、应用模式和工业生态，将推动我国工业生产从单点、局部的信息技术应用向数字化、网络化和智能化转变，从而有力支撑制造强国、网络强国建设。“5G+工业互联网”主要应用在工业设计、制造、质检、运维、安全等关键环节。

截至 2021 年底，全国工业企业建设“5G+工业互联网”项目超过 1800 个，覆盖 22 个国民经济重要行业，“5G+工业互联网”已成为工业互联网和 5G 发展进程中产业热情最高、创新最活跃、成效最显著的领域之一。但当前，中国在推动 5G 与工业互联网融合发展中也出现了一些挑战。随着 5G+工业互联网、工业上云等工作的推进，网络日益开放，打破了传统工业封闭的生产环境，带来了更加严峻的安全挑战。这些安全挑战主要表现在：

1) 技术融合带来新风险：工业互联网与 5G 技术的融合，将改变原有的网络结构与数据传输方式，在提升数字化、网络化和智能化同时，现有的 5G 和工业互联网各自原有的安全风险依然存在；

2) 安全运营能力不足带来新风险：工业互联网设备种类多、数量多，安全能力参差不齐，由于工业互联网设备软件更新缓慢、用户及厂商通常无法及时发现或修复漏洞，导致设备漏洞较多。同时，设备漏洞易被攻击者利用来构建完整的攻击链路，并获取更高权限，甚至制造病毒长期危害工业互联网安全。

3) 数据采集难度增加：5G 网络覆盖下的智能工厂中，所有生产控制数据通过 5G 网络灵活交互，传统的汇聚控制节点将不复存在，前端终端数量大幅增加，数据采集的复杂度和难度也随之大幅提升；

4) 供应链安全能力不足：工业互联网特别是底层工控系统我国自主可控能力不强，且行业分布差异性非常大。大量外国产品已深度渗透至我国能源、制造、交通等领域，有可能导致我国经济命脉部分信息实况被外方掌握，甚至存在被境内外敌对势力破坏的潜在威胁。

5) 亟需加快国产化进程：面向垂直应用的 5G 安全问题不仅是技术问题，还将对社会

民生产生深刻影响，特别是关键领域的工业数据还关系到国家安全，相关产品的国产化进程具有战略意义。

附录一 2021 工业互联网安全重大事件

一、 美国佛罗里达州水处理系统遭黑客攻击

2021 年 2 月，美国佛罗里达州水处理系统遭黑客攻击，试图将氢氧化钠（NaOH）（也称为碱液和苛性钠）的浓度从百万分之 100 更改为百万分之 11,100，也就是提高 100 倍。氢氧化钠常见于家用清洁剂中，在含量较低的情况下，水处理设施会使用它来调节酸度（pH）并去除重金属。但是如果摄入高浓度氢氧化钠会非常危险，对身体造成严重损害。

攻击者首先通过远程访问工厂员工计算机上的 TeamViewer 远程桌面软件以控制其他系统，攻击者仅在系统内部花费了 3-5 分钟，就调整了氢氧化钠的含量。幸运的是，操作员及时发现了异常，进行干预并切断了黑客对于系统的远程访问。

二、 起亚汽车遭受 DoopelPaymer 勒索软件攻击

2021 年 2 月，起亚汽车美国分公司（KMA）遭受 DoopelPaymer 勒索软件攻击，被开出 2000 万美元天价赎金。KMA 在全美拥有近 800 家经销商，所有轿车及 SUV 产品都在乔治亚州西点市郊区制造。

DoppelPaymer 向来以先窃取未加密文件、再对设备进行全面加密而闻名。一旦受害者拒绝支付赎金，则相关信息将很快被公开披露在专门的数据发布站点之上。目前窃取未加密文件并借此逼迫受害者就范已经成为勒索软件中的一种常见策略。迄今为止，全球有超过 1300 家企业受到此类攻击的影响。

三、 宏碁电脑遭受 REvil 勒索软件攻击

2021 年 3 月，中国台湾电子与计算机制造商宏碁（Acer）遭遇 REvil 勒索软件攻击，威胁方开出了迄今为止最高数额的赎金——5000 万美元（约 3.25 亿人民币）。

威胁情报公司 Advanced Intel 的情报平台监测到，REvil 团伙曾对宏碁域内的微软 Exchange 服务器发起攻击，利用微软 Exchange 安全漏洞窃取数据或者加密锁定目标设备，这是勒索攻击中首次使用该漏洞。

四、 伊朗核设施遭破坏性网络攻击导致断电

4 月 10 日，伊朗总统鲁哈尼在伊朗核技术日线上纪念活动上，下令启动纳坦兹核设施

内的近 200 台 IR-6 型离心机，开始生产浓缩铀。（IR-6 型离心机生产浓缩铀的效率是第一代 IR-1 型的 10 倍）。而就在开始生产浓缩铀后，伊朗纳坦兹核设施的配电系统就在第二天（4 月 11 日）发生故障。

根据以色列媒体 Kan 报告，美国和以色列情报机构的情报消息来源表示，以色列摩萨德是对伊朗伊朗纳坦兹核设施进行网络攻击的幕后黑手，该行动导致核设施断电。

五、 欧洲能源技术供应商遭勒索攻击

挪威公司 Volue 是一家专为欧洲能源及基础设施企业提供技术方案的厂商，该公司在 5 月 4 日-5 日遭遇勒索软件攻击。

在此次攻击事件中，黑客关闭了挪威国内 200 座城市的供水与水处理设施的应用程序，影响范围覆盖全国约 85%的居民。为了防止勒索软件进一步传播至其他计算机系统，Volue 公司不得不关闭了所托管的其他多种应用程序，并将约 200 名员工使用的设备进行隔离。

六、 美国燃油管道商遭勒索软件攻击停运

5 月 7 日，美国最大的燃油管道商 Colonial Pipeline 遭到勒索软件攻击，由于 Colonial Pipeline 负责美国东岸多达 45%的燃料供应，因此该攻击事件导致该公司暂停了所有的管道作业网络，并于晚间关闭一条主要的燃料传输管道。

根据多方外媒报道，该攻击由 DarkSide 勒索软件团伙发起，该组织仅两个小时的时间内就从位于佐治亚州阿尔法利塔的 Colonial 公司网络中窃取了近 100 GB 的数据。

七、 伊朗国家铁路遭网络攻击大屏传播虚假延误信息

7 月 9 日，据伊朗国内的法尔斯通讯社报道，伊朗铁路系统遭遇网络攻击，攻击者在全国各地车站的显示屏上大肆发布关于火车延误或取消的虚假信息。

显示屏上的通报信息提到，火车“因网络攻击而长时间延误”或“取消”，并敦促乘客拨打电话查询更多详细信息。而这里留下的，恰恰是伊朗最高领导人阿亚图拉·阿里·哈梅内伊办公室的座机号码。网络攻击导致伊朗火车站爆发出“前所未有的混乱局面”。

八、 美国大型农业企业遭勒索攻击离线

9 月 21 日，BlackMatter 勒索软件团伙入侵了爱荷华州的一家农业企业“新合作社”，要求 590 万美元的赎金。这家农业合作社证实自己遭到了网络攻击，并关闭了自己的系统作为

应对，这次攻击给食品供应链带来了严重影响。

威胁情报公司 Recorded Future 的分析师 Dmitry Smalyinets 表示：攻击者窃取了使用的精密工具的控制输入等相关的全部数据。

九、 英国工程巨头遭勒索攻击致运营临时中断

英国工程巨头伟尔集团主要服务于采矿、基础设施以及石油与天然气等市场。10 月 7 日，该公司披露今年 9 月遭受了一起勒索软件攻击，导致出货、制造与工程系统被迫发生中断。

这起攻击令伟尔集团损失惨重，仅 9 月因开销不足与收入延后带来的间接损失高达 5000 万英镑（约 4.38 亿元人民币），预计下一财季业绩将受到影响。

十、 伊朗各地加油站因网络攻击出现软件故障

10 月 26 日早上，伊朗国有天然气分销企业 NIOPDC 疑似遭到网络攻击，全国各地的加油站出现软件故障，无法正确计费收款，加油泵屏幕与油价广告牌上还莫名显示出涉政异常内容。NIOPDC 公司因此临时关闭了加油站运营，司机排长队等待加油，在社交网络引发了大面积讨论；

根据当地媒体报道以及社交网络消息，这次网络攻击导致 NIOPDC 加油站的加油泵屏幕上显示出“cyber attack 64411”。

附录二 2021 年新公开工业互联网超高危漏洞

CVSS（Common Vulerability Scoring System, 通用漏洞评估方法）提供了一种捕获漏洞主要特征并生成反映其严重性的数字评分的方法。漏洞库平台根据 CVSS 分级标准对漏洞进行 0 至 10 之间的数字评分，10 分为最高分，表示该漏洞的严重程度最高，一旦被攻击者利用，造成的损失也较大。本附录为 2021 年 CVSS v3.X（CVSS v3.0 或 CVSS v3.1）为 10 的 16 个工业互联网安全超高危漏洞 ，并参考美国网络安全和基础设施安全局（CISA）的建议给出漏洞的缓解措施。

一、 身份认证绕过漏洞 CVE-2021-22681（CNNVD-202102-1663）

漏洞简介：Rockwell Automation RSLogix 500 Software 和 Logix Designer Studio 5000 都是美国罗克韦尔（Rockwell Automation）公司的产品。RSLogix 500 Software 是一套用于工业控制系统的编程软件。Logix Designer Studio 5000 是一套逻辑控制器编程软件。

RSLogix 5000： Versions 16 through 20 和 Studio 5000 Logix Designer： Versions 21 and later 存在安全漏洞，攻击者可利用该漏洞绕过验证机制并通过 Logix 控制器进行身份验证。

危害等级： 超危（CVSS v3 10）

风险评估：成功利用此漏洞可能允许未经身份验证的远程攻击者绕过验证机制并连接 Logix 控制器。 此外，此漏洞可能使未经授权的第三方工具能够更改控制器的配置和/或应用程序代码。

受影响的产品：RSLogix 5000： Versions 16 through 20 和 Studio 5000 Logix Designer： Versions 21 and later

CISA 漏洞缓解措施：

1） 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1130301

2） 最小化工业控制系统/设备的网络暴露面。

3） 在防火墙后面找到控制系统网络和远程设备，并将其与业务网络隔离。

4） 限制或阻止来自工业控制系统网络区域外部的 TCP 44818 端口流量。

5） 采用身份认证和安全加密的安全方式进行远程访问。

6） 全面的纵深防御策略可以降低此漏洞的风险。为降低风险，建议用户确保他们采

用适当的网络分段和安全控制。

二、 代码注入漏洞 CVE-2021-23281（CNNVD-202104-900）

漏洞简介：Eaton Intelligent Power Manager（IPM）是美国 Eaton 公司的一款智能电源管理器，它支持从界面远程监视和管理网络中的多个设备。

Eaton Intelligent Power Manager 1.69 之前版本存在代码注入漏洞，攻击者可利用该漏洞可以发送一个特别制作的数据包，使 IPM 连接到 rouge SNMP 服务器，并执行攻击者控制的代码。

危害等级： 超危（CVSS v3 10）

风险评估：成功利用这些漏洞可能允许攻击者更改某些设置、上传代码、删除文件或执行命令。

受影响的产品：Eaton Intelligent Power Manager 1.69 and before

CISA 漏洞缓解措施：

1） 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/eaton-intelligent-power-manager-ipm-vulnerability-advisory.pdf

2） 最小化工业控制系统/设备的网络暴露面。

3） 在防火墙后面找到控制系统网络和远程设备，并将其与业务网络隔离。

4） 为了防止利用这些问题并保护软件免受恶意实体的攻击，建议在安装和使用智能电源管理器 （IPM） 软件的企业网络中阻止端口 4679 和 4680。

5） 采用身份认证和安全加密的安全方式进行远程访问。

6） 禁用/停用联网设备上未使用的通信通道、TCP/UDP 端口和服务（例如 SNMP、FTP、BootP、DHCP 等）。

三、 访问控制错误漏洞 CVE-2021-20998（CNNVD-202105-829）

漏洞简介：WAGO 是一家德国供应商，它的工业管理型交换机的基于 Web 的管理（WBM） 通常用于管理、调试和更新。报告的漏洞允许攻击者访问设备和基于 Web 的管理、安装恶意软件、访问密码并创建具有管理员权限的用户。

危害等级： 超危（CVSS v3 10）

风险评估：通过利用所描述的漏洞，攻击者可能能够操纵或破坏设备。

受影响的产品：WAGO switch 0852-0303 FW version V1.2.5 before

CISA 漏洞缓解措施：

1） 最小化工业控制系统/设备的网络暴露面。

2） 在防火墙后面找到控制系统网络和远程设备，并将其与业务网络隔离。

3） 禁用设备的 Web 服务器。

4） 使用设备的 CLI 界面。

5） 更新到最新固件。

6） 限制对设备的网络访问，请勿将设备直接连接到互联网。

四、 缓冲区错误漏洞 CVE-2021-30189（CNNVD-202105-1634）

漏洞简介：3S-Smart Software Solutions CODESYS V2 Web-Server 是德国 3S-Smart Software Solutions 公司的一个应用程序。一个 web 服务器。

CODESYS V2 Web-Server 1.1.9.20 之前版本存在安全漏洞。攻击者通过精心制作的 web 服务器请求导致基于堆栈的缓冲区溢出，并在 CODESYS web 服务器上执行任意代码，或者由于 CODESYS web 服务器崩溃而触发拒绝服务。

危害等级： 超危（CVSS v3 10）

风险评估：成功利用这些漏洞可能允许攻击者在 CODESYS Control 运行时系统中读取或写入任意内存或文件，导致执行代码的内存访问无效，或使 CODESYS Web 服务器或 CODESYS Control 运行时系统崩溃。

受影响的产品：All CODESYS V2 web servers running stand-alone or as part of the CODESYS runtime system，Versions<1.1.9.20

CISA 漏洞缓解措施：

1） 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14726&token=553da5d11234bbe1ceed59969d419a71bb8c8747&download=

2） 最小化工业控制系统/设备的网络暴露面。

3） 在防火墙后面找到控制系统网络和远程设备，并将其与业务网络隔离。

4） 采用身份认证和安全加密的安全方式进行远程访问。

5） 全面的纵深防御策略可以降低此漏洞的风险。为降低风险，建议用户确保他们采用适当的网络分段和安全控制。

五、 访问控制错误漏洞 CVE-2021-30190（CNNVD-202105-1632）

漏洞简介：3S-Smart Software Solutions CODESYS V2 Web-Server 是德国 3S-Smart Software Solutions 公司的一个应用程序。一个 web 服务器。

CODESYS V2 Web-Server 1.1.9.20 之前版本存在安全漏洞，该漏洞源于不正确的访问控制。CODESYS 的用户管理允许用户依赖于对可视化页面的访问控制。但是，不管身份验证是否成功，读取或写入值的下级请求都被转发到 CODESYS Control 系统运行。攻击者可以通过精心制作的 web 服务器请求绕过用户管理，无需身份验证就可以在 PLC 上读或写值。

危害等级： 超危（CVSS v3 10）

风险评估：成功利用这些漏洞可能允许攻击者在 CODESYS Control 运行时系统中读取或写入任意内存或文件，导致执行代码的内存访问无效，或使 CODESYS Web 服务器或 CODESYS Control 运行时系统崩溃。

受影响的产品：All CODESYS V2 web servers running stand-alone or as part of the CODESYS runtime system，Versions<1.1.9.20

CISA 漏洞缓解措施：

1） 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14726&token=553da5d11234bbe1ceed59969d419a71bb8c8747&download=

2） 最小化工业控制系统/设备的网络暴露面。

3） 在防火墙后面找到控制系统网络和远程设备，并将其与业务网络隔离。

4） 采用身份认证和安全加密的安全方式进行远程访问。

5） 全面的纵深防御策略可以降低此漏洞的风险。为降低风险，建议用户确保他们采用适当的网络分段和安全控制。

六、 输入验证漏洞 CVE-2021-30191（CNNVD-202105-1626）

漏洞简介：3S-Smart Software Solutions CODESYS V2 Web-Server 是德国 3S-Smart Software Solutions 公司的一个应用程序。一个 web 服务器。

CODESYS V2 Web-Server 1.1.9.20 版本之前存在安全漏洞，该漏洞源于程序没有检查输入数据的大小。

危害等级： 超危（CVSS v3 10）

风险评估：成功利用这些漏洞可能允许攻击者在 CODESYS Control 运行时系统中读取

或写入任意内存或文件，导致执行代码的内存访问无效，或使 CODESYS Web 服务器或 CODESYS Control 运行时系统崩溃。

受影响的产品：All CODESYS V2 web servers running stand-alone or as part of the CODESYS runtime system，Versions<1.1.9.20

CISA 漏洞缓解措施：

1） 目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法：
https://customers.codesys.com/index.php

2） 最小化工业控制系统/设备的网络暴露面。

3） 在防火墙后面找到控制系统网络和远程设备，并将其与业务网络隔离。

4） 采用身份认证和安全加密的安全方式进行远程访问。

5） 全面的纵深防御策略可以降低此漏洞的风险。为降低风险，建议用户确保他们采用适当的网络分段和安全控制。

七、 安全特征问题漏洞 CVE-2021-30192（CNNVD-202105-1621）

漏洞简介：3S-Smart Software Solutions CODESYS V2 Web-Server 是德国 3S-Smart Software Solutions 公司的一个应用程序。一个 web 服务器。

CODESYS V2 Web-Server 1.1.9.20 版本之前存在安全漏洞，该漏洞源于程序存在不正确的安全检查。

危害等级： 超危（CVSS v3 10）

风险评估：成功利用这些漏洞可能允许攻击者在 CODESYS Control 运行时系统中读取或写入任意内存或文件，导致执行代码的内存访问无效，或使 CODESYS Web 服务器或 CODESYS Control 运行时系统崩溃。

受影响的产品：All CODESYS V2 web servers running stand-alone or as part of the CODESYS runtime system，Versions<1.1.9.20

CISA 漏洞缓解措施：

1） 目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法： https://customers.codesys.com/index.php

2） 最小化工业控制系统/设备的网络暴露面。

3） 在防火墙后面找到控制系统网络和远程设备，并将其与业务网络隔离。

4） 采用身份认证和安全加密的安全方式进行远程访问。

5） 全面的纵深防御策略可以降低此漏洞的风险。为降低风险，建议用户确保他们采用适当的网络分段和安全控制。

八、 缓冲区错误漏洞 CVE-2021-30193（CNNVD-202105-1623）

漏洞简介：3S-Smart Software Solutions CODESYS V2 Web-Server 是德国 3S-Smart Software Solutions 公司的一个应用程序。一个 web 服务器。

CODESYS V2 Web-Server 1.1.9.20 版本之前存在安全漏洞，该漏洞源于程序存在越界读写。

危害等级： 超危（CVSS v3 10）

风险评估：成功利用这些漏洞可能允许攻击者在 CODESYS Control 运行时系统中读取或写入任意内存或文件，导致执行代码的内存访问无效，或使 CODESYS Web 服务器或 CODESYS Control 运行时系统崩溃。

受影响的产品：All CODESYS V2 web servers running stand-alone or as part of the CODESYS runtime system，Versions<1.1.9.20

CISA 漏洞缓解措施：

1） 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://customers.codesys.com/index.php

2） 最小化工业控制系统/设备的网络暴露面。

3） 在防火墙后面找到控制系统网络和远程设备，并将其与业务网络隔离。

4） 采用身份认证和安全加密的安全方式进行远程访问。

5） 全面的纵深防御策略可以降低此漏洞的风险。为降低风险，建议用户确保他们采用适当的网络分段和安全控制。

九、 缓冲区溢出漏洞 CVE-2021-30194（CNNVD-202105-1625）

漏洞简介：3S-Smart Software Solutions CODESYS V2 Web-Server 是德国 3S-Smart Software Solutions 公司的一个应用程序。一个 web 服务器。

CODESYS V2 Web-Server 1.1.9.20 之前版本存在安全漏洞。攻击者通过精心制作的 web 服务器请求导致基于堆栈的缓冲区溢出，并在 CODESYS web 服务器上执行任意代码，或者由于 CODESYS web 服务器崩溃而触发拒绝服务。

危害等级： 超危（CVSS v3 10）

风险评估：成功利用这些漏洞可能允许攻击者在 CODESYS Control 运行时系统中读取

或写入任意内存或文件，导致执行代码的内存访问无效，或使 CODESYS Web 服务器或 CODESYS Control 运行时系统崩溃。

受影响的产品：All CODESYS V2 web servers running stand-alone or as part of the CODESYS runtime system，Versions<1.1.9.20

CISA 漏洞缓解措施：

1） 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://customers.codesys.com/index.php

2） 最小化工业控制系统/设备的网络暴露面。

3） 在防火墙后面找到控制系统网络和远程设备，并将其与业务网络隔离。

4） 采用身份认证和安全加密的安全方式进行远程访问。

5） 全面的纵深防御策略可以降低此漏洞的风险。为降低风险，建议用户确保他们采用适当的网络分段和安全控制。

十、 数据伪造问题漏洞 CVE-2021-33885（CNNVD-202108-2341）

漏洞简介：B. Braun SpaceCom2 是德国贝朗（B. Braun）公司的一款硬件设备，用于连接外部设备以在患者数据管理系统、PC 或 USB 记忆棒中记录数据。

B.Braun SpaceCom2 012U000062 之前版本存在安全漏洞，该漏洞源于应用数据真实性验证不足，远程攻击者可以向设备发送恶意数据，这些数据将用于代替正确数据。

危害等级： 超危（CVSS v3 10）

风险评估：成功利用这些漏洞可能允许未经身份验证的远程攻击者获得用户级命令行访问权限、发送设备恶意数据以代替正确数据、从未知来源重新配置设备、获取敏感信息或覆盖关键信息文件。

受影响的产品：Braun SpaceCom2 012U000062 之前版本

CISA 漏洞缓解措施：

1） 目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.bbraunusa.com/en.html。

2） 尽量减少所有控制系统设备和/或系统的网络暴露，并确保它们不能从 Internet 访问。

3） 在防火墙后定位控制系统网络和远程设备，并将它们与业务网络隔离。

4） 当需要远程访问时，使用安全方法，例如虚拟专用网络 （VPN），认识到 VPN 可能存在漏洞，应更新到可用的最新版本。 还要认识到 VPN 仅与连接的设备一

样安全。

5） 在部署防御措施之前进行适当的影响分析和风险评估。

十一、 授权问题漏洞 CVE-2021-23857（CNNVD-202110-172）

漏洞简介：Bosch Rexroth Rexroth IndraMotion Mlc 是德国博世力士乐（Bosch Rexroth）公司的一种将运动与逻辑控制，以及机器人控制相结合的新型设备。

Rexroth IndraMotion Mlc 存在安全漏洞，该漏洞源于网络系统或产品未正确使用相关密码算法，导致内容未正确加密、弱加密、明文存储敏感信息等。

危害等级： 超危（CVSS v3 10）

风险评估：允许客户端不使用密码登录系统，而是使用密码的哈希登录。这允许攻击者随后登录系统。

受影响的产品：力士乐 IndraMotion MLC L25、L45、L65、L75、L85、XM21、XM22、XM41 和 XM42 IndraMotion XLC >= 12 VRS

CISA 漏洞缓解措施：

1） 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://psirt.bosch.com/security-advisories/bosch-sa-741752.html

2） 最小化工业控制系统/设备的网络暴露面。

3） 在防火墙后面找到控制系统网络和远程设备，并将其与业务网络隔离。

4） 采用身份认证和安全加密的安全方式进行远程访问。

5） 全面的纵深防御策略可以降低此漏洞的风险。为降低风险，建议用户确保他们采用适当的网络分段和安全控制。

十二、 代码问题漏洞 CVE-2021-38397（CNNVD-202110-231）

漏洞简介：Honeywell Experion Pks 和 Honeywell Ace Controllers 都是美国 Honeywell 公司的产品。Honeywell Experion Pks 是一个过程自动化系统。Honeywell Ace Controllers 是用于在服务器级计算机平台上执行 Honeywell 的控制执行环境 （Cee）。

Honeywell Experion PKS 和 ACE Controllers 存在代码问题漏洞，该漏洞源于文件上载过程中文件验证不足。攻击者可利用该漏洞上载恶意文件并在服务器上执行。

危害等级： 超危（CVSS v3 10）

风险评估：成功利用这些漏洞可能导致远程代码执行和拒绝服务条件。

受影响的产品：C200 所有版本，C200E 所有版本，C300 和 ACE 控制器所有版本

CISA 漏洞缓解措施：

1） 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.honeywellprocess.com/library/support/notifications/Customer/SN2021-02-22-01-Experion-C300-CCL.pdf

2） 最小化工业控制系统/设备的网络暴露面。

3） 在防火墙后面找到控制系统网络和远程设备，并将其与业务网络隔离。

4） 采用身份认证和安全加密的安全方式进行远程访问。

5） 全面的纵深防御策略可以降低此漏洞的风险。为降低风险，建议用户确保他们采用适当的网络分段和安全控制。

十三、 访问控制错误漏洞 CVE-2021-38454（CNNVD-202110-233）

漏洞简介：Moxa Mxview Network Management Software 是中国 Moxa 公司的一个整合式的管理平台。用于在工业以太网中完成网络设备的配置、监控、诊断。

Moxa MXview Network Management Software 存在访问控制错误漏洞，该漏洞源于受影响的产品具有允许远程连接到内部通信通道的错误配置的服务。攻击者可利用该漏洞绕过已实现的安全限制，进行交互并使用 MQTT。

危害等级： 超危（CVSS v3 10）

风险评估：成功利用这些漏洞可能允许攻击者创建或覆盖关键文件以执行代码、访问程序、获取凭据、禁用软件、读取和修改其他无法访问的数据、允许远程连接到内部通信通道，或交互和远程使用 MQTT。

受影响的产品：MXview 网络管理软件：版本 3.x 至 3.2.2

CISA 漏洞缓解措施：

1） 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://us-cert.cisa.gov/ics/advisories/icsa-21-278-03

2） 升级到软件包 v3.2.4 或更高版本。

3） 用户应定期更改其 Windows 密码并使用防火墙。

4） 如果用户需要使用多站点功能，Moxa 建议使用防火墙屏蔽 8883 端口。如果用户没有此要求，Moxa 建议使用防火墙在客户端分配 MXview 的可访问 IP。

十四、 输入验证错误漏洞 CVE-2021-40112（CNNVD-202111-355）

漏洞简介：Cisco Catalyst Passive Optical Network Series Switches（Catalyst Pon Series Switches）是美国思科（Cisco）公司的一系列高性能、结构简单、易于维护的交换机。用于提供具有竞争力的网络解决方案。

Cisco Catalyst Passive Optical Network Series Switches 存在安全漏洞，该漏洞源于 Cisco Catalyst PON 系列交换机 ONT 的 web 管理界面不正确的 HTTPS 输入验证造成的。攻击者可利用该漏洞通过向 web 管理界面发送精心设计的 HTTPS 请求来修改配置。

危害等级： 超危（CVSS v3 10）

风险评估：思科 Catalyst 无源光网络 （PON） 系列交换机光网络基于 Web 的管理界面中存在多个漏洞，终端可能允许未经身份验证的远程攻击者执行以下行动：

1） 如果启用 Telnet 协议，则使用默认凭据登录

2） 执行命令注入

3） 修改配置

受影响的产品：Catalyst PON 交换机 CGP-ONT-1P，Catalyst PON 交换机 CGP-ONT-4P，Catalyst PON 交换机 CGP-ONT-4PV，Catalyst PON 交换机 CGP-ONT-4PVC，Catalyst PON 交换机 CGP-ONT-4TVCW

CISA 漏洞缓解措施：

1） 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr

2） 最小化工业控制系统/设备的网络暴露面。

3） 在防火墙后面找到控制系统网络和远程设备，并将其与业务网络隔离。

4） 采用身份认证和安全加密的安全方式进行远程访问。

5） 全面的纵深防御策略可以降低此漏洞的风险。为降低风险，建议用户确保他们采用适当的网络分段和安全控制。

十五、 缓冲区错误漏洞 CVE-2021-40113（CNNVD-202111-357）

漏洞简介：Cisco Catalyst Passive Optical Network Series Switches（Catalyst Pon Series Switches）是美国思科（Cisco）公司的一系列高性能、结构简单、易于维护的交换机。用于提供具有竞争力的网络解决方案。

Cisco Catalyst Passive Optical Network Series Switches 存在安全漏洞，该漏洞源于 Cisco Catalyst PON 系列交换机 ONT 基于 web 的管理界面对用户提供的输入验证不足造成的。攻击者可利用该漏洞在受影响的设备上执行任意命令。

危害等级： 超危（CVSS v3 10）

风险评估：思科 Catalyst 无源光网络 （PON） 系列交换机光网络基于 Web 的管理界面中存在多个漏洞，终端可能允许未经身份验证的远程攻击者执行以下行动：

1） 如果启用 Telnet 协议，则使用默认凭据登录

2） 执行命令注入

3） 修改配置

受影响的产品：Catalyst PON 交换机 CGP-ONT-1P，Catalyst PON 交换机 CGP-ONT-4P，Catalyst PON 交换机 CGP-ONT-4PV，Catalyst PON 交换机 CGP-ONT-4PVC，Catalyst PON 交换机 CGP-ONT-4TVCW

CISA 漏洞缓解措施：

1） 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr

2） 最小化工业控制系统/设备的网络暴露面。

3） 在防火墙后面找到控制系统网络和远程设备，并将其与业务网络隔离。

4） 采用身份认证和安全加密的安全方式进行远程访问。

5） 全面的纵深防御策略可以降低此漏洞的风险。为降低风险，建议用户确保他们采用适当的网络分段和安全控制。

十六、 信任管理问题漏洞 CVE-2021-34795（CNNVD-202111-364）

漏洞简介：Cisco Catalyst Passive Optical Network Series Switches（Catalyst Pon Series Switches）是美国思科（Cisco）公司的一系列高性能、结构简单、易于维护的交换机。用于提供具有竞争力的网络解决方案。

Cisco Catalyst Passive Optical Network Series Switches ONT 存在信任管理问题漏洞，该漏洞源于允许未经身份验证的远程攻击者使用具有默认静态密码的调试帐户登录受影响的设备。

危害等级： 超危（CVSS v3 10）

风险评估：攻击者利用该漏洞获得系统的完全访问权限。该漏洞是由于设备上存在因调试原因而产生的。 未经身份验证的远程攻击者可以使用硬编码凭据访问受影响的系统。

受影响的产品：Catalyst PON 交换机 CGP-ONT-1P，Catalyst PON 交换机 CGP-ONT-4P，Catalyst PON 交换机 CGP-ONT-4PV，Catalyst PON 交换机 CGP-ONT-4PVC，Catalyst PON 交换机 CGP-ONT-4TVCW

CISA 漏洞缓解措施：

1） 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr

2） 最小化工业控制系统/设备的网络暴露面。

3） 在防火墙后面找到控制系统网络和远程设备，并将其与业务网络隔离。

4） 采用身份认证和安全加密的安全方式进行远程访问。

5） 全面的纵深防御策略可以降低此漏洞的风险。为降低风险，建议用户确保他们采用适当的网络分段和安全控制。

附录三 工业领域勒索病毒防护

一、 工业领域勒索病毒安全防护理念

为积极有效建设应对工业领域勒索病毒攻击事件的安全防御体系，针对勒索病毒攻击事件的事前、事中、事后三大防护阶段，主要内容为“事前防御”、“事中响应”、“事后溯源”，其中“事前防御”是防护重点。我们认为，当勒索病毒已经成功投递并加密数据，除事前做过数据备份，否则以目前任何技术手段是不可能解密加密数据的，只有交赎金从攻击者获取私钥解密一种办法。因此事后工作更多是溯源补救工作，“事前防御”才能真正做到御“敌”于外。而“事中响应”更多是在“事前防御”被突破后的应急响应。

三大防护阶段内容如下：

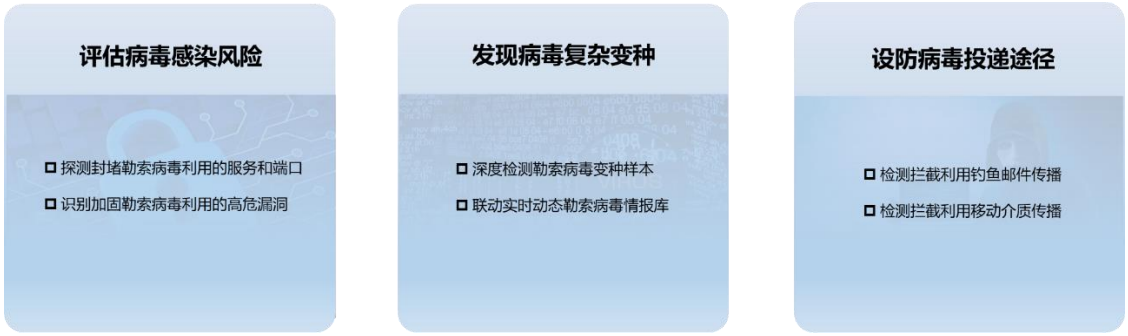
“事前防御”：①评估病毒感染风险；②发现病毒复杂变种；③设防病毒投递途径；

“事中响应”：①限制病毒落地执行；②联动处置病毒攻击；③安全服务应急处置；

“事后溯源”：①病毒攻击溯源定位；②黑客组织完整画像；③病毒文件查杀取证；

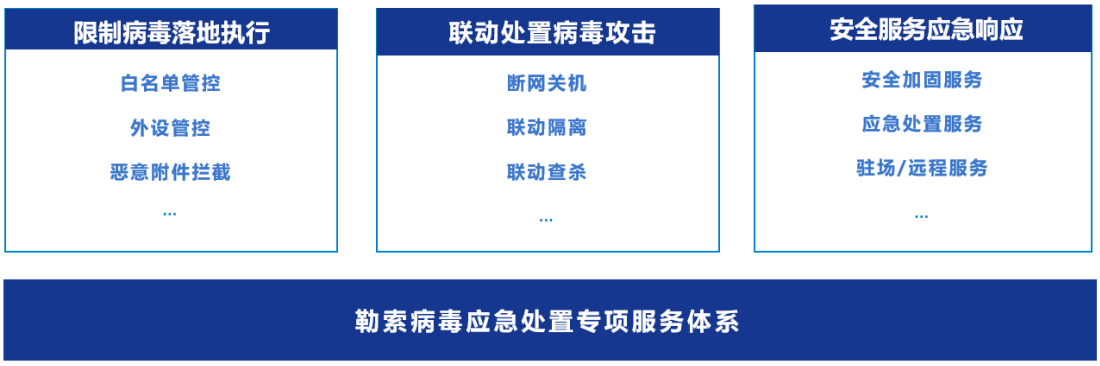
二、 事前防御：勒索病毒威胁感知

勒索病毒具有传播途径多，传播技术隐蔽，病毒变种复杂，勒索产业化发展等显著特点。有效的勒索病毒防御手段一定是尽可能地早于事故发生前检测发现异常，从而采取应对措施。而非着眼于事件发生后的补救行动。因此防御勒索病毒的思路应由“事后补救”转变为“事前防御”。事前防御主要目的即在勒索攻击事件的早起发现并拦截处置。



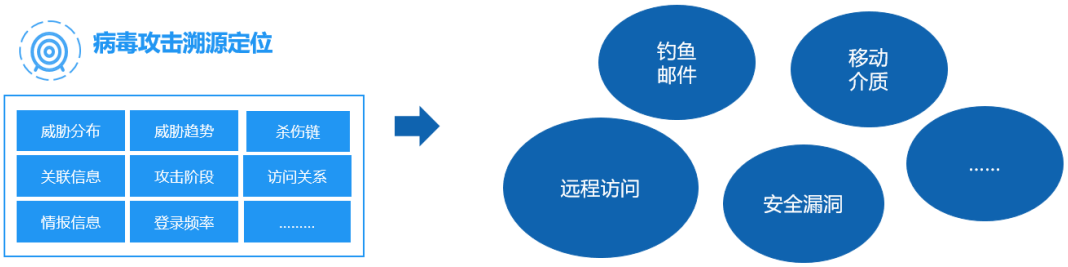
三、 事中响应：勒索病毒应急处置

有组织攻击者投递勒索病毒攻击持续且隐蔽，当遇到紧急问题时需具备较强应变能力，做出快速的应急响应处置，建立针对勒索病毒的专项应急响应体系，遏制工业企业内部资产遭投毒。



四、 事后溯源：勒索病毒溯源定位

当工业企业遭勒索病毒攻击后，应具备溯源定位能力，查明攻击源头，产出应对安全措施，固化安全经验，查漏补缺，避免事件再次发生。



病毒攻击溯源定位。排查分析安全事件发生的原因，避免同类安全事件再次发生。工业安全分析专家针对高级持续威胁监测与深度分析，发现和跟踪勒索病毒定向攻击，对重大事

件进行深度分析溯源，实现对新型勒索威胁、高级威胁的感知能力。针对威胁分布、威胁趋势、攻击杀伤链、访问关系等勒索攻击场景。当攻击事件发生时，现有的安全设备检测到攻击事件并以告警方式进行展现。攻击溯源是全面认知威胁的重要手段，是认知攻击者、攻击行为的良好途径。工业安全专家结合工业安全态势感知与管理平台、工业互联网安全公共服务平台等告警信息，深度分析攻击全过程，还原整个攻击事件，确定攻击路径和薄弱点。

附录四 工业数据安全防护

随着工业互联网、 物联网、 大数据等新一代信息技术的发展和普及， IT 与 OT 深度融合， 工业体系正在由封闭走向开放， 工业终端联网程度不断加深， 大量工业控制系统和设备暴露在互联网上，工业数据面临传统网络威胁和工业互联网安全风险“双重压力”，安全形势愈发严峻复杂。 加强工业数据安全， 构建工业数据安全管理体系刻不容缓。应将 IT 信息安全领域的数据驱动安全、 积极防御、 威胁情报、 基于威胁情报的态势感知、 安全可视化理念和方法引入工业数据安全防护。 其中数据驱动安全是技术基础， 积极防御是平台， 威胁情报是核心， 态势感知是结果， 安全可视化是手段。

一、 数据安全规划牵引

通过工业企业数据安全规划解决企业安全发展的战略问题，全面支撑企业业务战略，制定数据安全发展愿景、总体目标、方针原则，设计总体架构、提出重大措施。通过规划解决工业数据安全建设的项目设计与实施的工程问题，分解总体架构要求的项目体系，对各系统建设项目的目标、内容、方案、策略等逐一规划设计。根据项目间依赖关系，设计总体工程路线图、系统实施优先级次序，全面、系统的指导工业数据安全建设。

二、 业务与安全同步

工业数据安全管理和技术保护手段与生产运营、业务发展同步规划、同步建设、同步运行。同步规划，强调关口前移与预算保障。在工业企业业务系统的设计规划中，充分考虑数据安全，确保数据安全成为信息化系统的有机组成；同步建设，强调在工业企业业务系统建设的方方面面，充分考虑引入并融合数据安全能力，既要积极建设数据安全基础设施，又要开展业务系统内建安全机制的建设；同步运营，指在工业企业业务系统运维中将所有与数据安全相关的环节都与数据安全工作充分对接，而不仅仅是零散工作。

三、 数据采集安全

工业数据采集应当遵循合法、正当、必要的原则，不得窃取或者以其他非法方式收集数据。 数据收集过程中，采取配备技术手段、签署安全协议等措施加强对数据收集人员、设备的管理，并对数据收集的时间、类型、数量、频度、流向等进行记录。通过间接途径获取数据的，应当要求数据提供方做出数据源合法性的书面承诺，并承担相应的法律责任。

四、 数据传输安全

根据传输的数据类型、级别和应用场景，制定安全策略并采取保护措施。传输重要数据的，还应当采取校验技术、密码技术、安全传输通道或者安全传输协议等措施，涉及跨组织机构或者使用公共信息网络进行数据传输的，应当建立登记、审批机制。跨不同数据处理主体传输核心数据的，还应当通过国家数据安全工作协调机制审批。

五、 数据存储安全

依据法律规定或者与用户约定的方式和期限存储数据。存储重要数据的，还应当采用校验技术、密码技术等措施进行安全存储，不得直接提供存储系统的公共信息网络访问，并实施数据容灾备份和存储介质安全管理。存储核心数据的，还应当实施异地容灾备份。

六、 数据应用安全

工业企业未经个人、单位等同意，不得使用数据挖掘、关联分析等技术手段针对特定主体进行精准画像、数据复原等加工处理活动。 利用数据进行自动化决策的，应当保证决策的透明度和结果公平合理。使用、加工重要数据和核心数据的，还应当加强访问控制，建立登记、审批机制并留存记录。

七、 数据共享安全

数据共享应当真实、准确，并在共享前开展安全评估，对涉及个人隐私、个人信息、商业秘密、保密商务信息以及可能对公共利益及国家安全产生重大影响的，不得公开。依据行业数据分类分级管理要求，明确数据提供的范围、数量、条件、程序等。提供重要数据的，还应当采取数据脱敏等措施，建立审批机制。提供核心数据的，还应当通过国家数据安全工作协调机制审批。

八、 数据销毁安全

建立数据销毁策略和管理制度，明确销毁对象、流程和技术等要求，对销毁活动进行记录和留存。销毁重要数据和核心数据的，不得以任何理由、任何方式对销毁数据进行恢复。

九、 数据安全审计

在数据全生命周期处理过程中，实现对业务系统网络流量进行监测与审计，及时发现网

络中是否存在违反数据安全策略的行为和被攻击的迹象，记录数据处理、权限管理、人员操作等日志。日志留存时间不少于六个月，定期进行安全审计，并形成审计报告，涉及重要数据和核心数据的，应当至少每半年进行一次。

附录五 工业控制系统安全国家地方联合工程实验室

工业控制系统安全国家地方联合工程实验室（简称：工业安全国家联合实验室）是由国家发展与改革委员会批准授牌成立，由奇安信集团承建的对外开放的工业控制安全技术方面的公共研究平台。

工业安全国家联合实验室以对工业控制系统安全领域有重大影响的前沿性、战略性技术作为研究目标，建立以工程实验室为主，联合高等院校、科研院所和国家需求部门、企业共同参加的，产、学、研、用相结合的合作机制，发挥高等院校、科研院所在基础理论研究方面的力量和优势，发挥国家需求部门、企业在技术创新和应用方面的主体作用，共享科研成果。

工业安全国家联合实验室积极吸纳国内外优秀的科技人才，建立高水平专业人才培养基地。目前实验室已与北京大学、西安电子科技大学、吉林大学、武汉大学、北京理工大学、信息工程大学等均建立了人才联合培养机制。

工业安全国家联合实验室拥有软件著作权 7 项，专利 18 项，创新地提出了工业互联网自适应防护架构（PC4R），推出了工业主机安全防护系统、工业防火墙/网关、工业安全监测系统、工业安全监测控制平台、工业互联网安全监测服务平台等工业安全领域完整解决方案及产品，并已经在众多央企和工业企业中进行应用。未来，工业安全国家联合实验室将充分利用科技资源，发挥产学研联盟作用，打造产业链合作，与产业链企业实现互利共赢，在合作中共同壮大，努力成为工业互联网安全产业创新的龙头。