内部资料 免费交流

出版物准印证号：京内资准字 2123- L0058 号

SECURITY INSIDER

网安26号院

奇安信网络安全通讯

XZ后门：开源项目最复杂供应链攻击 P13

第40期

2024 年 4 月

奇安信
新一代网络安全领军者

打造新一代中国特色的安全托管服务

时刻守护您的网络安全

奇安信安全托管服务以威胁发现为基础、以分析处置为核心、以发现隐患为关键、以解决客户问题为目标，7*24小时全天候全方位守护客户网络安全。

两种模式
模式随心选择

- 直营服务模式：奇安信产品+MSS
- 合作服务模式：技术、产品、服务整体托管

多种形态
全面助力建成

- 城市运营中心
- 行业安全运营中心
- 企业安全运营中心

两化融合
帮您真正实现

- 集中服务化：统一监测、预警与通报
- 服务集中化：标准统一、质量可控、资源共享

首创“云地结合”模式

打破传统的托管仅限“云端监测”的认知开辟“云地结合”模式，云端+地端实现真正的闭环服务。

7*24h实时持续监测

“地球不爆炸，我们不放假”——7*24h持续监测，充分保障常态化运营。

安全事件响应快一步

对APT攻击、网络攻击等长效监测，提前预警，响应快一步。

安全事件处置规范化

事前检测、事中分析、事后总结，真正实现闭环，并在实战中不断加固。

专家“一对一”指导

专家通过视频一对一的方式与您“面对面”沟通指导，不仅让您了解现状，还能防患于未然。

世界就是一个巨大的草台班子吗?

3 月底，开源软件领域披露了一场差点就要成功的软件供应链攻击：广泛采用提供数据压缩功能的开源 XZ Utils 组件，被发现植入后门。

这个后门被评为 CVSS 10 分（严重程度最高级），在全球安全领域引发了一阵新的忙乱。如果未被及时发现，将会酝酿出一场重大的全球网络安全危机。安全专家表示，这可能是开源项目有史以来最复杂的供应链攻击。攻击的复杂程度反映出攻击者是经过精心策划才实施的：攻击者逐步获得合法开发人员的信任，甚至成为其核心维护团队的成员，从而使能在不被注意的情况下植入后门。

现在，手机、汽车、飞机，甚至许多尖端人工智能程序都使用开源软件。《 2024 年开源安全与风险分析报告 》发现，其所研究的代码库中 96% 包含开源代码。

XZ 后门还揭露出软件安全的残酷真相——企业软件堆栈中使用的大部分开源代码都来自资源不足、由志愿者运行的小型项目，其中的很多项目可能由于资源问题而不再更新。令人讽刺的是，XZ 后门的发现纯粹是由于运气——是由注意和调查性能问题下降的软件开发人员发现的。

这让人想起据称是来自马斯克的一句话——世界就是一个巨大的草台班子。繁华城市的桥梁楼宇，最后决定其安全与质量的，可能是一群缺乏基础培训的农民工。XZ 后门凸显出开源生态系统中关键点的脆弱性，以及维护者倦怠造成的持续的真实风险。

实际上，随着开源的普及和使用的不断增长，开源风险已经不断演变。对软件供应链有计划的、蓄意的攻击现在日益普遍。供应链安全公司 ReversingLabs 在 2024 年报告《 软件供应链安全状况 》中指出，过去三年中，源自开源软件包存储库的威胁增加了 1,300% 以上。

依靠开源生态系统的开放性，我们很幸运地在造成巨大损害之前发现这次供应链攻击。但下一次，我们可能就没那么幸运了。

与其他开源项目一样，XZ Utils 是由志愿者运行的。此类项目通常几乎没有资源来处理安全问题，这意味着，组织需要自行承担使用该软件的风险，安全和开发团队必须像管理内部开发的代码一样管理开源风险。

现在你需要认真考虑用奇安信的开源卫士等工具，进行全面的开源组件检查。这一覆盖 800 万开源项目、1.3 亿开源软件版本、20 万 + 开源软件漏洞的工具，可以让你清晰了解所使用的开源组件及风险。

世界可能是一个巨大的草台班子，但你肯定不能是。

总编辑

2024 年 4 月 1 日

CONTENTS 目录

安全态势

月度专题

XZ 后门：开源项目最复杂供应链攻击 P13

震惊开源社区的 XZ 恶意后门，揭开了一场精心策划、实施多年的供应链攻击，这一对 Linux 系统构成严重威胁的事件，为开源软件安全再次敲响警钟。国内外安全专家给出了应对方案。

安全之道

报告速递

专　栏

奇安资讯

《网安 26 号院》编辑部
主办　奇安信集团

总　编　辑：李建平
安全态势主编：王　彪
月度专题主编：李建平
安全之道主编：张少波
奇安资讯主编：陈　冲
报告速递主编：刘川琦
专　栏主编：李建平

奇安信集团　虎符智库　安全内参

索阅、投稿、建议和意见反馈，请联系奇安信集团公关部

索阅邮箱：26hao@qianxin.com
地　　址：北京市西城区西直门外南路 26 院 1 号
邮　　编：100044
联系电话：（010）13701388557
出版物准印证号：京内资准字 2123- L0058 号
编印单位：奇安信科技集团股份有限公司
发送对象：奇安信集团内部人员
印刷数量：4500 本
印刷单位：北京博海升彩色印刷有限公司
印刷日期：2024 年 4 月 26 日

政策篇

国内，数据要素安全受重视。国家网信办公布《促进和规范数据跨境流动规定》，更新数据跨境流动安全要求；《数据安全技术 数据分类分级规则》国标发布，确定重要数据识别指南；自然资源、银行保险行业纷纷发布管理办法，推动行业数据安全规范化。

国际上，美国 CISA 发布关键基础设施网络事件报告拟议规则，制定了关键基础设施如何向政府报告网络攻击事件的细则要求，据估算未来 11 年该规定的合规成本将达到 26 亿美元。

国内

国家金监总局《反保险欺诈工作办法》公开征求意见

4 月 11 日，国家金融监管总局起草了《反保险欺诈工作办法（征求意见稿）》，公开征求意见。该文件共六章三十七条，包括总则、反欺诈监督管理、保险机构欺诈风险管理、反欺诈行业协作、反欺诈各方协同、附则。该文件提出，保险机构和行业组织应按照职责分工统筹网络安全、数据安全与创新发展，依法履行安全保护义务，完善管理制度，加强网络安全和数据安全防护，保障必要的人员和资源投入，采取网络安全、数据安全管理和技术措施，确保反欺诈信息系统安全可控运行。

自然资源部印发《自然资源领域数据安全管理办法》

3 月 28 日，自然资源部印发《自然资源领域数据安全管理办法》，以规范自然资源领域数据处理活动，加强数据安全管理。该文件共七章三十七条，包括总则、数据分类分级管理、数据全生命周期安全管理、数据安全监测预警与应急管理、监督检查、法律责任、附则。该文件指出，自然资源领域数据是指在开展自然资源活动中收集和产生的数据，主要包括地理信息数据、自然资源调查监测数据、国土空间规划数据、自然资源管理数据。数据处理者应当定期按照自然资源领域数据分类分级标准规范梳理填报重要数据和核心数据目录，并对数据处理活动安全负主体责任。

国家金监总局《银行保险机构数据安全管理办法》公开征求意见

3 月 22 日，国家金融监督管理总局起草了《银行保险机构数据安全管理办法（公开征求意见稿）》，现公开征求意见。该文件共九章八十一条，包括总则、数据安全治理、数据分类分级、数据安全管理、数据安全技术保护、个人信息保护、数据安全风险监测与处置、监督管理、附则。该文件提出，银行保险机构应当建立与本机构业务发展目标相适应的数据安全治理体系，建立健全数据安全管理制度，构建覆盖数据全生命周期和应用场景的安全保护机制，开展数据安全风险评估、监测与处置，保障数据开发利用活动安全稳健开展。

国家网信办公布《促进和规范数据跨境流动规定》

3 月 22 日，国家互联网信息办公室公布《促进和规范数据跨境流动规定》，自公布之日起施行。该文件对数据出境安全评估、个人信息出境标准合同、个人信息保护认证等数据出境制度作出优化调整，明确了重要数据出境安全评估

申报标准，提出未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估，规定了免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的数据出境活动条件，还设立了自由贸易试验区负面清单制度等。

《数据安全技术 数据分类分级规则》等 5 项网络安全国家标准获批发布

3 月 21 日，根据 2024 年 3 月 15 日国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2024 年第 1 号），全国网络安全标准化技术委员会归口的 5 项网络安全国家标准正式发布。其中包括 1 项新发布标准《数据安全技术 数据分类分级规则》，4 项更新标准《信息技术 安全技术 抗抵赖 第 1 部分：概述》《信息技术 安全技术 抗抵赖 第 3 部分：采用非对称技术的机制》《信息技术 安全技术 实体鉴别 第 4 部分：采用密码校验函数的机制》《信息技术 安全技术 信息安全管理 监视、测量、分析和评价》。

国际

美国会议员公布《美国隐私权法案》，推动联邦隐私立法

4 月 7 日，美国众议员 Cathy Rodgers 和参议员 Maria Cantwell 公布了《2024 年美国隐私权法案》草案。该文件长达 53 页，内容包括数据最小化要求、消费者选择不接收定向广告的权利，以及查看、更正、导出或删除其数据的权利。此外，该法案还包括数据安全条款、国家数据中介登记处。当存在重大隐私损害发生时，保护组织机构免于执行强制性仲裁的部分。

美国防部发布《2024 年国防工业基础网络安全战略》

3 月 28 日，美国国防部发布《2024 年国防工业基础网络安全战略》，旨在加强美国防部与国防工业基础（DIB）合作，进一步协调和统筹资源，以提高美国国防供应商和生产商的网络安全。该战略旨在通过涵盖 2024 财年至 2027 财年的总体愿景和使命来增强 DIB 的网络安全和网络弹性，即“安全、有弹性、技术先进的国防工业基础”和“通过保护敏感信息、作战能力和产品完整性，确保美国作战能力的生成、可靠性和维持”。该战略概述了 4 项主要目标，包括加强 DBI 网络安全治理结构、增强 DIB 网络安全态势、保持关键 DIB 功能的弹性、改善与 DIB 的网络安全合作。

美国 CISA 发布关键基础设施网络事件报告拟议规则

4 月 4 日，美国网络安全和基础设施安全局 (CISA) 发布关键基础设施网络事件报告拟议规则，基于 2022 年《关键基础设施网络事件报告法案》授权，制定了关键基础设施如何向政府报告网络攻击事件的细则要求。这是美国联邦政府首次提出一套跨关键基础设施部门的全面网络安全规则。CISA 正在就规则草案征求公众意见，为期 60 天。CISA 估计，未来 11 年该规定的合规成本将达到 26 亿美元，即每年约 2.3 亿美元，其中行业成本为 14 亿美元，联邦政府成本为 12 亿美元。

联合国大会通过首个有关人工智能的决议草案

3 月 21 日，联合国大会一致通过一项决议，呼吁抓住“安全、可靠和值得信赖的”人工智能系统带来的机遇，让人工智能给人类带来“惠益”，并以此促进可持续发展。据介绍，这是联合国大会首次就监管人工智能这一新兴领域通过决议。决议草案由美国提交，同时还有 120 多个会员国成为“共同提案国”或表达支持。决议表示，各国认识到，“人工智能系统的设计、开发、部署和使用速度加快，技术变革日新月异，对加快实现可持续发展目标具有潜在影响”。为此，大会“决心促进安全、可靠和值得信赖的人工智能系统，以在全面实现《2030 年可持续发展议程》方面加快取得进展”。

事件篇

全球再掀数据泄露狂潮，多国发生重大泄露事件。美国 AT&T 公司承认超 5000 万用户数据泄露，已在地下论坛售卖多年；法国政府机构劳动局泄露 4300 万公民个人数据，被泄信息的时间跨度长达 20 年；连锁药房系统遭网络攻击，导致爱沙尼亚近半人口数据泄露。

中国代工巨头旗下芯片公司遭网络攻击，大量数据外泄并被勒索

4 月 12 日 Techzine 消息，中国智能手机代工巨头闻泰科技旗下荷兰芯片制造商安世半导体（Nexperia）遭到了黑客攻击。实施这次攻击的犯罪团伙 Dunghill Leak 为未授权渗透测试，声称窃取了 1TB 敏感数据，但仍要求安世半导体支付费用，否则将放出敏感的商业秘密数据。据悉数据泄露已经开始，数十份机密文件已在暗网上发布。安世半导体确认此次攻击事件发生在 3 月，并已向警方和荷兰个人数据管理局报告了发现的情况。

菲律宾科技部服务器遭黑客入侵：网站被篡改 25TB 数据被删除

4 月 3 日 Manila Bulletin 消息，一家名为 Ph1ns 的黑客组织宣布对菲律宾科技部的服务器进行了毁灭性攻击。该组织声称，已经获得对虚拟机管理器、网络附加存储（NAS）和路由器等关键基础设施的访问权限，甚至获取了域管理员权限，从而能够无限制地访问员工的计算机。雪上加霜的是，他们还夸耀称加密了域控制器，有效地封锁了授权用户的访问，并在受攻击服务器上留下信息：“这个网站被菲律宾人民夺取了！”菲律宾信息和通信技术部的消息人士透露，黑客删除了 25TB 数据，造成一片混乱。菲律宾信息和通信技术部基础设施管理、网络安全和技能提升副秘书长 Jeffrey Ian C. Dy 表示：“内部报警系统在夜间 10 点左右检测到了对科技部的攻击，我们正在与科技部合作，尽快恢复他们的服务，并提高我们的检测和事件响应能力。”

AT&T 承认超 5000 万用户数据泄露：已在地下论坛售卖多年

4 月 10 日 BleepingComputer 消息，美国电信巨头 AT&T 向 5100 万名用户发出数据泄露通知，告知他们的个人信息已在一个黑客论坛上被泄露。但是，该公司尚未透露黑客如何获取了这些数据。据悉，这批数据已在黑客论坛上被反复售卖，最早在 2021 年，就有用户 @ShinyHunters 以 100 万美元价格公开出售；今年 3 月，用户 @MajorNelson 在论坛上公开了整个数据集。整个数据集有超过 7100 万人的信息，由于一人多账号等原因，AT&T 官方称受影响用户为约 5100 万人。AT&T 还在通知中给出一年的身份盗窃保护服务和缓解措施。

英国宠物医院巨头被黑后运营受严重扰乱，猫狗和数据都面临风险

4 月 8 日 The Register 消息，英国最大宠物医疗连锁机构 CVS 集团宣布遭遇了一起“网络事件”，可能有数据被盗取，部分机构的临床护理受到影响。由于此次网络事件，CVS 集团被迫启动事件响应计划，下线 IT 系统以隔离事件影响。公司表示，临时关闭 IT 系统“在过去一周对运营产生重大干扰”，预计这种干扰还将持续数周。为了评估损害程度并支持采取应对措施，CVS 集团已聘请外部安全专家进行调查。CVS 集团表示，此次事件迫使公司加速实施云迁移策略。由于云解决方案能够增强安全性并提高运营效率，公司正在迁移机构管理系统及相关基础设施。

连锁药房系统遭网络攻击，导致爱沙尼亚近半人口数据被泄露

4 月 4 日 Cybernews 消息，连锁药房 Apotheca 的系统遭到破坏，导致爱沙尼亚近一半人口的个人数据被泄露。该国执法人员调查称，此次违规行为影响了 Apotheca 的会员及另外两家连锁店 Apotheca Beauty、PetCity 的用户。被盗数据库由 Allium UPI 运营，该公司主要经营药品和医院用品。Allium UPI 在 2 月首次报告了此事件，称其管理的会员卡系统遭到破坏，客户的个人代码、购买数据和联系数据被网络犯罪分子获取。执法人员调查后确认，被盗信息包含近 70 万人个人 ID、超 40 万封电子邮件、近 6 万个家庭地址、约 3 万个电话号码及约 4300 万次购买的详细信息，运营商 Allium UPI 未采取足够的安全措施，导致系统被入侵。

首个公开针对 AI 工作负载的大规模攻击：数千台服务器被黑

3 月 28 日 ArsTechnica 消息，网络安全厂商 Oligo Security 发现人工智能领域主流算力框架 Ray 的一个未修复安全漏洞（CVE-2023-48022）正被黑客野外大规模利用，导致数千台存放 AI 工作负载和网络凭证的服务器被黑，敏感数据和算力遭窃取。据了解，这些攻击已经持续了 7 个月，攻击者不仅篡改了 AI 模型，还泄露了访问内部网络和数据库的网络凭证，并获取了 OpenAI、HuggingFace、Stripe 和 Azure 等平台账号的访问令牌。除了破坏模型和窃取凭证，攻击者还在能够提供大量算力的被侵入基础设施上安装了加密货币挖矿软件，并设置了反向 Shell，以实现对服务器的远程控制。根据 Oligo 过去几周的监测，可能已遭到攻击的机器和算力总估值近 10 亿美元。

越南头部券商遭黑后服务中断，当地股市交易量骤降 10%

3 月 27 日 The Record 消息，越南第三大证券经纪公司 VNDirect 在周末遭遇网络攻击，目前正全力恢复运营。VNDirect 首席执行官 Nguyen Vu Long 表示：“公司被一群专业黑客攻击，数据遭到加密。”他说，“我们已成功解密这些数据，现在开始系统恢复工作。”该公司 27 日宣布部分服务已经恢复上线，但据当地媒体报道，投资者仍然无法登录平台。据路透报道，由于使用 VNDirect 的投资者无法交易，胡志明市证券交易所 25 日的交易量下降了 10%。河内证券交易所宣布，“在问题得到解决之前”暂时中断 VNDirect 的远程或在线衍生证券交易、债务工具交易和个人公司债券交易。

富士通多个系统感染恶意软件，客户数据遭窃取

3 月 18 日 Bleeping Computer 消息，日本科技巨头富士通披露了一起重大网络安全事件，该公司的一些系统遭到恶意软件感染，客户的敏感信息可能已经被窃取。公司公告称：“我们确认公司多台计算机感染了恶意软件，经过内部调查发现，客户的个人信息和相关文件可能已被非法窃取。发现恶意软件后，我们迅速隔离了受影响的商务电脑，并采取了加强其他商务电脑监控等措施。”富士通表示，将继续调查恶意软件是如何侵入其业务系统，以及窃取了哪些数据。虽然该公司表示没有收到客户数据被滥用的报告，但他们已经将此事件通知了日本个人信息保护委员会，并正在为受影响的客户准备单独的通知函。

法国政府机构劳动局泄露 4300 万公民个人数据

3 月 14 日 The Register 消息，法国政府负责登记和协助失业者的法国劳动局（France Travail）日前披露，高达 4300 万公民的信息遭到窃取。该机构已向法国数据保护监管机构（CNIL）报告这起事件，其导致大量个人信息被暴露，被泄信息的时间跨度长达 20 年。法国劳动局称，泄露的信息包括姓名、出生日期、社会保障号码、法国劳动局标识符、电子邮件地址、邮政地址和电话号码。目前尚未发现用户密码和银行支付信息受到影响。CNIL 警告称，在此次事件中被窃取的数据可能与其他入侵事件中被窃数据相关联，可以用来构建关于任何具体个人的更大信息库。

漏洞篇

开源软件项目 XZ Utils 被曝植入后门 (CVE-2024-3094)，攻击者通过一系列社会工程学手段取得信任并接管项目，当满足一定条件时，将会解密流量里的 C2 命令并执行。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Palo Alto Networks PAN-OS 命令注入漏洞安全风险通告

4 月 15 日，奇安信 CERT 监测到 Palo Alto Networks PAN-OS 命令注入漏洞 (CVE-2024-3400)，Palo Alto Networks PAN-OS 软件的 GlobalProtect 功能中针对特定 PAN-OS 版本和不同功能配置下，未经身份验证的攻击者可能利用此漏洞在防火墙上以 root 权限执行任意代码。目前该漏洞已发现在野利用。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

Rust 命令注入漏洞 (CVE-2024-24576) 安全风险通告

4 月 11 日，奇安信 CERT 监测到 Rust 官方发布新版本修复 Rust 命令注入漏洞 (CVE-2024-24576)。在 Windows 上使用 Command API 调用批处理文件（使用 bat 和 cmd 扩展名）时，Rust 标准库没有正确地对参数进行转义。攻击者如果能够控制传递给生成的进程的参数，就可以通过绕过转义来执行任意的 Shell 命令。目前该漏洞 PoC 已在互联网上公开，鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

微软 2024 年 4 月补丁日多个产品安全漏洞风险通告

4 月 10 日，微软补丁日共发布了 149 个漏洞的补丁程序，修复了 SQL Server、Microsoft Office Outlook、Windows Kernel 等产品中的漏洞。经研判，有 17 个重要漏洞值得关注（包括 3 个紧急漏洞、14 个重要漏洞），如下表所示。鉴于这些漏洞危害较大，建议客户尽快安装更新补丁。

编号	漏洞名称	风险等级	公开状态	利用可能
CVE-2024-26234	代理驱动程序欺骗漏洞	重要	公开	在野利用
CVE-2024-21323	用于 IoT 的 Microsoft Defender 远程代码执行漏洞	紧急	未公开	一般
CVE-2024-29053	用于 IoT 的 Microsoft Defender 远程代码执行漏洞	紧急	未公开	一般
CVE-2024-21322	用于 IoT 的 Microsoft Defender 远程代码执行漏洞	紧急	未公开	一般
CVE-2024-28903	安全启动安全功能绕过漏洞	重要	未公开	较大
CVE-2024-28921	安全启动安全功能绕过漏洞	重要	未公开	较大
CVE-2024-26241	Win32k 权限提升漏洞	重要	未公开	较大
CVE-2024-26158	Microsoft 安装服务权限提升漏洞	重要	未公开	较大
CVE-2024-26230	Windows 启用电话服务器权限提升漏洞	重要	未公开	较大
CVE-2024-26209	Microsoft 本地安全认证子系统服务信息泄露漏洞	重要	未公开	较大
CVE-2024-26185	Windows 压缩文件夹篡改漏洞	重要	未公开	较大
CVE-2024-26218	Windows 内核权限提升漏洞	重要	未公开	较大
CVE-2024-26212	DHCP 服务器服务拒绝服务漏洞	重要	未公开	较大
CVE-2024-26211	Windows 远程访问连接管理器权限提升漏洞	重要	未公开	较大
CVE-2024-29056	Windows 身份验证权限提升漏洞	重要	未公开	较大
CVE-2024-26256	Libarchive 远程代码执行漏洞	重要	未公开	较大
CVE-2024-29988	SmartScreen 提示安全功能绕过漏洞	重要	未公开	较大

Ivanti Connect Secure IPSec 组件堆越界写漏洞 (CVE-2024-21894) 安全风险通告

4 月 9 日，奇安信 CERT 监测到 Ivanti 官方发布补丁修复多个漏洞。奇安信天工实验室安全研究员协助 Ivanti 修复 3 个 Ivanti Connect Secure(ICS) 产品安全漏洞。其中，CVE-2024-21894 IPSEC 组件堆越界写漏洞和 CVE-2024-22053 IPSEC 组件堆越界读漏洞两个漏洞，攻击者通过构造恶意请求，在特定条件下可触发任意代码执行；CVE-2024-22052 IPSEC 组件空指针漏洞可被攻击者用于引发拒绝服务攻击。鉴于上述漏洞影响范围较大，建议客户尽快做好自查及防护。

JumpServer 多个高危漏洞安全风险通告

4 月 1 日，奇安信 CERT 监测到 JumpServer 远程代码执行漏洞 (CVE-2024-29201)、JumpServer 后台模板注入漏洞 (CVE-2024-29202)。在 CVE-2024-29201 中，攻击者可以绕过 JumpServer 的 Ansible 中的输入验证机制，在 Celery 组件中执行任意代码；在 CVE-2024-29202 中，攻击者可以利用 JumpServer 的 Ansible 中的 Jinja2 模板注入漏洞在 Celery 组件中执行任意代码。由于 Celery 组件以 root 权限运行并具有数据库访问权限，因此攻击者可以从所有主机窃取敏感信息或操纵数据库。鉴于这些漏洞影响范围较大，建议客户尽快做好自查及防护。

XZ Utils 工具库恶意后门植入漏洞安全风险通告

3 月 30 日，奇安信 CERT 监测到 XZ Utils 工具库恶意后门植入漏洞 (CVE-2024-3094)，3 月 29 日有开发人员在安全邮件列表上发帖称，他在调查 SSH 性能问题时发现了涉及 XZ 包中的供应链攻击，进一步溯源发现 SSH 使用的上游 liblzma 库被植入了后门代码，当满足一定条件时，将会解密流量里的 C2 命令并执行。目前，企业使用的主流 Linux 发行版（Red Hat/CentOS/Debian/Ubuntu）的 Stable 稳定版仓库中尚未合并该存在后门的软件版本，鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

泛微 E-Office10 远程代码执行漏洞安全风险通告

3 月 28 日，奇安信 CERT 监测到泛微 E-Office10 远程代码执行漏洞 (QVD-2024-11354) 在互联网上公开，由于系统处理上传的 PHAR 文件时存在缺陷，未经身份验证的远程攻击者能够上传伪装的恶意 PHAR 文件到服务器，从而在目标服务器上执行任意代码。目前该 PoC 已在互联网上公开，鉴于该漏洞影响范围较大，利用简单，建议客户尽快做好自查及防护。

Adobe ColdFusion 任意文件读取漏洞安全风险通告

3 月 26 日，奇安信 CERT 监测到 Adobe ColdFusion 发布新版本，修复了 Adobe ColdFusion 任意文件读取漏洞 (CVE-2024-20767)。由于 Adobe ColdFusion 的访问控制不当，未经身份认证的远程攻击者可以构造恶意请求读取目标服务器上的任意文件，泄露敏感信息。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

Atlassian Confluence 路径遍历漏洞安全风险通告

3 月 21 日，奇安信 CERT 监测到 Atlassian Confluence 路径遍历漏洞 (CVE-2024-21677)，未经身份验证的远程攻击者需要与受害者交互来利用该漏洞，成功后可对 Confluence 服务器机密性、完整性和可用性造成严重影响。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

注：使用公司邮箱发送企业名称和需开通订阅的邮箱地址至 cert@qianxin.com，即可申请订阅最新漏洞通告。

对抗篇

国内攻防演习 3 月态势：哪些薄弱点最易被利用？

作者 | 奇安信安服团队

一、本月演习整体情况

2024年3月，奇安信Z-TEAM团队共承接攻防演习服务 15 场，地市级攻防演习 2 场，客户自主攻防演习 13 场。

本月承接攻防演习数量与上月对比呈明显上升趋势（见图 1）。

本月承接的攻防演习涉及金融、政府部委、运营商行业较多，此情况较上月承接攻防演习涉及行业范围数据变化较大，金融、政府部委、运营商行业攻防演习数量明显增多（见图 2）。

本月攻防演习成果如表 1 所示：

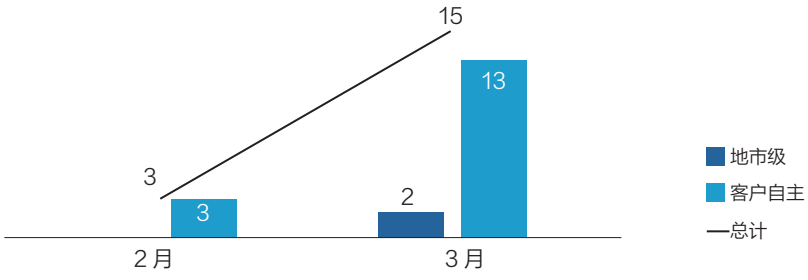


图 1 2-3 月 Z-TEAM 承接攻防演习数量统计

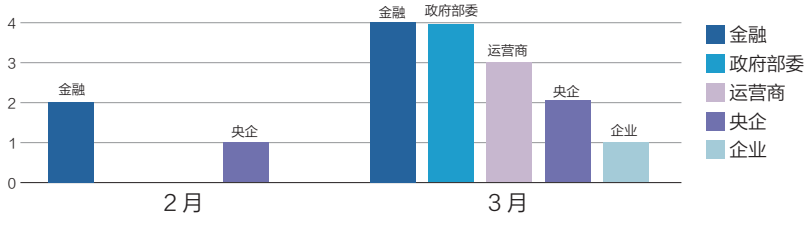


图 2 2024 年攻防演习涉及行业统计

目标系统	靶标	强隔离内网	核心业务网	网站	堡垒机	安全设备	业务系统	服务器
数量	21	33	38	66	31	53	312	996

表 1

二、本月任务目标特点

本月攻防演习和评估任务覆盖行业比较集中，涉及目标包括金融、政府部委、央企、运营商、传媒、企业等行业。随着计算机网络技术的不断发展，运营商业务日趋数字化和网络化，网络安全威胁也日渐繁多且复杂多样，运营商处理大量的用户数据，包括个人身份信息、通信记录等。如果网络攻击、勒索软件和其他安全威胁可能导致系统故障、服务中断和数据丢失，这些数据可能会被窃取、篡改或滥用，给用户和运营商带来严重的风险和损失。因此，运营商应高度重视网络安全，并采取有效措施来防范和应对安全威胁。在本月攻防演习中，运营商行业占比为 20%（见图 3）。

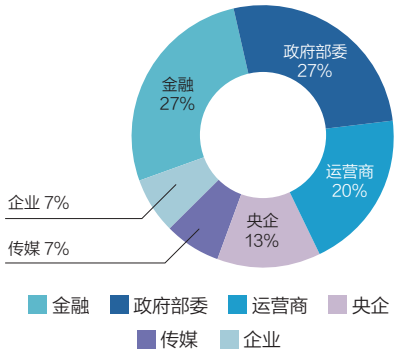


图 3 3 月攻防演习分布

三、主要攻击手段分析

基于本月奇安信 Z-TEAM 团队实战成果分析，本月任务中对多行业不同目标网络进行攻击分析，总结了各个行业的攻击特点。如央企、传媒行业外网突破的主要攻击手段包括漏洞扫描利用和口令爆破等；运营商、企业、金融行业的主要攻击手段包括漏洞扫描利用和 VPN 仿冒接入、钓鱼攻击等；政府部委外网突破的主要攻击手段包括漏洞利用、隐秘隧道外联等。本月攻击队突破目标安全防护使用的主要技术手段分布如下（见图 4）。

本月攻防演习服务中，攻击队使用攻击手段主要有：漏洞扫描利用、钓鱼攻击、口令爆破、VPN 仿冒接入、隐秘隧道外联，供应链攻击技术等。

整体攻击手段与上月对比，漏洞扫描利用和隐秘隧道外联手段利用率基本趋同，钓鱼攻击和供应链攻击有明显下降趋势，VPN 仿冒接入和口令爆破有明显上升趋势（见图 5）。

本月任务中运营商行业攻防演习任务占比五分之一，通过对该行业的演习数据分析，发现攻击队的外网纵向突破重点是寻找薄弱点，并利用历史漏洞和钓鱼攻击手段结合实现突破。内网横向移动则采用弱口令爆破、VPN 仿冒接入、隐秘隧道外联等攻击手段来实现横向拓展和渗透。在攻防演习中，攻击者通常需要多种攻击手段相互配合才能成功地进行渗透和拓展。

四、典型攻击手段实现案例

随着信息通信技术的日新月异，网络安全问题逐渐凸显，如计算机病毒木马的扩散、系统安全漏洞的暴露及网络违法犯罪的频发等。这些问题对运营商而言，不仅是一个重要的考量因素，更是他们必须面对和解决的挑战。运营商只有通过不断强化网络安全措施，确保用户数据的安全性和隐私性得到充分的保障，及时应对网络安全事件，才能赢得用户的信任，保护自身的业务运营能够持续稳定地进行。因此，其对于网络安全的要求十分严苛，这决定了运营商行业攻防安全验证的必要性。通过网络攻防演练对运营商的网络平台和信息系统进行全方位渗透测试，旨在挖掘可能引发数据泄露、资产受损、系统被篡改

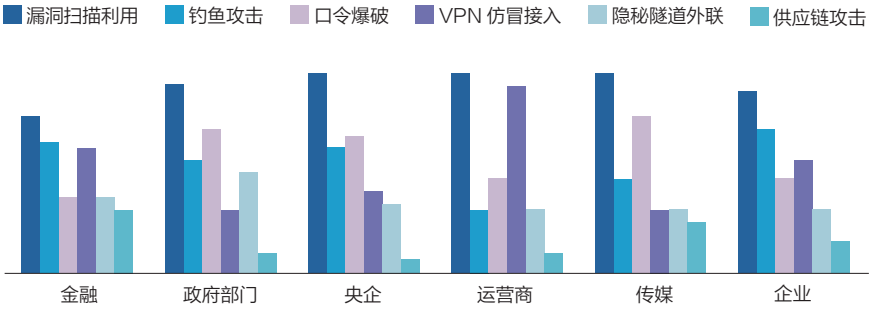


图 4 行业攻击手段分布

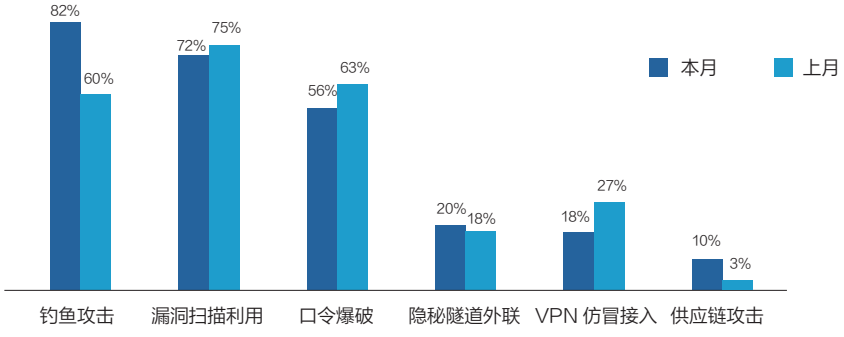


图 5 攻击手段对比

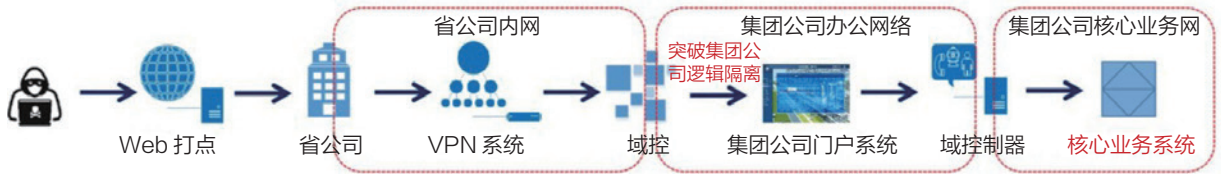


图 6 案例攻击路线图

等安全风险的漏洞，从而为客户提供及时的安全隐患发现服务，未雨绸缪，确保客户的网络空间安全。

案例：漏洞利用结合 VPN 仿冒接入突破目标

在最近的一次针对某运营商的攻防演练中，奇安信攻击队在确定了攻击目标后，进行了深入的侦察和探测工作，但并未发现集团公司网络上存在任何可利用的安全薄弱点。于是攻击队对目标企业的域名、IP 段、端口和业务信息等进行全面地收集，并对可能存在的漏洞进行了尝试性攻击。结果发现大部分目标对象或已停止服务，或配置了高级别的安全防护设施。鉴于当前不存在 0day 漏洞，且时间紧迫，攻击队果断放弃正面突破。

既然未在集团公司网络上发现任何可利用的薄弱点，攻击队决定转变攻击策略，经过细致的信息搜集与分析，将矛头指向省公司。团队根据目标业务地域分散的特点，决定对省公司进行细致的侦查，期望实现“李代桃僵”。在全面的信息收集过程中，攻击队利用目标业务地域分散，外地业务需要 VPN 通联的特点，通过 VPN 网关漏洞实现仿冒接入分支机构业务子网，进一步向集团公司业务网络拓展渗透。

攻击队首先针对目标展开了详尽的外网信息搜集工作。在搜集探测的过程中，他们发现了某省公司网络接入 Fortinet VPN 网关的入口。经过进一步分析，攻击队发现该 VPN 网关存在一个严重的任意文件读取漏洞。利用这一漏洞，攻击队成功地获取了入口 VPN 的用户名和密码。接着，他们利用这些信息仿冒登录 VPN，成功地接入了目标内网。

攻击队通过内网横向渗透提取分公司工作域控 HASH，控制该工作域网络，并控制大量域内服务器与重点系统，进一步通过搜集获取的口令复用账户 xxxxx/xxxx，利用任意文件上传漏洞获取总公司门户权限。通过数据库命令执行、口令复用等内网横向方式获取大量服务器权限。

攻击队首先利用 Tomcat 服务器的弱口令漏洞，上传了恶意的 WAR 包，从而获得了开发测试阶段的初步入口点权限。随后，他们利用 Weblogic 的反序列化漏洞、弱口令及 HASH 传递等多样化手段，在内网中进行了横向渗透和移动。经过一系列精细操作，最终成功获取了 50 台域控制器的权限，进而实现对多个工作域的接管。这一行动使攻击队控制了总计 4 万台机器的权限，涵盖了众多关键业务系统和数据服务器。攻击队成功地实现了对关键业务域网络的突破，并掌握了对大量目标核心业务应用系统、业务数据服务器的控制权。

五、安全加固建议

1. 案例剖析

运营商作为国家关基组成部分，是国内最早入场安全防护建设的行业之一，在经历多年的安全运营和攻防沉淀，建立了具备企业特色的安全运营体系，可以监测发现网络安全风险并有效处置。

然而，运营商庞大的企业规模，拥有复杂的分布式网络和供应链体系，致使存在安全防护盲区和短板，导致攻击队成功突破企业安全防护壁垒进入内网，通过内网层层突破，最终拿下了大量服务器权限和核心生产设备控制权。

案例暴露问题：存在“安全运营体系”和“网络层风险检测”缺失的问题。

2. 防护策略

安全防护建设应该具备一体化视角，能力建设应结合安全运营体系，多点布防、以点带面、多面成体，形成纵深防御体系，安全防护能力的分层防护作为防护基础，安全运营的人机一体化提升防护效率，通过《安全运营驻场服务》《攻击队评估服务》，提升现有安全防护能力不足。

《安全运营驻场服务》：提供专业安全团队在现场提供持续技术支持，深度参与客户安全运营体系，提供服务内容包括实时监控、安全设备管理、应急响应、安全事件处理等。确保信息系统稳定运行，提高安全防护能力利用效率。

《攻击队评估服务》：通过模拟高级威胁攻击手法全面评估客户网络安全防护能力。基于 ATT&CK 框架，提供详细的攻防分析报告，包括企业安全漏洞和加固建议。旨在提高客户网络安全防御水平，确保业务安全稳定。安

XZ 后门：开源项目最复杂供应链攻击

震惊开源社区的 XZ 恶意后门，揭开了一场精心策划、实施多年的供应链攻击，这一对 Linux 系统构成严重威胁的事件，为开源软件安全再次敲响警钟，国内外安全专家给出了应对方案。

揭秘：开源项目有史以来最复杂供应链攻击

2024 年 3 月 29 日，微软软件工程师披露了震惊开源社区的 XZ 恶意后门——严重程度高达 10 级（CVSS 最高级）的远程代码执行后门。由此揭开了一场精心策划实施多年、对 Linux 系统构成严重威胁的供应链攻击事件。

这一被称为开源史上最复杂的供应链攻击，为开源软件安全再次敲响警钟。开源软件开放和协作开发模式可能早已悄然引入我们毫无防备的潜在威胁。2024 年《软件供应链安全状况》报告发现，过去三年，源自开源软件包存储库的威胁增加了 1,300% 以上。

XZ 后门事件提醒业界，应对开源软件隐藏的安全威胁已成为数字经济时代无法回避的棘手挑战，我们现在就需要着手，从开源软件安全开始保护脆弱的网络空间。

> XZ 后门事件被称为开源史上
> 最复杂的供应链攻击，
> 为开源软件安全再次敲响警钟。

纯属侥幸的发现

3 月 29 日，在微软公司从事 PostgreSQL 开发人员的软件工程师 Andres Freund，在对 Debian Linux（Beta 版）系统进行测试时，发现其 SSH（远程设备访问协议）远程安全代码运行缓慢。

这一异常的性能问题引发他的好奇，在进一步调查中，Freund 发现了 XZ Utils 中的可疑更新，最终暴露了精心策划的后门，并将其发布到 Openwall oss-security 邮件列表中。

XZ Utils 提供基本无损数据的压缩功能，被广泛采用并集成到类 Unix 操作系统（包括 Linux）中，使其成为跨不同计算环境压缩和解压缩数据的不可或缺的工具。

XZ 后门事件被称为自 Solarwinds 以来最大的供应链攻击尝试。计算机科学家亚历克斯 · 斯塔莫斯 (Alex Stamos) 表示，“借助这一后门，攻击者就会获得一把万能钥匙，可以打开全世界数亿台计算机中的任何一台。”

XZ 后门的序号为 CVE-2024-

3094，其 CVSS 评级为 10 分（最高分）。红帽公司发布了有关的安全警报。美国网络安全和基础设施安全局 (CISA) 也发布警告，建议开发者和用户将 XZ Utils 降级到未受影响的版本。

迄今为止，已确认受到攻击影响的 Linux 发行版包括 Fedora Rawhide 和 Fedora Linux 40 beta（不包括红帽企业 Linux）、openSUSE Tumbleweed 和 openSUSE MicroOS、Kali Linux 和 Arch Linux。

这意味着，如果这一后门未被及时发现，未来将会酝酿出一场重大的全球网络安全危机——可能以一波勒索软件事件的形式出现，或者作为看不见的致命漏洞，使攻击者在被发现之前随意访问世界各地的大量计算机。

讽刺的是，这一差点就要成功的供应链攻击的发现，完全是因为偶然。正如 Kubernetes SIG 安全联合主席 Ian Coldwater 所表示，这个后门是由注意和调查性能问题下降的软件开发人员（Freund 不是安全研究员或逆向工程师）所发现，基本上纯粹是由于运气，这也凸显了开源社区需要进行更严格的安全测试和对供应链攻击保持警惕。

精心策划的攻击

安全专家表示，这可能是开源项目有史以来最复杂的供应链攻击。攻击的复杂程度是前所未有的，反映出攻击者是经过精心策划才实施的。另一位开源维护者认为：“这可能是我们见过的执行得最好的供应链攻击。”

> 持续多年的耐心行动，
> 加上植入后门本身的技术特点和复杂性，
> 让网络安全界的许多人相信，
> 攻击者实际上是由国家支持的黑客。

目前，网络攻击者越来越多地采用软件供应链攻击。一般的软件供应链攻击多是在软件开发过程中设法入侵关键账户，借此将恶意内容植入到合法软件中，但这些攻击通常会很快被检测到。

XZ 后门事件的情况则完全不同——攻击者精心计划，实施多年。攻击活动似乎酝酿了三年之久，可能从 2021 年起就已计划和实施了，目标是多个 Linux 发行版。攻击者逐步获得合法开发人员的信任，甚至成为其核心维护团队的成员，从而使能在不被注意的情况下，在 XZ 植入后门。XZ Utils 5.6.0 和 5.6.1 版本被植入后门的复杂性也说明，攻击者为渗透关键软件基础设施而付出的精心努力。

后续的溯源发现，XZ 恶意后门是由其首席开源管理员——一位名叫 Jia Tan 的开发人员引入的。2021 年 11 月，未知个人或组织用 Jia Tan 的名字创建了 GitHub 账号 (JiaT75)。自注册以来，Jia Tan 一直是 XZ 项目的贡献者，并与参与该项目的开发者社区建立了信任。最终，Jia Tan 与创始人 Lasse Collin 一起成为项目的共同维护者，可以在无需批准的情况下添加代码。2024 年年初，恶意代码被插入到 xz Libs 项目中。

攻击者历经多年建立开源软件贡献者的可信声誉，并使用高度混淆的代码来逃避代码审查的检测。这种持续多年的耐心行动，加上植入后门本身的技术特点和复杂性，让网络安全界的许多人相信，攻击者实际上是由国家资助的黑客。

安全研究人员一致认为，攻击者 Jia Tan 不太可能是一个真人，甚至不太可能是一个单独工作的人员。俄罗斯网络安全公司卡巴斯基高级研究员兼全球研究和分析团队负责人 Costin Raiu 表示，这可能是一个由国家支持的攻击组织，有着长期目标，有能力针对开源项目进行多年渗透。

再次敲响供应链警钟

一场侥幸的胜利，阻止了差点就发生的软件供应链攻击，组织似乎不应因为没有受到影响而简单放松。事

件应该为整个行业敲响警钟，让已备受瞩目的供应链攻击事件再次引发关注。

供应链攻击并不是一个新问题，在 GitHub 和 NodeJS 中频繁发现恶意软件包。自 2021 年以来，重大供应链攻击一直成为焦点，SolarWinds 供应链攻击给受影响的公司造成了超过 9000 万美元的损失。

XZ 后门的新颖之处，在于攻击者获得了对行业普遍使用代码的访问权限，禁用了检测所利用功能的安全工具，并在广泛使用的程序植入了高度复杂的后门。

有人甚至猜测，这个后门是否是为了转移对“真正”后门的注意力而被发现的，这带有阴谋论的观点，也并非完全没有道理。高级网络攻击者不会将所有精力都花在单个机会目标上，他们会追逐多个目标，因为每一次入侵的时间都是有限的。

安全人员发现，化名的攻击者留下的唯一足迹似乎是对开源开发社区的贡献——攻击者还是个多产的开源贡献者。更令人不安的是，攻击者提交的第一个代码更改是“libarchive”压缩库——另一个广泛应用的开源组件。

网络安全公司 NetRise 联合创始人迈克尔·斯科特 (Michael Scott) 称，2021 年至 2024 年 2 月期间，攻击者（Jia Tan）对至少 7 个项目提交了 6000 次代码更改。他认为，要确定这些变化的所有影响几乎是不可能的。由于这些更改（称为“提交”）通常会通过称为“合并提交”的方式，因此并不总是很清楚攻击者具体提交了哪些更改。

假扮角色似乎是这个有序管理的新组织的策略——这一策略几乎奏效了。这意味着未来攻击者将会用其他名字重回开源社区：攻击者会从错误中吸取教训，将性能影响作为可能的检测向量，从而更好地实施下一次攻击尝试，继续扮演热情的开源项目贡献者，在其提交的代码中隐藏着背后支持政府的秘密意图。

这可能是此类攻击的第一次，但肯定不会是最后一次。

后门风险呼唤业界重视开源安全

XZ 后门是一个避免重大危机的英雄故事，但也带来开源安全新警示：攻击者同样可以潜入流行的开源项目，将受污染版本带到供应链中。JFrog 研究人员表示：这次供应链攻击令开源软件社区感到震惊，因为 XZ Utils 一直被认为是值得信赖且经过严格审查的项目。

> 攻击策略奏效，这意味着攻击者将会
> 用其他名字重返开源社区，
> 继续扮演开源项目贡献者，
> 在提交代码中隐藏着背后的秘密意图。

在 XZ 后门事件中，攻击者成功地在受信任、广泛使用的开源组件中植入几乎无法检测的后门，这让业界开源软件的安全问题引发全面质疑。这一事件导致大多数公司更新其安全态势，以应对供应链攻击，许多企业的反应是使用软件成分检测工具来保护其开源开发环境。

这一事件也让开源模式面临不可持续的挑战：科技巨头利用开源软件创造了巨额财富，但许多关键开源组件却是由少数人免费创建和维护的库和依赖项构建的。与商业软件公司雇佣大批开发人员来修复错误、测试新功能并通过安全角度检查代码更改不同，开源项目过度依赖于志愿者。例如，Log4j 是苹果、推特等巨头公司所依赖软件的关键组件，它一直是由志愿者免费运行的项目。

随着开源的普及和使用的不断增长，开源风险也不断演变，从许可兼容性问题到漏洞的机会性利用，再到恶意攻击。对软件供应链有计划的、蓄意的攻击日益普遍，恶意行为者不仅利用代码缺陷，还实际篡改代码和开发管道来传播受感染的恶意软件。供应链安全公司 ReversingLabs 在 2024 年报告《软件供应链安全状况》中指出，过去三年中，源自开源软件包存储库的威胁增加了 1,300% 以上，其中包括攻击者直接通过软件包推送恶意软件的事件。

为了应对 XZ 后门之类的风险，政府主管部门应该将 SBOM 作为行业标准，推动软件开发商提供软件物料清单 (SBOM)，这将有助于软件开发人员有效降低开源软件的风险。

在 XZ 后门事件中，
攻击者成功地在受信任、广泛使用的开源组件中
植入几乎无法检测的后门，
这让业界开源软件的安全问题引发全面质疑。

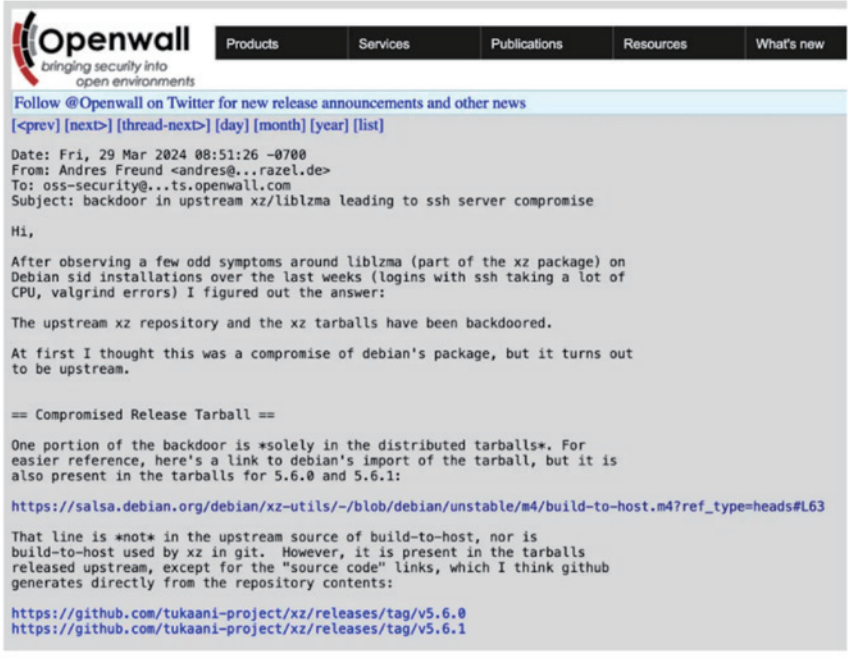
企业需要花费更多的资源来审查开源软件——要么审查开源代码，要么为开源项目设定更高的标准。使用开源组件的组织（实际上是所有组织），都需要主动识别和管理类似的开源安全威胁，将此作为保护其软件供应链的一部分。

从行业来说，仅仅考虑管理开源代码是不够的，还需要激励使用开源代码的软件开发人员，通过贡献后台代码来积极支持开源社区。这对于培育健康的软件生态系统，从而使开源和专有软件更加安全至关重要。开源社区应该考虑第三方制衡，强制检查所有提交的项目更改，这对查找恶意代码的添加至关重要。

随着开源社区努力应对这一事件的后果，增强安全协议和提高软件开发流程透明度的迫切性变得前所未有的紧迫。只有通过集体警惕和协调一致的行动，我们才能加强数字基础设施，抵御不断变化的威胁，并维护开源软件生态系统的完整性。

liblzma/xz 被曝植入后门，如何降低危害?

3 月 29 日，liblzma / xz 被曝遭植入后门，将有相当一部分的 SSH 版本受到该后门影响，迅速引发密切关注。据悉，微软公司连夜加班处理本次后门事件，主流云厂商加急排查风险和安全修复。奇安信已开 95015 专线，可应急排查救援。


Openwall
bringing security into open environments

Products | Services | Publications | Resources | What's new

Follow @Openwall on Twitter for new release announcements and other news

[<prev>] [next>] [thread-next>] [day] [month] [year] [list]

Date: Fri, 29 Mar 2024 08:51:26 -0700
From: Andres Freund <andres@...razel.de>
To: oss-security@...ts.openwall.com
Subject: backdoor in upstream xz/liblzma leading to ssh server compromise

Hi,

After observing a few odd symptoms around liblzma (part of the xz package) on Debian sid installations over the last weeks (logins with ssh taking a lot of CPU, valgrind errors) I figured out the answer:

The upstream xz repository and the xz tarballs have been backdoored.

At first I thought this was a compromise of debian's package, but it turns out to be upstream.

== Compromised Release Tarball ==

One portion of the backdoor is *solely in the distributed tarballs*. For easier reference, here's a link to debian's import of the tarball, but it is also present in the tarballs for 5.6.0 and 5.6.1:

https://salsa.debian.org/debian/xz-utils/-/blob/debian/unstable/m4/build-to-host.m4?ref_type=heads#L63

That line is *not* in the upstream source of build-to-host, nor is build-to-host used by xz in git. However, it is present in the tarballs released upstream, except for the "source code" links, which I think github generates directly from the repository contents:

https://github.com/tukaani-project/xz/releases/tag/v5.6.0
https://github.com/tukaani-project/xz/releases/tag/v5.6.1

奇安信 CERT 第一时间发布了《liblzma/xz 库被植入后门影响 SSH 事件紧急通告(CVE-2024-3094)》。通告称，有开发人员在调查 SSH 性能问题时发现了涉及 XZ 包中的供应链攻击，进一步溯源发现 SSH 使用的上游 liblzma 库被植入了后门代码，恶意代码可能允许攻击者通过后门版本的 SSH 非授权获取系统的访问权限。恶意代码修改了 liblzma 代码中的函数，该代码是 XZ Utils 软件包的一部分，链接到 XZ 库的任何软件都可以使用此修改后的代码，并允许拦截和修改与该库一起使用的数据。

XZ 是类 Unix 操作系统上的一种无损数据压缩格式，通常与 gzibzip2 等其他常见数据压缩格式进行比较。XZ Utils 是一个命令行工具，包含 XZ 文件和 liblzma 的压缩和解压缩功能，liblzma 是一种用于数据压缩的类似 zlib 的 API，并且还支持旧版 .lzma 格式。

奇安信 CERT 指出，liblzma/xz 被植入源码级后门，渗透了多个 Linux 的较新发行版，在核心的远程管理工具 SSH 中被使用，可能影响大量的喜欢尝鲜的系统管理员的系统，对网络基础设施构成威胁，目前实际的影响范围还需要时间评估。

奇安信 CERT 通告提醒，目前已

知 XZ Utils 版本 5.6.0 和 5.6.1 受到影响，恶意代码还不存在于 XZ 的 Git 发行版中，仅存在于完整的下载包中。已知的 Linux 发行版包括 Fedora Rawhide、Fedora 41、Debian 非稳定的测试版 5.5.1alpha-0.1 到 5.6.1-1 等。

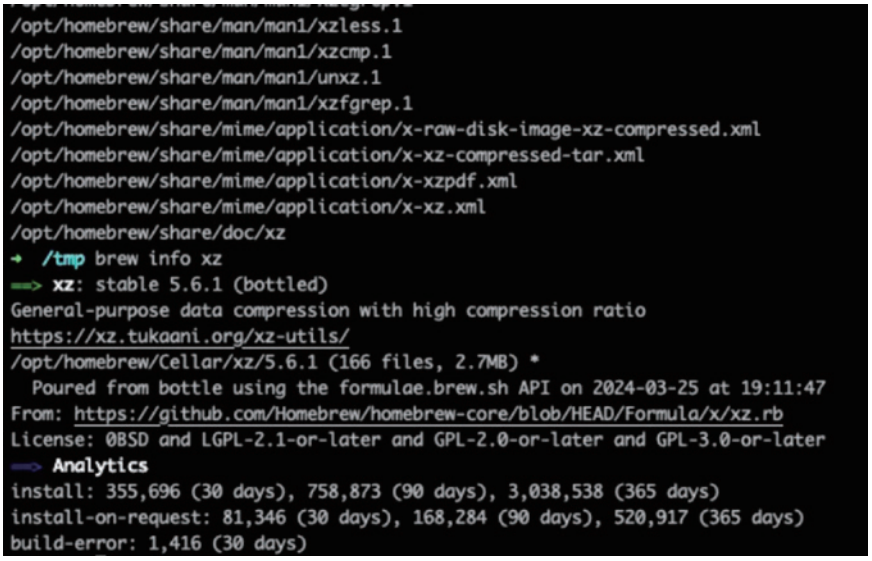
分析人士指出，本次影响范围虽然不及 2021 年的“核弹级漏洞”Apache Log4j2 事件，但也充分暴露出数字世界中无处不在的漏洞和后门，给网络安全带来巨大的潜在威胁。

首次曝光该后门的为 3 月 29 日有开发人员在安全邮件列表上的发帖。该帖内容称，起先有人发现服务器上 sshd 出现异常资源占用的现象，一番排查后发现，竟然是从 XZ 软件包里感染的后门程序。目前已知的后门存在于 v5.6.0 和 v5.6.1 版本。但是这个代码的提交人两年前就加入了项目维护，暂时不能确定之前的版本有没有问题。

据介绍，这个后门会篡改 Makefile 注入恶意脚本到 configure 里执行，从而在生成的代码里链接恶意的 .o。当满足一定条件，即当前进程是 /usr/sbin/sshd，不存在调试环境变量，配置了 LANG，就会触发后门逻辑。

该帖给出了一段快速检测后门是否存在的脚本，该恶意后门被分配了编号 CVE-2024-3094。

目前迹象表明，后门作者有选择地针对 Linux 发行版下手。但这个 liblzma 可不只 Linux 上用。比如，目前流行的 iOS 越狱环境，大部分 tweak 包还是以 .deb 格式发行，比较新的版本就用到了 lzma 作为压缩。



除此之外，近期有在 macOS 上使用 brew 安装过 XZ 包的应该也受到影响，暂时不能证明有恶意行为。

后门，本质上是设计或开发者有意留下的可供特殊情况使用的系统漏洞，其如同“定时炸弹”，危害要远大于相当于开发人员无意之间留下的普通 bug 类漏洞。因此当前网络安全最突出矛盾之一就是软件供应链漏洞、后门难防。据奇安信统计，仅国内外应用最广泛的 Java 编程语言，就有近 1500 万个版本的 Java 开源组件，它们当中很多存在漏洞、后门等安全风险。

如何降低后门的危害？奇安信 CERT 建议：首先要加强系统本身的安全性，定期自查系统漏洞，降低系统被植入后门木马的可能；其次是加强系统内主机的安全监测，在系统被植入后门木马后，可以快速的发现并查杀；然后是定期开展员工安全意识培训，防止员工误下载后门木马，给攻击者提供可乘之机；最后是积极关注威胁情报信息，第一时间获取全球最新威胁动态，及时改进和优化安全策略，提前应对新型攻击。

xz/liblzma 后门影响全网软件测绘分析

作者 | 星图实验室

2024 年 3 月 29 日，开发人员在 SSH 性能调查中发现 XZ 组件中包含后门，影响了 liblzma 库，并且该后门事件已被分配编号 CVE-2024-3094。奇安信技术研究院 [“天问”软件供应链安全监测平台](https://tianwen.qianxin.com/) 利用积累的海量软件空间测绘数据，发现开源生态中的若干软件存在使用后门组件的情况，其他系统、软件和固件上暂未发现直接使用后门组件的情况。

具体地，我们的测绘分析发现 crates.io 中的 liblzma-sys 包使用了受后门影响的版本。对于其他软件及固件，由于含有后门的两个版本的发布时间在 2024 年 2 月 24 日之后，目前尚未被多数软件使用，因此对现有软件的影响有限。但是，由于实际使用中历史版本的 XZ 组件有可能升级到后门版本从而产生影响，因此，我们对 XZ 组件的历史版本影响情况进行了全面测绘分析，以便相关人员和组织排查可能的风险，尽管这些版本没有受后门影响。

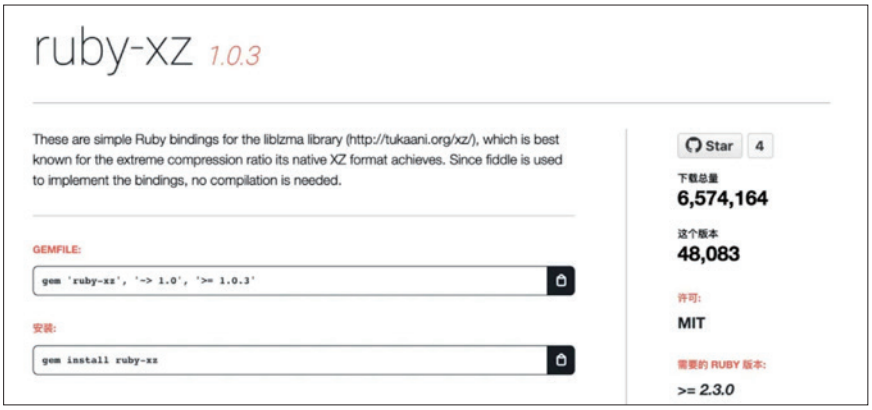
> 由于 XZ 组件包含后门的版本发布时间短，多数软件和固件没有使用该组件的后门版本，目前仅在开源生态 crates.io 中发现该后门版本。

背景介绍

XZ Utils 是一组在类 Unix 系统中使用的开源数据压缩工具，包括程序 lzma 和 XZ，目前已集成在 Debian、Ubuntu、CentOS 等发行版中。它采用高效的 LZMA 算法，能够实现较高的压缩比率，支持多种压缩格式，适用于各种文件存档、数据备份和软件分发等场景。

3 月 29 日，一名开发人员在安全邮件列表中 [发帖](https://www.openwall.com/lists/oss-security/2024/03/29/4) 称 [1]，在调查 SSH 性能问题时发现了涉及 XZ 包的供应链攻击。调查发现，SSH 所用的 liblzma 库被植入了后门，可能导致攻击者非授权获取系统权限。该后门修

改了 liblzma 代码，允许攻击者拦截和修改数据，影响使用 xz 库的下游软件。目前在 xz 组件的 v5.6.0 和 v5.6.1 版本中发现了该后门，两个版本分别发布于 2024-02-24 和 2024-03-09。该贴同时发布了快速检测脚本，并公布了该后门的编号 CVE-2024-3094。



天问测绘结果

奇安信技术研究院[“天问”软件供应链安全监测平台](https://tianwen.qianxin.com/)基于强大的知识库，拥有软件供应链安全事件监测和影响范围测绘能力，能够自主进行软件成分分析，并生成软件影响图谱。天问平台具备三大能力：软件组成成分分析能力、全网软件空间测绘能力和安全事件监测预警能力。用户可通过浏览器访问天问平台，将待测试软件直接上传天问进行分析。天问支持跨 CPU 指令集、支持跨操作系统平台检测，目前支持十余种软件安装包格式，二十余种打包格式和十余种固件格式的的分析，还支持对 Docker 等容器镜像的分析。

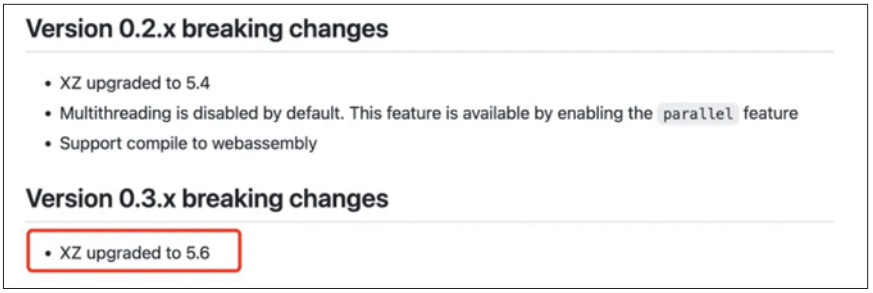
“天问”软件供应链安全监测平台提供软件成分分析功能，能够从软件中提取其使用的组件和版本并给出安全建议。在 xz 组件后门事件曝光后，我们立刻对 xz 组件的影响进行了初步的事件影响测绘分析，分析范围涵盖操作系统、开源生态、安卓应用、固件镜像、存量软件等多个不同维度。

2.1 可能受后门影响的软件

我们在部分知名开源软件生态中发现了明确使用后门版本的组件。

2.1.1 crates.io

在 crates.io 生态中，我们发现了 **liblzma-sys** 和 **liblzma** 两个软件包可能受该后门影响，其中 liblzma-sys 仅被 liblzma 包依赖。我们发现 liblzma-sys 在 2024 年 1 月 26 日更新了 0.3.0 版本，并在 3 月 12 日更新了 0.3.1 版本。在该包的简介中，开发者明确说明了 0.3.x 版本使用了 XZ 的 5.6 版本，正好是存在后门的版本。此外，根据我们的测绘数据，crates.io 生态中依赖这两个包的全部包名如下：**libpna**、**pna** 和 **nod**。

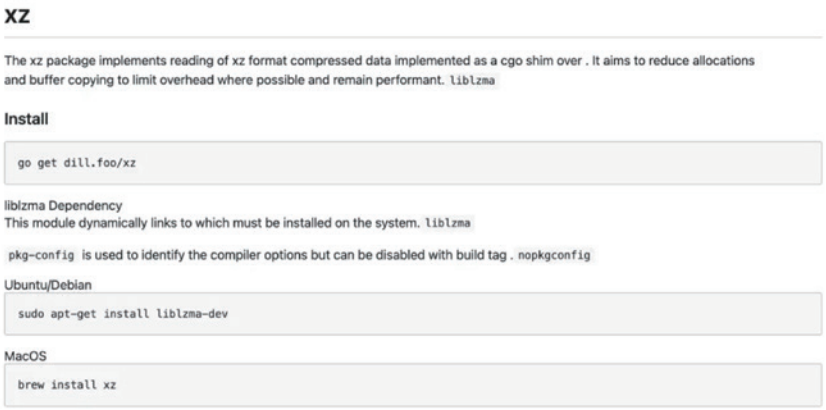


2.1.2 Rubygems

在 Rubygems 生态中，我们发现了与 XZ 组件相关的流行软件包 ruby-xz，总下载量达到 6,574,158 次。该包调用了本地环境中的 liblzma.so 和 liblzma.so.5 等动态链接库，如果本地运行环境中存在受后门影响的版本，那该包也可能受到影响。依赖该包的全部包名如下：smc-get、cure-fpm、fpm-aeppert 和 dwca_hunter。

2.1.3 Go

在 Go 生态中，我们发现了一个软件包 dill.foo/xz 使用了本地的 liblzma，该包明确要求本地先安装 liblzma，如在本地环境中使用了受后门影响的版本，那该包也可能会受影响。



2.2 不受后门影响的软件

2.2.1 Linux 发行版

我们对多个 Linux 发行版的软件源，如 Ubuntu 官方源、麒麟官方源和 Deepin 官方源中的软件进行了分析，发现了若干使 XZ 组件的软件，但未发现直接使用后门版本的软件，以下数据仅为使用 XZ 组件的软件统计。

- 在 Ubuntu 仓库总计 1,084,083 个软件中发现 192 个使用 XZ 组件的软件，占比万分之 1.7；
- 在 Kali 仓库中总计 492,253 个软件中发现 124 个使用 XZ 组件的软件，占比万分之 2.5；
- 在 CentOS 仓库中总计 409,429 个软件中发现 87 个使用 XZ 组件的软件，占比万分之 1.9；
- 在麒麟官方源仓库中 313,723 个软件中发现 88 个使用 XZ 组件的软件，占比万分之 2.8；
- 在 Deepin 仓库中 94,799 个软件中发现 46 个使用 XZ 组件的软件，占比万分之 4.8。

上述软件仓库中均未发现使用包含后门版本 XZ 组件的软件，我们的测绘分析结果与 Ubuntu[2]、Red Hat[3] 和 Debian[4] 等组织发布的官方通告一致。从测绘结果来看，目前该后门的影响有限。

2.2.2 安卓应用

在安卓生态中，天问平台测绘数据中共发现 279 款安卓应用调用了 XZ 组件，涉及 20 个组件版本，这些组件版本及软件均不受后门影响。部分样本的相关信息如下表所示。

通过分析发现，安卓软件通过多种方式调用 xz 组件。如根据对飞书安卓 版 _bc92da1573c39c15f5d68e8b44a3a92f.apk 的扫描结果，我们发现该样本通过调用 lib/arm64-v8a/libarchive.so 的方式间接调用了 XZ 组件，组件版本为 5.3.0alpha。此外，根据天问分析结果，目前一部分 apk（包括几款知名应用）通过导入 libarchive.so 库的方式引入了 XZ 组件，这些 apk 的安全性有待进一步审

组件名	组件版本	样本数量	部分样本名称	应用名称
XZ	5.2.4	126	org.dolphinemu.dolp hinemu_18283.apk	Dolphin Emulator
XZ	5.2.5	23	com.topjohnwu.magis k_24300.apk	Magisk
XZ	5.3.0alpha	23	com.webmob.super.do wnloader.for.ig1. apk	Super Downloader for IG
XZ	5.2.1	16	飞书 _46410ace75acfdb e5b0d796a10e3e864 .apk	飞书
XZ	5.2.9	11	la.daube.photochiot te_34.apk	PhotoChiotte
XZ	5.2.3	7	仁恒美光随身牙医 _79a92 5fb1638af433e1581 a165c13796.apk	仁恒美光随身牙医
XZ	5.4.0	6	YandexNavigator15.6 .0beta_172533348b 8fa6407b22657524f8b1c5.apk	Yandex Navigator
XZ	5.2.10	5	org.briarproject.br iar.android_10420 .apk	Briar
XZ	5.4.4	5	WPSTV 版 _3604bf20199 47851e322232f79f6 c9b4.apk	WPSTV 版
XZ	5.2.6	4	Briar1.4.18.apk	Briar

查。

2.2.3 固件镜像

在固件生态测绘中，我们从156,787个固件文件中发现了11,210个固件使用了XZ的组件，检出率为7.14%。

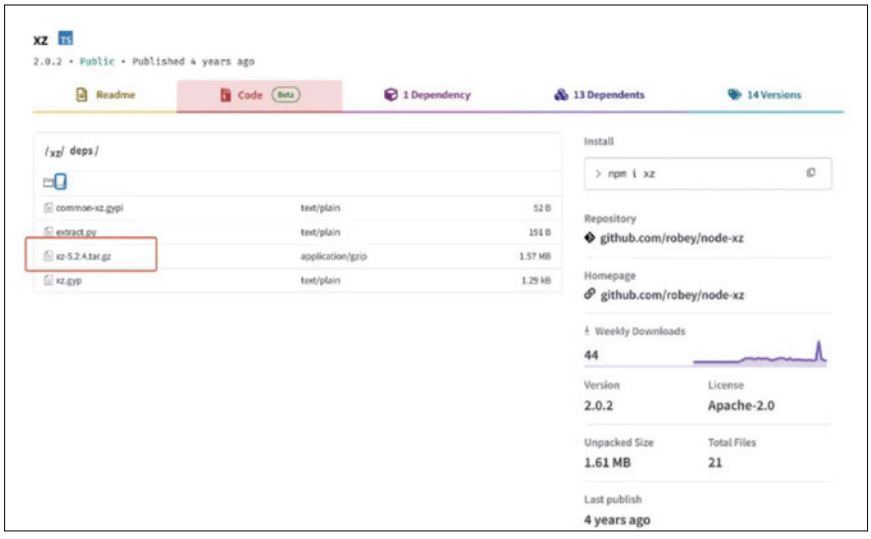
通过对测绘数据的进一步分析，我们统计了使用XZ组件较多的厂商和涉及产品型号数量较多的厂商。其中Synology、Poly和Apple的固件中使用XZ组件的次数均超过了1,000次，分别为3,902、1,699和1,150。另外Synology和Axis涉及产品的型号数量超过了100，分别为244和193款。影响的产品中包含我们熟知的iPad mini4和Watch Series 2等。这些固件虽然没有使用受后门影响的版本，但若使用过程中存在升级过XZ组件的情况，则可能存在安全风险。

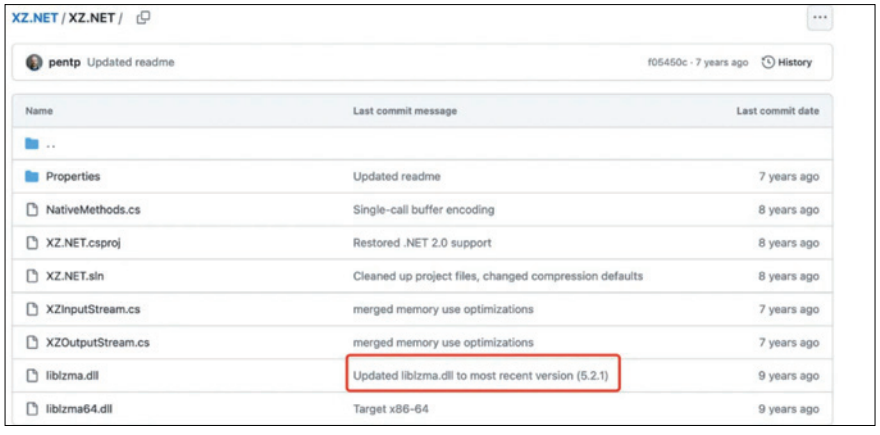
此外，在分析了多款固件后，我们发现XZ组件主要以动态调用库的形式存储在/usr/lib64/、/usr/lib/目录下，常见的文件名为liblzma.so、libarchive.so，为系统提供解压、读取压缩包功能，例如，在思科型号为FPR1100固件中存储形式如下：

2.2.4 存量软件

在Windows平台上的存量软件

测绘数据中，天问共发现 58,718 款软件调用了 XZ 组件，涉及 32 个组件版本，其中使用最多的版本为 5.0.5，达 19,709 次。在这些使用 XZ 组件的软件中，有很多我们熟知的软件，如 Syncovery 使用了 5.2.2 版本，Youtube Video Downloader 使用了 5.2.4 版本。目前，天问存量软件测绘中未发现包含受后门影响版本组件的软件。





2.2.5 其他开源生态

在 npm 生态中，没有找到受到此次后门影响的软件包。已有的 XZ 软件包最后一次更新为 4 年前，且使用的 XZ 版本为 5.2.4，并未受到此次后门的影响。

在 NuGet 生态中，已有的使用 XZ 组件的软件包为 XZ.NET 和 XZ.NET-netstandard，其均使用的是 5.2.1 版本的 liblzma.dll，未受到此次后门的影响。

在 Go 生态中，我们发现 github.com/simon-graham/go-liblzma 包使用了 5.2.5 版本的 liblzma，未受到此次后门影响。

处置建议

根据奇安信威胁情报部门的[事件紧急通告](https://mp.weixin.qq.com/s/RSRwJf2HpoxBLrV5C6sbeg)[5]，目前可用以下脚本检测当前环境是否可能使用后门版本的 XZ Utils。

```
#! /bin/bash  set -eu

# find path to liblzma used by sshd  path="$(ldd $(which sshd) | grep liblzma | grep -o '/[^ ]*')"

# does it even exist?  if [ "$path" == "" ]  thenecho probably not vulnerable  exitfi

# check for function signature if hexdump -ve '1/1 "%.2x"' "$path"
```

| grep -q f30f1efa554889f54c89ce5389fb81e7000000804883ec28488954241848894c2410 thenecho probably vulnerable elseecho probably not vulnerable fi

结语

由于 XZ 组件包含后门的版本发布时间短，多数软件和固件没有使用该组件的后门版本，我们仅在开源生态 crates.io 中发现 liblzma-sys 包明确使用了该后门版本。以上的测绘数据仅是我们初步的分析结果，目前尚未对可疑软件进行进一步的验证。奇安信技术研究院 [“天问”软件供应链安全监测平台](https://tianwen.qianxin.com/) 将会持续对该组件进行监测和分析，后续会适时发布更多关于该组件影响的测绘数据和分析结果。

参考链接

[1] oss-security - backdoor in upstream xz/liblzma leading to ssh server compromise, https://www.openwall.com/lists/oss-security/2024/03/29/4

[2] Xz/liblzma security update - Announcements - Ubuntu Community Hub, https://discourse.ubuntu.com/t/xz-liblzma-security-update/43714)

[3] Urgent security alert for Fedora 41 and Fedora Rawhide users (redhat.com), https://www.redhat.com/en/blog/urgent-security-alert-fedora-41-and-rawhide-users

[4] \[SECURITY] \[DSA 5649-1] xz-utils security update (debian.org), https://lists.debian.org/debian-security-announce/2024/msg00057.html

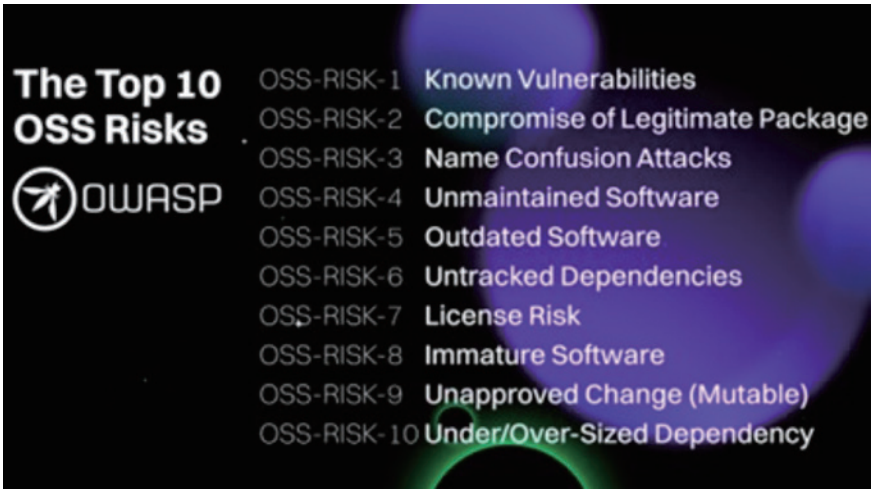
[5] liblzma/xz 库被植入后门影响 SSH 事件紧急通告（CVE-2024-3094），https://mp.weixin.qq.com/s/RSRwJf2HpoxBLrV5C6sbeg

OWASP 发布十大开源软件安全风险及应对指南

为帮助用户更安全地使用开源软件 (OSS)，降低开源软件安全漏洞的潜在风险，近日开放全球应用程序安全项目 (OWASP) 发布“十大开源软件风险”清单，并对每种风险给出了安全指南。

最近爆发的 XZ 后门事件，尽管未酿成 Log4j 那样的灾难性后果，但它再次敲响了警钟：软件供应链严重依赖开源软件，导致现代数字生态系统极其脆弱。面对层出不穷的安全漏洞，我们需要关注开源软件 (OSS) 风险 ，改进其保护和使用方式。

风险 1 | 存在已知漏洞



这一风险是指存在包含已知漏洞（如软件缺陷）的开源软件组件。这些漏洞通常由软件开发人员和维护人员无意中引入，然后由社区的安全研究人员公开披露。这些漏洞可能会被利用，具体取决于它们在组织和应用中使用的上下文。

应对指南：OWASP 建议组织采取多种措施，来降低包含已知漏洞的开源软件组件风险，如扫描使用的所有开源软件组件中的漏洞，根据已知利用、利用概率、可达性分析 (可将误报率降低 80% 以上) 等方法对发现结果进行优先级排序等。

此外，业界还开发了一系列平台来应对这一挑战，如 CISA 的已知被利用漏洞 (KEV) 目录和利用预测评分系统 (EPSS)。

风险 2 | 合法软件包遭植入

第二个风险是指攻击者通过破坏合法软件包，将恶意代码注入开源组件，从而影响采用的组织和下游用户。

攻击者可以使用多种方法来追踪这种攻击媒介，如劫持项目维护者的账户或利用软件包存储库中的漏洞。

攻击者还可以成为开源项目的志愿维护者，以便日后实现其邪恶意图。

最近的 XZ 后门事件正是这种情况：在代码中嵌入后门前，攻击者很长一段时间一直冒充合法的开源贡献者。

应对指南： 目前没有单一的措施可以检测和防止摄入被注入恶意代码的软件包。组织应参考安全供应链消费框架（S2C2F）等新兴标准和框架，了解可行的安全措施，并根据安全要求和风险偏好进行选择和优先级排序，可能的措施包括根据软件制品供应链级别框架（SLSA），验证验证组件来源；从可信来源构建组件，以及手动或自动进行代码审查等。

> 软件供应链严重依赖开源软件，
> 导致现代数字生态系统极其脆弱。
> 面对层出不穷的漏洞，
> 我们需要关注开源软件风险，
> 改进其保护和使用方式。

风险 3 | 名称混淆攻击

在名称混淆攻击中，攻击者创建的恶意组件，使用与合法开源软件包或组件相似的名称（拼写错误），建议可信的软件作者（品牌劫持），或使用不同软件 / 生态环境的常见命名模式（组合仿冒），希望潜在受害者会无意中下载和使用。受破坏的软件包进入组织 IT 环境时，可能会影响系统和数据的机密性、完整性和可用性（CIA）。

应对指南： 在安装 / 使用开源软件组件之前，检查代码特征和项目特征以获取主要风险指标。此外，还要验证组件是否带有来自受信任方的签名。

风险 4 | 组件缺乏维护

这是指开源软件的组件或组件版本开发不再活跃，因此，原始的开源项目可能不及时（或根本不会）提供功能性和非功能性的漏洞补丁。

与专有软件不同，开源软件的一个残酷现实是没有“供应商”。开源软件维护者“按原样”提供软件，这意味着无法保证该软件开源得到及时的维护、更新或持续。

Synopsys 的开源软件报告显示，其所评估的代码库中，85% 拥有已过时四年多的开源软件组件，且两年内没有任何新的更新。软件的老化速度很快，新漏洞正以创纪录的速度出现，如果现代软件使用不及时更新开源软件组件，其安全性将面临严峻的挑战。

开源软件主要由志愿者无偿支持。软件组件可能不会得到及时的开发或维护，修复漏洞也可能不及时或者可能不会按照组件使用者所期望的时间表进行，也不会提供专有供应商那样的漏洞修复服务级别协议（SLA）承诺。

造成开源软件缺乏维护的另一个关键因素是维护人员过少：25% 的开

> 借助软件成分分析 (SCA) 和
> 软件物料清单 (SBOM) 等相关工具，
> 可以帮助企业了解开源软件的使用情况。

源软件项目只有一名开发人员贡献代码；94% 的开源项目由 10 名或更少的开发人员维护，其中隐藏的风险是显而易见的。

60 ~ 80% 的现代软件代码库是由开源软件组成的，这意味着我们的数字生态系统的很大一部分，甚至是最关键的系统，都在受到最低限度支持和维护的软件上运行，这代表着重大的系统性风险。

应对指南：相应的应对建议包括检查开源项目的活跃程度和健康状况，例如维护者和贡献者的数量、发布频率和漏洞修复时间（MTTR）。

风险 5 | 使用过时组件

这种情况是指尽管可能存在新的组件版本和更新，项目仍使用过时的组件版本。 Synopsys 公司在报告中指出，这种状况实际上是一种常态，经常会出现在绝大多数代码库和存储库中。

过于落后于最新版本的依赖项，可能会导致紧急情况下难以及时开展更新，如所使用的版本发布漏洞时。旧版本可能也无法获得与最新版本相同级别的安全评估，尤其是否受到漏洞的影响。

现代软件应用和项目之间令人眼花缭乱的依赖关系，令这一问题变得更加错综复杂。Sonatype 和 Endor Labs 等机构发布的报告强调了这个问题，后者所发布的《依赖管理现状报告》显示，95% 的安全漏洞与传递依赖相关。

应对指南：OWASP 的应对建议包括（1）将依赖项更新设为重复待办事项；（2）实现发现和建议更新的自动化；（3）利用软件变更影响分析工具，检测是否出现变更或不向下兼容的破坏性变更。

风险 6 | 未跟踪依赖项

这种情况是指开发人员 / 组织不知道自己使用了特定的依赖项或组件。发生这种情况的原因可能是组织缺乏软件成分分析 (SCA) 等相关工具，以了解开源软件的使用情况，或者没有采用软件物料清单 (SBOM) 等新兴工具。这些工具可以帮助组织清晰了解所使用或发布的软件组件。

这些工具实际上是推动软件物料清单和供应链安全广泛努力的一部分。业界通过 SolarWinds 和 Log4j 等事件认识到，尽管多年前 SANS 研究所已将软件资产清单列入 CIS 关键安全控制清单中，大多数组织仍缺乏深入到软件组件 / 库层级的全面软件资产清单。

应对指南：建议评估和比较软件成分分析 (SCA) 工具生成准确的物料清单的能力，包括粗粒度级别和细粒度级别。

风险 7 | 许可和监管风险

这种风险是组件或项目可能缺乏许可或可能拥有阻碍下游使用的许可情况。

OWASP 指出，组织需要确保其对开源软件组件的使用符合相关适用许可条款，否则可能会导致许可或版权侵权，甚至法律诉讼。

随着组织在其专有产品、服务和产品中更广泛地使用开源软件组件，这种风险可能会影响组织的业务目标、并购活动等。

应对指南：组织可以通过确定其

软件所使用及计划使用组件的适用许可，以降低相关风险。除了了解组件是否使用多个许可或冲突的许可，组织还应该完全避免使用未经许可的组件。

风险 8 | 软件不成熟

开源项目可能不采用软件开发的最佳实践，因而在成熟度方面肯定存在差异，部分原因是维护人员的参与程度不同。

某些开源软件项目可能未采用安全软件开发实践【如 NIST 安全软件开发框架 (SSDF) 所提到的】。具体案例可能包括没有开发文档、缺乏回归测试、没有审查指南和许多其他最佳实践。

另一令人不安的现实是很多开发人员对软件安全不感兴趣。Linux 基金会和哈佛大学创新科学实验室 (LISH) 等机构的研究发现，自由和开源软件开发人员只花费 2.3% 的时间来提高软件代码的安全。

对不成熟组件或项目的依赖会带来运营风险。依赖软件可能无法按预期工作并导致运行时可靠性问题，或者其使用可能过于复杂和昂贵。

应对指南：目前有一些行业推动的措施和工具可应对这一风险，如 OpenSSF 的记分卡，为 Github 的开源软件项目提供强大的检查，如分支保护的存在与否、贡献者 / 组织的数量、CI 测试、模糊测试、维护、许可等。另一项降低此风险的工作是 CISA 和 OpenSSF 联合发布的“组件存储库安全原则”。

风险 9 | 未经批准的更改

OWASP 将这种风险定义为软件组件可能在开发人员未注意到、未审核或批准的情况下发生更改的情况。当下载链接发生改变、指向未版本化的资源、甚至是被篡改的不安全数据传输时，可能会出现这种风险。这一风险主要强调安全传输的作用。

应对指南：OWASP 建议的操作和缓解措施包括使用资源标识符用于安全保证，以及指向相同的不可变软件工件。此外，还可以在安装和使用开源软件组件之前，验证组件的签名和摘要。为了降低开源软件组件在传输中受到破坏的风险，组织应使用安全协议来开展网络流量的传输和通信。

风险 10 | 组件过小 / 过大

最后一种情况是，开源软件组件可能提供很少或很多的功能，但组织实际上只使用其中的一部分。

非常小的组件会遭受与大型组件相同的供应链风险，而且严重依赖上游项目的安全性和开发态势。非常大的组件堆积了许多标准用例中不需要的功能，却因此增加了组件的攻击面和潜在可利用代码 / 依赖项。

应对指南：在这些情况下，OWASP 建议组织了解未使用的组件功能，评估禁用未使用功能的可能性，或用功能少的小开源组件进行替代。同时，尽可能在内部重新开发所需的功能。安

从“灯下黑”到“灯火通明”，灯塔工厂打通看见网络威胁的任督二脉

作者｜安全攻防 PBU

灯塔工厂“黑灯”，网络安全不能黑灯。

灯塔工厂素有智能制造“奥斯卡”之称，是由达沃斯世界经济论坛和麦肯锡咨询公司共同遴选的“数字化制造”和“全球化 4.0”示范者，代表当今全球制造业领域智能制造和数字化最高水平。作为装备制造业的龙头，某企业就是灯塔工厂名单里的一员。

有趣的是，该企业的智能制造“灯塔”就是“无灯”，在“黑灯车间”，高达 3 米的生产机器人挥舞着“手臂”，全程数字化和柔性自动化，从零部件到整机一气完成……一幅生态、生产与安全交相辉映的和谐场景，让人惊叹。

当然，我们可以看出，上述提到的黑灯车间，可不是漆黑一片的车间，而是一种不需要太多工人的新型智能车间。这样的智能车间，在该公司遍布全国各地的产业园内拥有无数个，这也是它多年成为中国装备制造业龙头的原因之一。

“智能工厂的发展，需要建立在网络安全的基础之上，没有得到全面保护的智能工厂，就是一座‘灯下黑’的工厂，根本无法防御任何精心策划的攻击行动。”该公司网络安全部门相关负责人表示，由于智能车间应用了大量的新技术，机械设备与物联网、企业网中运行的信息系统实现了互联、互通、互控，因此，像该公司这样的工程机械企业，面临的网络风险则更大。

而面对网络威胁，看不见已经成为数字时代最大的痛点之一。作为在全国各地拥有多个智能产业园的集团性企业来说，让网络威胁全面可见、可查、可追溯，是一个系统再造的工程，不可能单兵独进。该企业网络安全部门相关负责人认为，只有将企业旗下遍布全国的产业园形成合力，才能打通集团企业看见威胁的“任督二脉”，才能真正让该企业的网络安全从“灯下黑”走向“灯火通明”。

如今，该企业携手奇安信天眼，在企业数字化转型发展的同时兼顾安全，真正地打通了全国各地产业园网络威胁检测的“任督二脉”，让网络流量像“毛细血管”一样融会贯通，像水和电一样随取随用，为安全人员进行威胁监测和分析提供了便利，同时也极大地提高了集团企业整体的威胁防御能力。

装备制造数字化转型，网络安全难题如何解决

装备制造业作为国之重器，是重工业的心脏和国民经济的生命线。因此，也成为全球攻击者的首选目标。

这类企业一旦遭受网络攻击，可能会导致制造设备无法正常运行，生产线停止，工厂无法运转，或造成制造工艺研发数据、知识产权和商业机密泄露，给企业带来无可挽回的经济损失和声誉损失，甚至面临法律责任和赔偿责任。

近年来，该企业抱着“要么翻身，要么翻船”的决心和魄力，不断建设智能工厂和数字化车间，坚定不移地推动数智化转型，已经成为全球领先的装备制造企业。

而随着该企业数字化持续升级和发展版图的日益扩张，使得公司网络安全问题更加突出，已经无法满足数字时代的网络安全需求。尤其是面对新一代复杂的高级网络攻击时，公司现有的监测预警和防御能力明显不足，更容易受到网络攻击，主要体现在以下几个方面：

管理离散，安全防御体系不完整。由于各地产业园负责不同的装备制造，零部件加工过程互相独立、互不配合，因此在网络安全管理上也“各自为政”，导致集团难以形成整体的防御体系，更容易成为攻击目标。而且，各地产业园的安全管理策略和运维人员水平存在差异，导致某些产业园网络安全水平较低，但又没有足够的能力单独应对网络攻击。

数据孤岛，高级威胁难应对。分支单位防护产品独立部署，导致数据无法与总部共享，出现了数据孤岛问题。这使得各单位间协同联动的防护能力差，难以发现更深层次的网络安全问题，无法形成合力应对高级威胁。

追溯断链，威胁源头难发现。当安全事件发生时，安全人员无法准确判断攻击者身份、攻击方式和窃取的信息，也无法提出针对性的应急处置方案，所以导致无法从根源上解决问题。由于无法获得根源，下次攻击者可能会再次入侵单位，对整个企业的信息和业务造成更大的威胁。

当然，该装备制造企业在数字化转型中面临的上述网络安全顽疾，也代表了大多数装备制造行业企业普遍存在的通病。

一直以来，装备制造行业对网络安全的投入并不突出，再加上攻击者

对该行业愈发虎视眈眈，面对内忧外患的双重夹击，装备制造类企业亟需一套在网络威胁检测发现、溯源取证、事件处置方面的解决方案，建立全面感知、协同联动的主动防护体系，来保证智能工厂安全稳定运行。

打通数据孤岛，威胁全面可见，溯源追根联动

奇安信的出现，解决了该装备制造龙头企业的燃眉之急。

借助奇安信天眼强大的威胁监测与分析能力，通过集群化部署，该企业成功地完成了整体攻防态势感知平台的搭建，让 15 个各自为政的产业园走向统一，使得分析人员可以通过一个天眼分析平台全面掌控 15 个产业园的整体威胁态势，并且可以根据需要，呈现出各产业园的安全态势。

具体部署方式如下：

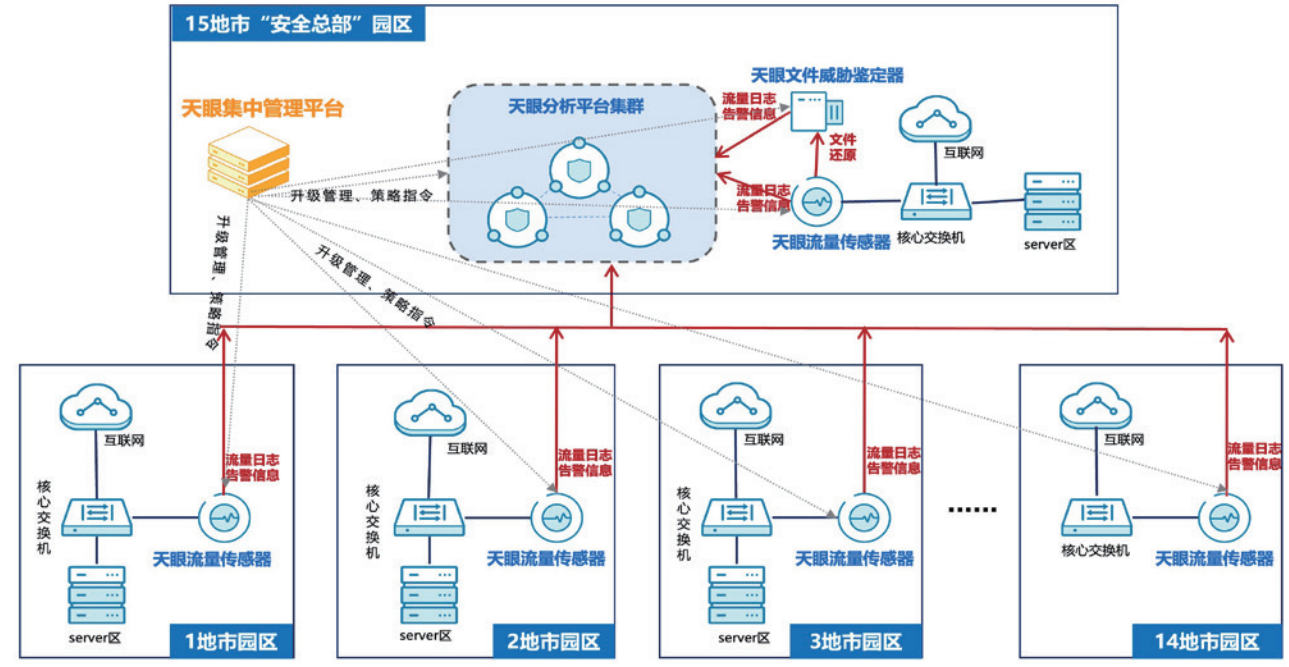
在各产业园方面，通过在全国 14 个产业园核心交换机侧部署天眼流量传感器设备，把各产业园的流量日志和告警日志全部上传到作为“安全总部”产业园的分析平台，集群进行统一监测和分析。

在全局方面，“安全总部”产业园既可以监测本产业园天眼流量传感器上传的异常流量日志和告警日志、天眼文件沙箱传递的异常文件告警信息，也能监测到其他 14 个产业园天眼流量传感器上传的异常流量日志和告警日志。

通过集中安全态势监测，安全总部园区可以对其他园区的网络安全情况进行实时监测和预警，及时发现和应对网络安全事件，最大程度地保障智能工厂的生产安全。同时，还可以将各个园区的安全态势进行对比和分析，发现安全隐患和风险，为安全水平较低的园区提供有针对性的改进建议和指导，以提高公司整体的网络安全水平。

“原来，有些产业园在网络威胁监测上属于‘裸跑’，我们总是担心发生‘一着不慎，全盘皆输’的事情发生。”该 AI 公司网络安全部相关负责人表示，部署了天眼之后，公司可以全面监测到各产业园出口的流量，看到智能工厂在机械加工、仓储、下料、焊接、涂装、装备等各个环节所涉及的网络风险，同时结合其他安全产品，将威胁和风险业务对照起来，全面狙击更复杂的网络攻击。

看见威胁的下一步动作，就是分析溯源。在原来，一个产业园受到攻击，其他产业园无法感知，也无法帮助一起溯源，更不能有所预防。从以往的威胁溯源过程中，该公司深刻地洞察到，在威胁溯源的过程中，数据孤岛成为分析人员进一步揪出攻击者的重要难题。



某装备制造业龙头：部署在全国各地的14个智能产业园区

现在，借助奇安信天眼的集群化与一体化，装备制造“巨无霸”通过将 15 个产业园的数据互相碰撞、综合关联分析，自动将数以万亿的零散告警形成智能化的攻击事件链条，打通了散落在各产业园的网络流量数据，跨过了这道坎。

“只要攻击者从任何一个产业园区进来，我们都能掌握他的行踪轨迹，看其他园区是否也受到攻击，从而进行追根溯源。”该公司网络安全相关负责人说道。

当奇安信天眼帮助该公司解决了网络威胁不可见、攻击证据溯源难之后，公司又面临了新的问题。十几台天眼设备分布在全国各地产业园，安全运营人员对于天眼设备的日常运营和管理难免面临较大压力，造成设备运维效率低、设备异常排查不到位的情况。

为了解决上述天眼设备运维难的问题，该公司在“安全总部”产业园部署“天眼集中管理平台”。通过一套天眼集中管理平台，安全运维人员可以统一轻松管理和监测各产业园的所有天眼设备，并统一完成天眼设备版本升级、漏洞补丁升级、漏洞规则升级；当设备遇到故障时，该平台不仅能发现问题点，还能通过邮件及时通知客户。有了天眼集中管理平台，该装备制造企业安全人员管理天眼设备更轻松、效率更高。

谈及未来合作展望，该装备制造企业网络安全部门相关负责人介绍，公司曾入选福波斯全球企业 500 强，已经在全球形成了产业集群，在全球多个国家都建设了产业园。基于天眼在日常运营中的实践及多次在国家网络安全攻防演习中的良好表现，未来，该公司将继续扩大分支机构天眼设备的覆盖范围，加强在海外产业园的部署，让中国新一代网络安全的领军者为“中国制造”出海保驾护航。

后记：

智能制造是装备制造业转型升级的重要方向，数字化是装备制造产业发展的必然趋势。而包括工程机械在内的装备制造企业，要想高质量推进智能制造和数字化转型，实现可持续发展，必须确保企业网络威胁全面可见，网络攻击有效防御，安全事件妥善处置，最终保障生产业务系统及智能工厂的稳定、高效和安全运行。

以“智”赋能，奇安信天眼作为网络威胁检测与响应领域的龙头产品，为各行业数字化转型的企业提供专业的集网络威胁检测、响应、溯源、预警为一体化的解决方案。未来，天眼也将继续以核心技术和自主创新守护智能制造网络安全，筑牢工程机械、装备制造及整个重工行业的安全底座，守护中国制造生命线。安

3 月全球多家公司推出生成式 AI 安全相关产品，如 Sentra、Nightfall AI、Perception Point、德勤、Nametag Autopilot、Legit Security、Bedrock Security 等。MIT、Gartner、IBM 等也先后发布了有关生成式 AI 的报告 / 指南。

下文就其中三篇报告做了部分内容摘录。

IBM 发布 CEO 生成式 AI 行动指南：将生成式 AI 视为迫切需要加以保护的重要平台

几乎所有受访高管（96%）表示，采用生成式 AI 可能会在未来三年内导致其组织出现安全漏洞。

生成式 AI 引入全新的风险与威胁

生成式 AI 为网络攻击者提供了全新的武器库。当今的黑客不再仅仅是伪造电子邮件，而是可以模仿声音、面孔，甚至个性来诱骗受害者。而这还只是开始。

随着生成式 AI 在未来半年到一年内持续普及，专家们预计新型入侵攻击将达到前所未有的规模、速度、复杂性和精密度，各种新的威胁形式也会不断涌现。从可能性和潜在影响的角度来看，大规模发起的自主攻击将成为最重大的风险。不过，受访高管们预计，黑客伪造或冒充可信用户将对业务产生最大的影响，其次是创建恶意代码。

组织实施生成式 AI 的方式也可能会带来新的风险。事实上，47% 的受访高管担心在运营中采用生成式 AI 会引发针对其组织自主 AI 模型、数据或服务的新型攻击。

全球数据泄露的平均成本为 445 万美元，美国更是高达 948 万美元。在此形势下，许多企业正在加大投资力度，以应对新兴网络安全风险。受访高管表示，其组织 2023 年的 AI 网络安全预算相比 2021 年增加了 51%。而且，他们预计到 2025 年，这一预算将再增加 43%。

将生成式 AI 视为迫切需要加以保护的重要平台

敦促网络安全领导者紧急行动，即刻着手应对生成式 AI 的风险，而不是采取分步措施。

如果缺乏安全的数据，实现值得信赖的生成式 AI 就无从谈起。

数据是生成式 AI 的命脉。所有模型都依靠数据来回答、查询并提供见解，也正是因此，训练数据成为了网络攻击的主要目标。

黑客仍然希望窃取数据并高价出售，但数据渗透提供了一条获取非法利润的新途径。如果黑客可以更改驱动组织生成式 AI 模型的数据，就可以通过有针对性的操纵或错误信息来影响业务决策。这种不断演变的威胁带来了一系列新的法律、安全和隐私问题，而 CEO 则需要在整个企业范围内管理这些问题。

高管们看到了问题的严重性。在采用生成式 AI 方面，受访高管预计会出现各种各样的风险——84% 的受访高管担心广泛或灾难性的网络安全攻击有可能会引发新的漏洞。三分之一的受访高管表示，如果没有全新的治理形式，例如，全面的监管框架和独立的第三方审计，就无法管理这些风险。

总体而言，94% 的受访高管表示，在部署之前确保 AI 解决方案的安全性至关重要。不过，只有 24% 的生成式 AI 项目将在未来六个月内纳入网络安全组件。而且，69% 的受访高管表示，在部署生成式 AI 方面，创新优先于网络安全。

这表明对生成式 AI 网络安全需求的理解与网络安全措施的实施之间存

在明显脱节。为了规避代价高昂且不必要的后果，CEO 需要采取有力举措来应对数据网络安全和数据溯源问题，包括投资部署数据保护措施（如加密和匿名化）。数据跟踪和溯源系统可以为生成式 AI 模型所使用的数据提供更好的完整性保障。

让可信数据成为组织的支柱

持续迭代网络安全实践，全面考虑多种生成式 AI 模型和数据服务的要求。

由于收益显著，CEO 面临着迅速广泛引入生成式 AI 的压力。但为了避免增长结构倒塌，企业高管迫切需要利用生成式 AI 来增强韧性。这样一来，高管们不仅可以规避生成式 AI 的风险，还可以借生成式 AI 之力，让组织变得更强大。

超过一半的受访高管（52%）表示，生成式 AI 将帮助他们更好地分配资源、能力、人才或技能；而 92% 的受访高管表示，在采用生成式 AI 之后，这项技术更有可能增强或提升而不是取代其网络安全人员。

这些新兴技术工具可以帮助团队降低复杂性并专注于最重要的任务，或许也正是因此，84% 的受访高管计划优先部署生成式 AI 网络安全解决方案，而不是传统的网络安全解决方案。

在网络安全领域使用生成式 AI，有助于在整个企业生态系统中实现“倍增效应”。84% 的受访高管表示，开放创新的生态系统对于其组织未来的增长战略非常重要。由于企业高管希望建立支持创新和增长的合作关系，大多数受访高管预计生成式 AI 功能将影响其组织在未来两年内对云计算（59%）和整个业务（62%）的生态系统合作伙伴的选择。

围绕速度和规模重新调整网络安全投资

让 AI 成为加强安全防御的重要工具。鼓励网络安全领导者将生成式 AI 和自动化嵌入到其工具包中，以便快速、大规模地应对安全风险与事件。这将大幅提高生产力，并让网络安全成为业务增长的推动力。

运用 AI 加速实现安全成效。自动处理不需要人类专业知识和判断力的日常任务。运用生成式 AI 简化人类与技术协同合作的任务，如安全策略生成、威胁搜寻和事件响应。

部署 AI 来检测新威胁。更新工具和技术，使您的团队在速度、规模、精度和复杂性上能够跟上攻击者的步伐。运用生成式 AI 更迅速地识别模式和异常，让团队能够及时发现新的威胁向量，从而防患于未然。

发挥合作的力量。与值得信赖的合作伙伴携手合作，共同定义 AI 安全成熟度，并实施全面的生成式 AI 战略，以推动整个组织创造价值。

Gartner 最新生成式 AI 报告：300 个行业用例揭示 GenAI 垂直行业发展的五个关键的不确定性

我们对各行业 GenAI 用例的分析，揭示了高管在规划工作时面临的五个关键不确定性。首席信息官可以利用这项研究来战略性地应对这些不确定性，并最大限度地提高 GenAI 投资的成果。

主要发现

- 我们对 300 多个特定行业的生成式 AI 用例的分析，揭示了五个关键的不确定性，这些不确定性将决定生成式 AI（GenAI）是否能够带来变革性成果，以及何时能够实现：

◎ GenAI 的技术进展

◎ GenAI 的人机界面
◎ GenAI 的商业市场
◎ GenAI 的监管环境
◎ GenAI 的安全、隐私和安全

• 行业业务和技术领导者主要关注了解 GenAI 目前的机遇和风险。他们对 GenAI 的期望，基于其职业生涯中过去采用技术的经验。

• 对 GenAI 未来不确定性的全面考虑，包括极端结果的可能性，可以显著影响投资规模、时机、重点和用例优先级。

建议

• 培养一种能够应对 GenAI 未来不确定性的领导文化。促进对规划假设的批判性质疑，并明确评估新 GenAI 计划的风险和机遇。

• 向执行团队介绍本研究中的五个关键不确定因素。引导讨论这些发展可能如何影响 GenAI 投资、它们与公司的技术采用概况的一致性，以及哪些信号与组织在 GenAI 方面的机会和风险最相关。

• 在设计 GenAI 策略时，优先考虑适应性作为基本要素，确保方法保持灵活并能够响应不断变化的 GenAI 技术和市场动态。

Gartner 发布网络安全应用生成式 AI 指南：应用生成增强功能提升企业网络安全能力和效率的三个领域

生成增强功能是专门为提高知识工作者的生产力、解决网络安全技能短缺问题并降低大型语言模型带来的风险而构建的。安全和风险管理领导者通过在运营中采用生成增强来提高团队的能力。

主要发现

• 与其他人工智能实现相比，生成式人工智能 (GenAI) 解决方案，特别是大型语言模型 (LLM)，具有一系列独特的风险。

• 部署 GenAI 能力以支持内部示例的成本更高，企业机构的试错空间较小。

• GenAI 能够并且将会改变组织在企业几乎所有方面（包括安全团队）设计工作、资源任务和分配职责的方式。

建议

寻求在组织内采用和部署 GenAI 功能的安全和风险管理 (SRM) 领导者（包括 CISO）应做到：

• 开发或获取生成增强 (GA) 来协调与内部企业用例的大语言模型的交互，而不是使用对话界面。这将有助于减轻该技术特有的新的和未探索的风险。

• 从一开始就确保投资回报率一致，并优先考虑在线增强而不是对话部署，以减轻标准聊天界面带来的风险，并降低开发和运营中的相关复杂性 / 成本。

• 专注于构建 / 获取与业务目标明确一致的劳动力增强，而不是寻求 GenAI 可以解决的新挑战。

战略规划假设

• 到 2025 年，30% 的用于内部企业用例的生成式 AI 对话式部署将无法带来任何有意义的投资回报率。

• 到 2028 年，生成增强技术的采用将缩小技能差距，从而消除 50% 的入门级网络安全职位对专业教育的需求。安

奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

奇安信威胁情报中心

中国威胁情报行业领军者

奇安信威胁情报中心是奇安信集团旗下专注于威胁情报收集、分析、生产的专业部门，以业界领先的安全大数据资源为基础，基于奇安信长期积累的威胁检测和大数据技术，依托亚太地区顶级的安全分析师团队，通过创新性的运营分析流程，开发威胁情报相关的产品和服务，输出威胁安全管理与防护所需的情报数据，协助客户发现、分析、处置高级威胁活动事件。

威胁情报中心

威胁研判分析平台ALPHA： 一站式云端SaaS服务的威胁分析工具平台。是安全分析师为同行打造的利器，针对IOC查询、线索关联、事件溯源、样本行为检测和同源分析等威胁分析场景提供全面的解决方案。

高对抗云沙箱分析平台： 提供多种动静态检测、分析技术，展现文件各方面特征，帮助分析师快速判别、并掌握恶意软件的详情。

威胁分析武器库： 服务于安服、安运、安全分析师及各类企业用户。支持IOC自动化数据流检测、失陷情报、恶意IP批量查询；支持邮件批量自动化检测；支持WEB应急日志、主机应急日志分析。

威胁情报系统QAX TIP： 威胁情报平台是情报收集、维护、使用的综合性平台。可帮助企业在安全运营中，利用威胁情报快速检测、响应、分析和预防各类网络攻击威胁，并分析产生行业威胁情报。

威胁雷达： 利用大数据和威胁情报监测技术，整合了奇安信的高、中位威胁情报能力，提供指定区域内网络威胁高位监控、案件拓线分析、样本深度分析等多种能力。

样本同源分析系统： 奇安信威胁情报中心红雨滴团队基于样本基因深度解析，使用机器学习算法用于APT数字武器追踪的可视化分析系统。

高级威胁分析服务： 为网络安全主管单位、政府机构、行业客户及高校科研机构提供情报线索拓线和威胁分析服务，输出深度分析报告供其决策参考。

奇安信威胁情报中心：
ALPHA网址：https://ti.qianxin.com
雷达网址：https://r.ti.qianxin.com
扫描关注我们的微信公众号
邮箱：ti_support@qianxin.com

大事记

奇安信中标中国移动某省网络安全服务项目

近日，奇安信集团中标中国移动某省公司 2024—2025 年网络与信息安全运维支撑服务项目，项目内容包括漏洞扫描、系统渗透测试、网络安全培训与竞赛、安全事件应急处置、重保演练、安全合规运维（如安全审计、代码审计）、安全风险评估（包含网络安全、数据安全、App 合规）等。该项目是奇安信在运营商行业获得的又一个安全服务大单，对于同类省级运营商分公司具有很好的标杆示范效应。

中国海油科技与信息化部总经理单彤文一行来访奇安信

4 月 11 日，中国海洋石油集团有限公司科技与信息化部总经理单彤文、副总经理陈溯一行到访奇安信安全中心，与奇安信集团董事长齐向东、奇安信安全专家就油化行业数字化转型中的数据安全、工控安全、信创安全、人工智能应用及安全等内容进行了深入交流。

奇安信安全大模型线上开放，打造 AI 时代最专业的安全助手

4 月 9 日，奇安信宣布基于 QAX-GPT 安全大模型的知识问答服务体验中心（https://qgpt.qianxin.com/）正式上线。通过简单的自然语言交互，用户能够快速获取威胁情报信息、漏洞情报信息、安全资讯信息、代码片段解读、样本分析报告解读、Web 日志分析等，从而赋能安全团队快速决策，高效应对各类网络威胁，大幅节省复杂任务的处理时间。

截至目前，知识问答服务可以提供威胁情报查询、漏洞情报查询、漏洞资讯解读、安全资讯解读、Web 日志分析、脚本代码片段、文件沙箱报告解读、安全通用知识问答 8 种任务类型。以上能力由奇安信安全能力中心、奇安信技术研究院、安全内参等提供数据和技术支撑。

奇安信与辽宁大学签订战略合作协议 辽宁省网络安全人才培养基地挂牌成立

4 月 2 日，辽宁省委网信办与辽宁大学共建网络与信息安全学院签约暨揭牌仪式在沈阳举行。仪式上，由辽宁省委网信办指导、辽宁大学与奇安信科技集团股份有限公司共建的“辽宁省网络安全人才培养基地”挂牌成立，省委常委、宣传部部长，省委教育工委书记刘慧晏与全国政协委员、全国工商联副主席、奇安信集团董事长齐向东共同揭牌。同时，奇安信与辽宁大学签订战略合作协议，校企双方将在网络与信息安全学科建设和人才培养等方面开展合作。

奇安信集团与黑龙江联通签署战略合作协议

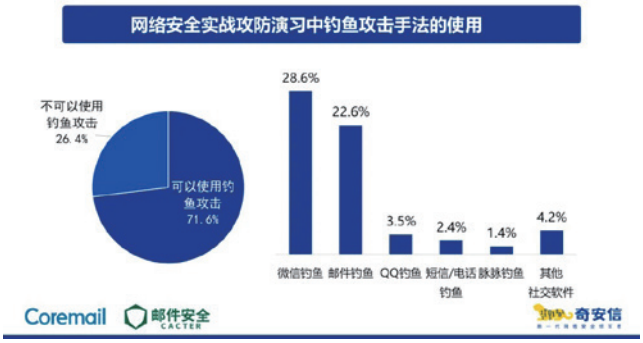
4 月 1 日，奇安信集团与黑龙江联通在哈尔滨成功签署战略合作协议，黑龙江联通党委书记、总经理王传宝与奇安信集团党委书记、董事长齐向东在签约仪式上致辞，并共同为共建的智链网络安全联合实验室揭牌。黑龙江联通副总经理吕威与奇安信集团副总裁张龙代表双方现场签约。

签约仪式后，黑龙江联通总经理王传宝和奇安信集团董事长齐向东共同为共建的智链网络安全联合实验室揭牌，该实验室将重点围绕 5G 安全、工业安全、业务安全等场景进行联合技术攻关，共同打造符合市场需求和技术趋势的安全能力，提升安全水平和竞争力。

邮件安全报告：AI 安全大模型或成邮件安全破局关键

4 月 1 日，奇安信行业安安全研究中心、Coremail 邮件安全人工智能实验室和 CACTER 邮件安全研究团队联合发布了《2023 中国企业邮箱安全性研究报告》。报告从企业邮箱应用、垃圾邮件、钓鱼邮件、带毒邮件、账号安全、未来趋势等多个方面展开分析，并给出了 6 个年度典型案例。

报告还结合真实案例，特别分析了邮件钓鱼在网络安全实战攻防演习中的应用情况，报告显示，邮件钓鱼是攻防演习活动中，仅次于微信钓鱼的第二大社工手法。特别是攻击队编写的钓鱼邮件水准通常远超一般黑产团伙：不仅邮件内容逻辑严谨、极具吸引力和迷惑 性，且攻击脚本还有可能使用多种免杀对抗技术和多重伪装技术。没有经过有针对性的安全意识培训，普通员工很难识破。



全国总工会机关 2024 年第一期工会大讲堂开讲 齐向东作辅导报告

全国总工会机关 3 月 29 日举办 2024 年第一期工会大讲堂，深入学习领会习近平总书记关于发展新质生产力的重要指示精神和党中央决策部署，进一步提高认识、深化理解、明确思路、推动工作。

大讲堂现场，全国工商联副主席、奇安信科技集团董事长齐向东作了题为《统筹好发展和安全两件大事 实现新质生产力跃升》的辅导报告，从理解新质生产力、把握“新”与“质”两方面，发展新质生产力、统筹处理好六对关系，护航新质生产力、网络安全是底板工程等 3 个方面，为工会干部深入学习领会习近平总书记关于发展新质生产力的重要指示精神和党中央决策部署，在发展新质生产力中贡献工会力量提供指导。

奇安信中标某互联网巨头数据安全项目

近日，奇安信中标某头部互联网公司数据安全项目，中标产品包括安全代理网关（SWG）、行为感知分析系统

（BAAS）等。该项目的成功落地，代表了以行为分析为技术，解决数据安全问题的可行性和有效性，对于互联网等多个行业的数据安全建设，具有广泛的推广示范效应。

重庆市委常委、两江新区党工委书记罗蔺到访重庆奇安信

3 月 25 日，重庆市委常委、两江新区党工委书记罗蔺到访重庆奇安信科技有限公司（以下简称“重庆奇安信”），参观了重庆奇安信展厅，听取了重庆奇安信在当地的发展情况、业务布局、科研创新、未来规划等情况汇报，并与工作人员进行了深入交流。

荣誉墙

2024 IT 市场权威榜单：奇安信连续三年获评新一代信息技术领军企业

4 月 17 日，赛迪顾问发布了“2024 IT 市场权威榜单”评选结果，奇安信连续三年获评“新一代信息技术领军企业”。同时，奇安信 QAX-GPT 安全机器人、奇安天盾数据安全保护系统、奇安信网络资产攻击面管理系统（CAASM）、奇安信安全代理网关 SWG、奇安信威胁图谱分析系统共五款产品入选“新一代信息技术创新产品”，全面肯定了奇安信在信息技术领域的技术实力和创新能力。

奇安信获批建设广东省工程技术研究中心

近日，广东省科学技术厅公布了 2023 年度广东省工程技术研究中心名单，由奇安信集团全资子公司深圳云安宝科技有限公司建设的“广东省云计算与大数据信息安全加密工程技术研究中心”，经过科技创新能力、科研综合能力、自主知识产权、管理架构与运行管理机制等多方面考核，获得了广东省科学技术厅批准认定。

奇安信连续多年蝉联安全牛全景图细分领域最多企业

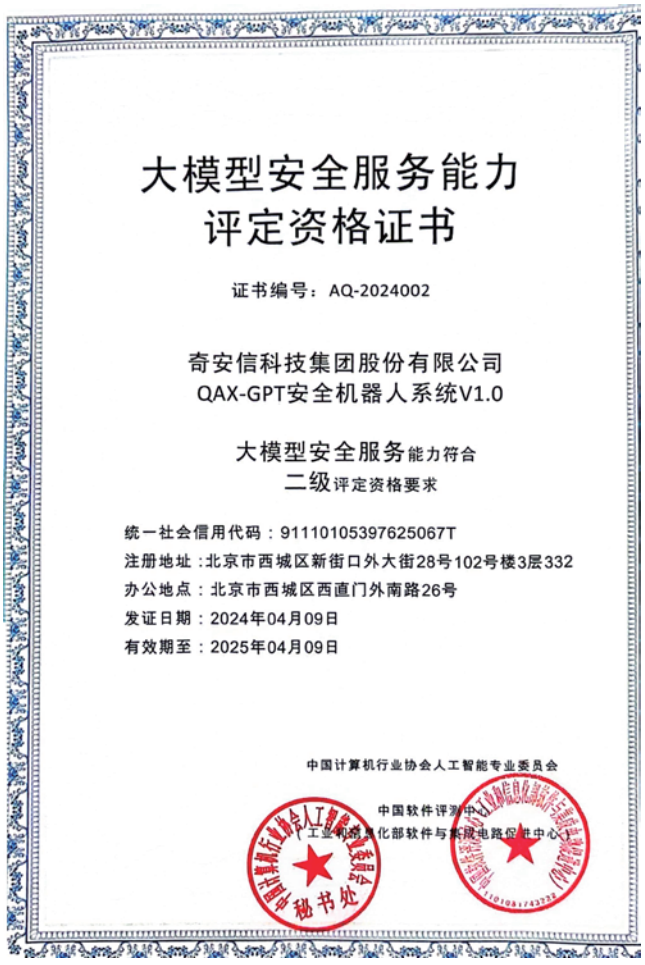
4 月 12 日，安全牛第十一版《中国网络安全行业全景图》（以下简称“全景图”）正式发布。该报告共收到 510 家国内安全厂商 4941 项申报，实际收录 2413 项（包含部分往年已收录项目），共包含了 16 项一级安全分类，108 项二级安全分类。

奇安信集团几乎覆盖了全部的一类安全领域，在二级安全分类覆盖广度也位居领先地位，连续多年蝉联入选全景图细分领域最多的企业。

首批、最高级别！奇安信 QAX-GPT 安全机器人获评大模型安全认证

4 月 9 日，奇安信 QAX-GPT 安全机器人凭借多个方面的综合优异表现，获评国内首批“大模型安全评定证书”，被认定符合二级评定资格要求，这也是迄今为止大模型安全服务能力的最高级别认证，处于业界领先水平。与此同时，AI 安全工作组正式成立，奇安信集团作为唯一网络安全企业，获聘为 AI 安全工作组副组长单位。

为进一步推动人工智能技术安全系列标准完善，在由人工智能场景化应用与智能系统测评工信部重点实验室、人工智能产业创新联盟（中国计算机行业协会人工智能专委会）联合主办的 AI 大模型安全治理研讨会暨 AI 安全工作组成立会议上，奇安信集团作为唯一网络安全企业，获聘为 AI 安全工作组副组长单位。


大模型安全服务能力
评定资格证书

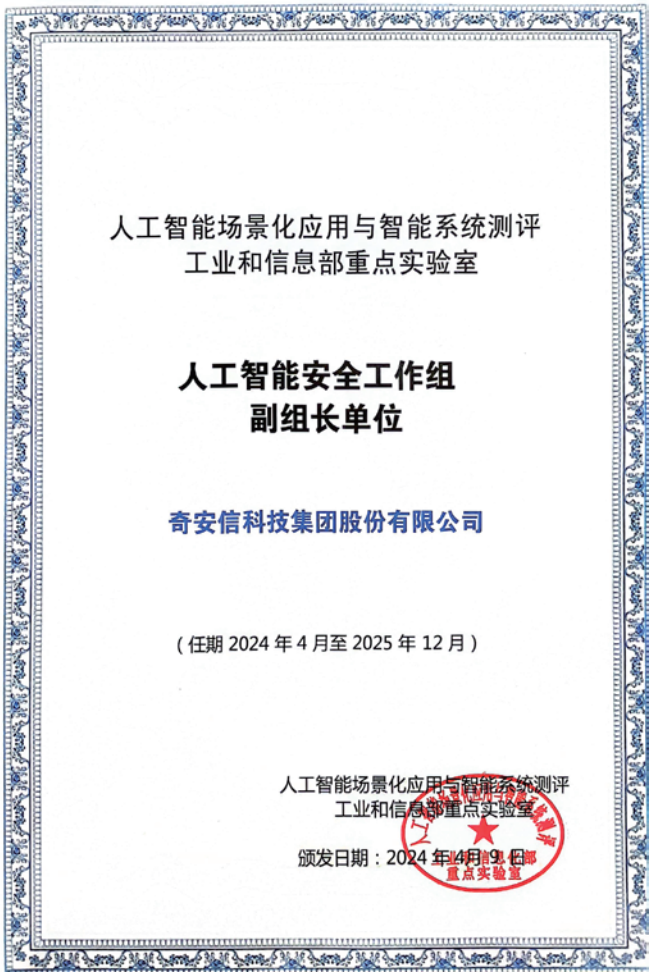
证书编号：AQ-2024002

奇安信科技集团股份有限公司
QAX-GPT安全机器人系统V1.0

大模型安全服务能力符合
二级评定资格要求

统一社会信用代码：91110105397625067T
注册地址：北京市西城区新街口外大街28号102号楼3层332
办公地点：北京市西城区西直门外南路26号
发证日期：2024年04月09日
有效期至：2025年04月09日

中国计算机行业协会人工智能专业委员会
中国软件评测中心（工业和信息化部软件与集成电路促进中心）


人工智能场景化应用与智能系统测评
工业和信息部重点实验室

人工智能安全工作组
副组长单位

奇安信科技集团股份有限公司

（任期 2024 年 4 月至 2025 年 12 月）

人工智能场景化应用与智能系统测评
工业和信息部重点实验室
颁发日期：2024 年 4 月 9 日

奇安信再次入选 Gartner® 《网络检测与响应市场指南》全球代表性供应商

近日，国际市场研究与咨询机构 Gartner® 对外发布了 2024 年《网络检测与响应市场指南》，对全球范围内 NDR 市场发展、技术变化、部署建议、代表供应商等进行了详细

的剖析。其中，奇安信凭借天眼（威胁监测与分析系统），入选为网络检测与响应（NDR）领域全球代表性供应商。

值得一提的是，这已经是奇安信及天眼连续第二年被 Gartner® 评定为全球 NDR 领域的代表性供应商。

奇安信威胁情报运营系统 TIOS 入选中央企业科技创新成果产品手册（2023 年版）

4 月 1 日，国资委发布了《中央企业科技创新成果产品手册（2023 年版）》。本次科技创新成果产品手册共涉及电子元器件、零部件、仪器设备、软件产品、新材料、工艺技术、高端装备七个领域。其中，“奇安信威胁情报运营系统 TIOS”成果入选。

奇安信获评 CCIA 数据安全和个人信息保护社会责任试点评价二星

4 月 2 日，中国网络安全产业联盟（CCIA）数据安全工作委员会（以下简称“CCIA 数安委”）举行促进数据安全合规流通利用专题研讨会，介绍了数据安全和个人信息保护社会责任试点评价工作的开展情况，并发布了试点评价结果。奇安信集团首次参与试点评价就获评二星，在网安企业中名列前茅。同时，凭借在 2023 年度对 CCIA 数安委工作支持的突出表现，奇安信获得“优异表现奖”。

奇安信入选交通运输部公路院交通强国专项试点单位

3 月 30 日，由交通运输部公路科学研究院（以下简称“部公路院”）牵头实施的“综合运输服务‘一票制’信息融合与赋能平台技术研发及示范应用”交通强国专项试点任务启动会，在公路科学研究院顺利召开。奇安信集团、中路高科集团等 11 家参与试点单位共同签署承诺书，部公路院给试点单位颁发了“交通强国专项试点实施单位”荣誉牌匾。

“综合运输服务‘一票制’信息融合与赋能平台技术研发及示范应用”是交通运输部首批综合运输服务交通强国专项试点任务。“一票制”就是要实现旅客出行“一次购票、一次支付、一证（码）通行”，不断改善用户的出行服务体验。

奇安信集团作为国内网络安全和数据安全领域的龙头企业，在“一票制”交通强国专项试点任务中承担网络安全及数据安全体系的设计、研发及保障工作。

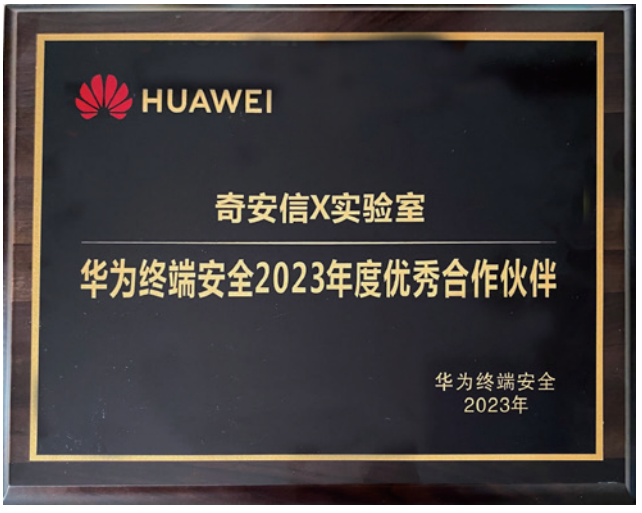
盘古实验室连续四年获评年度华为终端安全突出贡献奖

3 月 28 日，华为终端安全奖励计划年度大会在深圳成功举办，盘古实验室作为长久以来华为终端安全关键技术的支撑方与合作方，凭借在移动安全领域的卓越贡献，连续四年荣获华为终端安全年度“突出贡献奖”。

奇安信 X 实验室获评华为终端安全 2023 年度优秀合作伙伴

近日，华为终端安全奖励计划 2024 年度大会在深圳召开。作为成立不到一年的崭新团队，奇安信 X 实验室因突出贡献，荣获华为终端安全优秀合作伙伴奖。

X 实验室与华为的终端安全团队开展的紧密合作，不仅对提升产品本身的安全性有积极贡献，同时也在加强全球网络稳定性方面发挥了重要作用。



奇安信两方案入选工信部《网络安全保险典型服务方案目录》

近日，工业和信息化部公示了网络安全保险典型服务方案目录，由奇安信集团牵头申报的“网络安全终端（主机）防护类产品 + 网络安全保险方案”和“网络安全远程服务类产品 + 网络安全保险方案”两个方案经评审遴选后，入选《网络安全保险典型服务方案目录》（以下简称《目录》），同时，奇安信集团作为联合申报单位的 8 个方案一同入选，成为此次入选方案最多的网络安全企业。

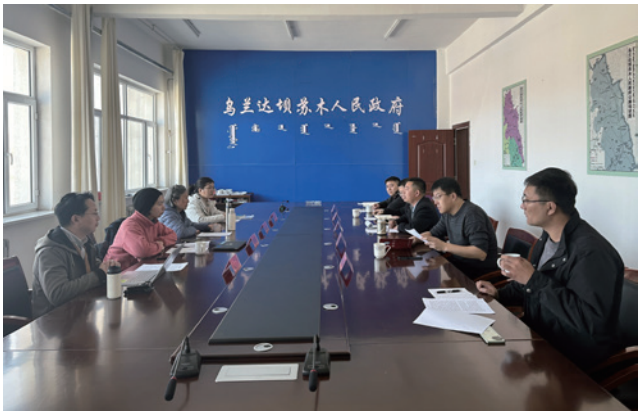
二、产品服务类方案

序号	方案名称	牵头申报单位
37	[redacted]	[redacted]
38	网络安全终端（主机）防护类产品+网络安全保险方案	奇安信科技集团股份有限公司
39	[redacted]	[redacted]
40	[redacted]	[redacted]
41	[redacted]	[redacted]
42	[redacted]	[redacted]
43	[redacted]	[redacted]
44	[redacted]	[redacted]
45	网络安全远程服务类产品+网络安全保险方案	奇安信科技集团股份有限公司

社会责任

关注乡村生态可持续发展 巴林左旗乡村振兴项目组再赴乌兰达坝苏木调研

为助力坚定不移走好生态优先、绿色发展之路，近日，“心安助农·巴林左旗乡村振兴项目”成员邀请相关专家，赴乌兰达坝苏木调研域内生态环境情况，深入牧户、牧场、矿山、沙地、牧道等环境进行实地考察，了解苏木党委政府、农牧民对当地生态和产业发展的需求、问题，探寻适合当地情况的经济、生态共同发展思路。



基金会相关负责人表示，希望通过本次考察活动，了解苏木政府、牧民如何应对生态变化给、生产生活带来的影响，并借助专家力量，共同探索适合当地生态、经济发展的经营建设方式，进一步优化未来三年的发展方案，切实助力本地区乡村可持续发展。安

《赴一场春日约会》主题摄影展

▲ 应用科学研究院　吴天舒

▲ 终端安全 PBU　王洪飞

▲ 财商部　刘芳芳

▲ 安全能力中心　刘晓娟

◀ 前端研发中心　金振祖

网安创新方兴未艾，数字化与智能化引领创业热潮

作者｜陈华平

近年来的宏观经济环境波动对互联网和科技行业带来了巨大的冲击，网络安全行业也受到较大影响。不少人对产业发展前景感到忧虑，但同时也看到，在外部环境不稳定和数字智能加速发展的背景下，网络安全的刚性需求更加明确，面对困难挑战的同时，也孕育着新的机遇。

鉴于当前整体经济不太景气，各种不确定因素影响着企业经营过程中的发展，融资难、市场难让很多创业者充满焦虑，但数据显示，全球网络安全需求依然强劲，人工智能与数据安全、云安全等传统热点领域的融合发展成为新的趋势。

网络安全产业供需两侧的基本面没有改变。从网络安全产业发展的整体规模和趋势来看，根据 Gartner 和 IDC 等机构的预测，预计 2023 年全球网络安全市场规模达到 2200 亿美元，增速为 11% 左右，这反映出网络安全产业供需两侧的基本面没有改变，全球网络安全需求依然强劲。我国网络安全市场面临宏观经济波动与产业生态调整的双重挑战，增速出现短期下降。从我国网络安全企业的主营业务总营收来看，2023 年中国网络安全市场规模约为 800 亿元，但随着网络安全内生及与数字产业的融合发展，更多运营商、IT 厂商、行业数科及集成商入局网安生态，在广义上网络安全产业规模总体可达到 2200 亿元以上，整体增速达到 10% 以上，成长空间更为广阔。

从投融资角度看，网络安全仍是热门投资方向。美国网络安全投融资以私募股权（PE）为主，投资者更加关注商业价值。十年前美国网络安全投融资市场以战投为主，交易量较低。近年来以私募股权为主，交易量大幅增长。由于注重商业价值，美国的网络安全市场具有较高的流动性。这一特点在一二级市场上表现为交易活跃，投资者对于市场信心更加充足，有力地推动了股价的整体上涨。我国网络安全投融资市场当前主要以战投为主，其中，国资占了相当大的比例，收购方注重业务能力的整合，而市场流动性较低，交易相对不活跃。注重网络安全产业对于国家的战略价值在现阶段是首要的，国资加大对网络安全产业的投资和业务整合有利于集中力量应对当前复杂的网络安全形势，同时也应借鉴美国市场经验，引导私募股权进入网络安全市场做商业价值投资，提供更完善的进入和退出机制，丰富和活跃我国网络安全产融发展，加强市场对产业发展的推动作用。

> 网安行业是“长坡厚雪”，
> 我国在推进数字化和智能化进程
> 一定会产生出新安全挑战，
> 驱动安全技术革新和服务模式转变，
> 推动整个行业发展。

RSAC2024 创新沙盒十强出炉，BCS 安全创客汇正在火热报名中。尽管经济大环境对网络安全产业发展带来一定的冲击，但网络安全创新依然活跃。结合近几年历届明星创企的创业方向来看，中美热门领域相对一致，主要涉及人工智能、云安全、数据安全、身份安全、供应链安全等，其中人工智能与数据安全、云安全等传统热点领域的融合发展成为新的趋势。外部环境不稳定、产业数字化和智能化技术发展为网络安全创新带来了更多机会。同时，中美两国数字产业生态的不同，使得需求侧产生了一定的差异。美国市场托管安全服务（MSSP）、M2M 通信安全、区块链安全成为美国今年的网络安全热点；中国市场由于密码合规要求、新能源汽车行业的快速发展及中美高科技领域的竞争等原因，使得密码安全、车联网络安全全及信创领域安全，成为网络安全热点细分领域。

从网络安全产业生态看，我国网络安全生态扩展，供给多样化，需求差异化，为网络安全技术和应用创新提供了更好的环境。我国由政企和行业主导的 to B 市场的客户需求，具有大量具备网络安全完整解决方案能力的安全厂商；传统安全厂商在安全解决方案、安全服务细分领域覆盖更为完整。受外部环境变化、国家政策驱动、应用场景变迁、资本市场助力、全民安全意识提升等多方面因素的影响，网络安全行业进入群雄逐鹿、百花齐放的时代，国内企业积极探索和创新，在一些技术领域我国网络安全产品和服务水平已接近或达到国际一流水准。

产业变革为网络安全带来新的驱动力，也成为网络安全产业创新创业的主要方向。数字经济以业务数字化转型带动的信息系统新建、升级和重构为主，未来仍将是宏观经济的主要驱动力，也是我国网络安全潜力市场。数据要素市场的发展使得数据安全得到政策重点加强，不断完善数据安全治理可操作性。智能化将带来网络安全技术和产品的迭代，也将引领产业变革。信创关基行业稳步发展，也将持续导入安全需求。海外市场为我国网络安全企业带来新的机遇，网络安全国际市场、国家海外利益保护、中东 / 东南亚数字化加速带来的配套网络安全市场均是潜在增长点。

2024 年形势依然严峻，但网络安全产业创新创业依然活跃，适应新形势、新变化并不断寻求突破，为产业大发展做准备。一方面紧跟全球网络安全产业发展趋势，学习国外先进企业经验；另一方面紧跟我国数字智能产业变革趋势，深入挖掘新型安全需求，开拓新的产业增长点，丰富网络安全生态，推动网络安全创新创业公司迅速成长。

网络安全行业是“长坡厚雪”，我们国家在全力推进数字化和智能化进程，在推进数字化和智能化过程中一定会产生出新的安全挑战，并驱动安全技术革新和安全服务模式转变，从而推动整个网络安全行业发展。对于创业者来说需要有战略定力和耐力跑赢网络安全创业这场“冰雪马拉松”，对于投资者来说需要有独立的机会研判和长期价值主义的坚持从而投出高价值高成长的项目。安

关于作者

陈华平

虎符智库专家、安全创客汇评委会主任、奇安信科技集团副总裁。

美军“雷穹”零信任网安项目进展分析与启示建议

作者｜赵慧杰

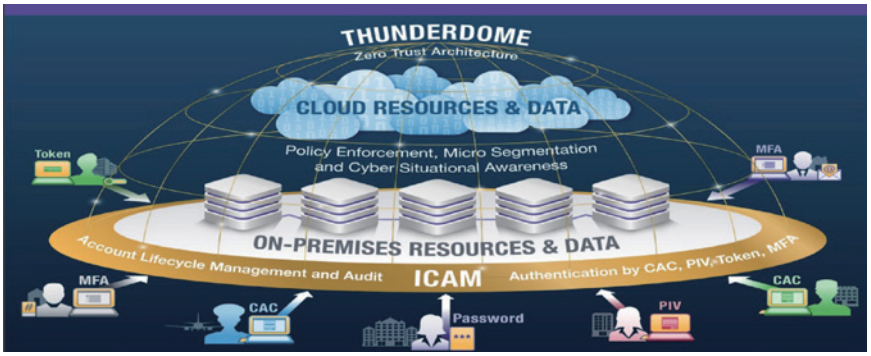
美军认为，传统的以网络为中心的边界防护手段已经无法应对当前和未来的网络安全威胁，正迫切将现有基于边界的网络安全方式转变为零信任网络安全模式。作为美军信息网络运维的主责机构，美国防信息系统局（DISA）正在通过“雷穹”（Thunderdome）项目，推动零信任网络安全架构的实践落地。

一、“雷穹”项目概况

“雷穹”项目旨在为美国防部提供尖端的零信任网络访问和应用程序安全架构，以改变美军处理网络安全和网络基础设施的方式。美军视“雷穹”项目为加强国防部网络安全的创新解决方案，能够在不断发展的网络安全环境中保护其网络和数据免遭各类威胁。

（一）基本情况。“雷穹”是DISA于2021年启动的零信任网络安全项目，其革命性方法的核心在于强大的网络强化工具和尖端分段技术，为针对敌对威胁提供强化防御奠定基础。该项目旨在提供一整套IT和基于网络的技术，利用体系身份凭证和访问管理（ICAM）、商业安全访问服务边缘（SASE）及软件定义的网络和安全工具来提供保护和可靠性。DISA拟利用“雷穹”为国防部实施重大转变，为更安全的数字环境提供下一代解决方案。

（二）基本原则。“雷穹”项目通过基本原则的动态相互作用重新定义网络安全的基础，包括：一是零信任安全重塑，即通过始终验证任何用户或设备来增强传统的纵深防御安全模型；二是更高的安全性和更强的性能，即同时增强安全性和网络性能；三是以身份为中心的访问，即植根于使用增强的安全控制来验证用户身份的需求，仅向需要了解信息的用户提供访问权限；四是捍卫美国防部使命，即采用3个基本且现代的零信任概念，包括验证用户和设备、



有条件提供访问和特权，以及明确验证数据和应用程序。

（三）突出特性。“雷穹”项目超越了传统安全范式的界限，开创了防御、优化性能和简化管理的新时代。其突出特性包括：一是实现无缝身份和端点协同；二是简化访问并释放云潜力；三是开创零信任合规性；四是符合美国政府和军队战略；五是提升用户体验和效率；六是为任务合作伙伴提供选择和灵活性；七是提高互操作性，并增强命令和控制。

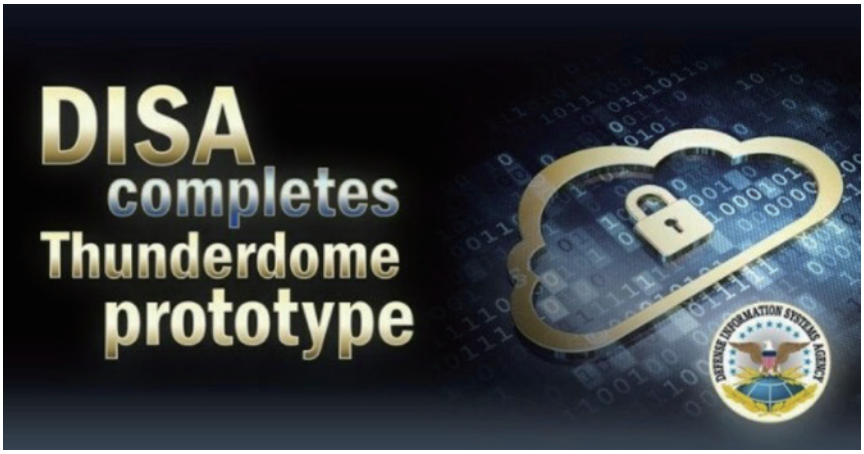
二、“雷穹”项目推进情况

为确保该前瞻性网络安全项目顺利落地，DISA 采取了需求征集、原型研发和生产部署的三阶段渐进性计划推进方式。

（一）征集需求。2021 年 7 月，DISA 向行业合作伙伴发布信息征集，寻求关于“雷穹”零信任架构和实施的拟议解决方案的白皮书。根据信息征集书，DISA 希望采用一种新方法，为安全访问服务边缘（SASE）、具有客户边缘安全堆栈和应用程序安全堆栈原型的软件定义广域网（SD-WAN）架构提供初始的最简可行产品，并计划到 2025 年对这些能力进行改进和运营实施。供应商的技术优势评估标准涉及 SASE、安全堆栈、网络态势感知、用户和设备验证、安全策略、访问策略、端点技术、数据遥测、分布式拒绝服务攻击抵御、安全 DNS 架构、网络和安全服务设计部署的自动化和编排、软件定义广域网（SD-WAN）等方面。

（二）研发原型。2022 年 1 月 24 日，DISA 授予博思艾伦公司一份价值 680 万美元的合同，用于开发原型“雷穹”解决方案。DISA 希望在为期 6 个月的工作中，通过利用安全访问服务边缘和软件定义广域网等商业技术，在操作上测试如何实施零信任参考架构，从而生产一个可在美国防部范围内扩展的“雷穹”原型。2023 年 3 月 1 日，DISA 宣布成功完成“雷穹”原型。DISA 表示，该机构在过去的 12 个月里开发并实施了一个零信任网络访问架构，这将加强美军网络，并阻止对手日益增长的网络威胁；“雷穹”原型测试证明，包括安全访问服务边缘（SASE）、软件定义广域网 / 客户边缘安全堆栈和应用程序安全堆栈在内的商业技术，可以提高现有环境的安全性和网络性能。

（三）全面生产。2023 年 7 月 26 日，DISA 授予博思艾伦公司一份大规模部署“雷穹”的后续生产其他交易协议（OTA）。该单一授予合同的履约基期为 1 年，并有 4 个 1 年的选择期。根据该协议，博思艾伦将帮助美国防部迈向零信任架构。博思艾伦将广泛实施和运营“雷穹”的零信任网络访问和应用程序安全架构，该架构将强化国防部网络，并通过采用网络和资源访问工具及分段技术来帮助作战人员防御敌对活动。“雷穹”零信任架构未来有望在美军全面铺开部署，并从根本上提升美军网络安全防御的水平。

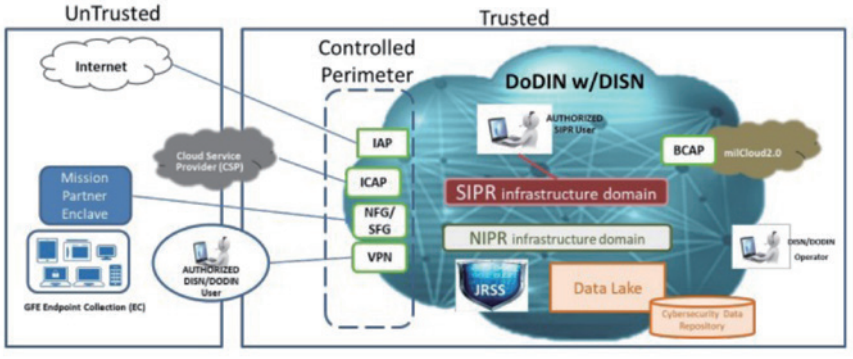


三、“雷穹”设计与实施情况分析

基于 DISA 授权的协议，博思艾伦公司将协助大规模部署“雷穹”零信任网络访问和应用安全架构，助推美军机构全面迈向零信任范式。根据该公司对零信任网络安全架构的整体理念和方法论，分析认为该公司计划全面审查美军机构的优势和挑战，制定通向零信任架构的路径，利用商业技术付诸行动，从而协助美军落实核心零信任原则。

（一）致力于解决四项挑战问题。博思艾伦公司表示，实施“雷穹”零信任架构的主要挑战存在四个方面：一是遗留基础设施。云环境和遗留 IT 基础设施的拼凑产生了众多漏洞，同时安全性在数字现代化工作中往往是事后考虑因素。二是数据管理。必须厘清如何发现、分类和标记其数据，然后才能根据批准的策略启用受限访问。三是身份管理。正确进行身份管理对于实现零信任原则至关重要，而应用条件访问需要强大的身份验证和强大的属性。四是日志数据处理。零信任对持续监控的关注会导致大量日志收集，需要智能、高效地处理日志数据，来避免安全团队“不堪重负”。

（二）致力于采用四个重要方法。为解决上述挑战问题，博思艾伦“雷穹”解决方案建基于以下四个方法：一是模型评估利用零信任成熟度模型五个成熟度级别（（初始、最低、基本、创新和领先）来评估在美国防部在零信任七大支柱方面的能力。二是基线建立。在零信任、当前工具和能力的背景下围绕威胁了解自身优势和挑战，同时考虑关键任务、战略优先事项、新兴威胁和风险偏好。三是方案创建。通过评估现有能力和差距来权衡优先级并创建特定于支柱的路线图。四是量身定制。通过制定量身定制的实施指南来实现可衡量的改进，如在整个基础设施中以协调的方式部署全面的安全监控、基于风险的精细动态访问控制和系统安全自动化。



（三）致力于实施四大关键步骤。博思艾伦构想采用四步方法来识别和部署新的网络安全解决方案，以转向零信任架构。一是诊断。围绕零信任重点领域，确定当前的 IT 能力和路线图，针对七大支柱进行零信任成熟度评估，客观了解美国防部优势和改进领域。二是设计。创建零信任总体策略，确定解决方案来弥补诊断阶段发现的关键差距，提供统一的目标状态和路线图，并优先制定强有力的治理政策，推动条件访问的执行。三是开发。在实验室环境中测试新的配置、集成和解决方案，对新技术进行概念验证试验，并制定迁移和实施计划。四是部署。使用经过验证的实施计划重新配置现有系统，安装并集成新的解决方案以缩小能力差距，将用户迁移到新的解决方案，并进行持续监控。

四、对我军事国防建设的启示与建议

零信任架构颠覆了传统的网络安全新范式，是信息数字时代军事网络安全架构演进的必然选择。美军通过“雷穹”项目为零信任能力下一步实施和部署奠定了良好的基础，我军应借鉴美军的经验和教训，并根据自身情况开展系统性布局和建设推进。

（一）通过转换范式强化军事网络安全。当前，国防网络基础设施变得日益复杂，这种复杂性已经超越了传统的基于边界的网络安全方法。随着军事用户和终端数量的不断增加，军事网络被攻击面也不断增加，网络安全防御面临极限挑战。我军迫切需要将现有基于“边界”的网络安全方式转变为“零信任”方式，通过为军事网络内的特定应用程序和服务创建离散的、精细的访问规则，从而显著抵消网络漏洞和威胁。

（二）通过结合实际情况制订实施方针。零信任不是简单的产品或服务，而是一种设计安全防护架构的方法，旨在以更具适应性、灵活性和敏捷性的方式，有效阻止当前和未来的网络攻击。中美军方网络在网络架构、环境、设备等方面均有极大差异，因此我军在开展军事网络安全体系建设方面绝不能生搬硬套、照猫画虎，必须因地制宜，结合实际情况制订整体规划，并有计划、有步骤、有秩序地推动方案落地，才能构建动态开放的国防网络安全体系，为军事网络运维和网络空间防御提供强大保障。

（三）通过技术攻研创新解决瓶颈问题。零信任架构理念新、应用场景多，技术的应用部署较为复杂。“雷穹”项目紧紧围绕美国防部定义的用户、设备、应用程序和工作负载、数据、网络和环境、自动化和编排、可见性可分析等七大零信任支柱开展部署，全面运用了现有的先进网络安全技术能力。我军应加强零信任核心技术研发，重点研究突破软件定义边界、身份权限管理和微隔离等关键技术，着力解决技术瓶颈。同时，还应根据军队的安全需求、应用环境和业务场景，制订差异化零信任创新解决方案，加快概念、构想和技术的转化落地。

（四）通过军民融合推动创新技术落地。国防网络安全是高度军民融合的领域，网络安全装备与技术发展是多专业、多领域在多层级、多角度的融合。美军推动“雷穹”项目方向充分利用了国防承包商的力量，前期向业界充分征询方案意见，中期授权承包商开发原型并进行效果测试，后期全面投产和部署。我军应集聚军方、业界和学术界等各方力量，探索关于零信任的解决方案和设计，利用商业技术创新来促进科技成果转移转化，提升国防和军队网络安全防御。安

关于作者

赵慧杰

虎符智库专家、网络空间安全军民融合创新中心高级研究员、奇安网情局主编。主要从事网络安全领域研究工作，对国外国防网络建设发展、网络空间战略政策、网络空间国际斗争、网络武器研发和新兴技术应用等长期进行跟踪研究。

为什么情报共享对建立强大的集体网络防御计划至关重要

作者 | Marc Solomon

借助自动化、详细、情境化的威胁情报，组织可以更好地预测恶意活动，并利用情报加快对已证实攻击的检测。

当我们谈论情报共享时，我们会自动想到间谍、双重间谍、间谍活动和秘密行动。但如今，共享情报、与行业同行合作，已成为企业的当务之急，而且可能没有我们之前想象的那么隐蔽。特别是在与网络犯罪分子的无情战争中，我们共享有关网络安全威胁和漏洞的信息至关重要，因为这正是我们的对手正在做的事情。

网络犯罪分子共享情报以支持精心策划的攻击。事实上，共享有关数据泄露机会和可利用漏洞的情报对于网络犯罪分子更有效地执行攻击至关重要。这就是为什么作为一个行业、供应商和企业组织，我们合作并建立情报网络、社区和能力非常重要。成立于第二次世界大战后的五眼联盟（FVEY）无疑是世界上最大、最持久的多国情报共享网络之一。这个错综复杂的全球情报网络，由五个英语国家组成，是最早的信息共享社区之一。

快进到今天，威胁情报共享和协作已成为大多数大型企业的首要任务。客户和供应商多年来一直是信息共享组织 ISAC 的成员，其中一些最重要和最活跃的成员与关键的国家基础设施有关。例如，电力信息共享和分析中心 (E-ISAC) 为电力行业提供质量分析和快速共享安全信息，以了解如何减轻对电网复杂、不断变化的网络和物理安全威胁。运营商和精选合作伙伴致力于通过提供独特的见解、领导力和协作来降低整个北美行业面临的网络和物理安全威胁的风险。

数字化改变了我们关键的国家基础设施 (CNI) 部门，推动了其在服务提供、可靠性和敏捷性的进步，从而更好地服务公民并推动经济增长。然而，CNI 部门受到出于经济或意识形态动机、寻求破坏服务的威胁行为者的无情攻击。

网络战、民族国家行为者，特别是勒索软件攻击仍然对 CNI 组织的安

> 威胁情报共享和协作
> 已成为多数大型企业首要任务。
> 深入研究威胁情报时，
> 组织在保护敏感内部运作的同时，
> 与外部合作伙伴进行合作面临几个挑战。

全构成重大风险。事实上，黑客不断开发专门针对支撑 CNI 的工业控制系统的定制工具，目的是获得持久的完整系统访问权限。

保护关键的国家基础设施免受网络威胁需要采取多方面的方法，加强安全控制、提高意识和促进协作，对于保护关键基础设施至关重要。信息和情报共享也是建立强大的集体网络防御计划的基本要素。

事实上，更多地了解复杂网络威胁的需求变得如此重要，以至于 2021 年白宫《关于改善国家网络安全的行政命令》将“消除信息共享障碍”列为首要要求。如今，越来越多的法规脱颖而出，例如，将于 2025 年 1 月生效的《数字运营弹性法案》(DORA)，专门旨在解决欧盟金融监管在运营弹性方面的差距。新立法的支柱之一侧重于与网络威胁和漏洞相关的信息和情报共享。

深入研究威胁情报时，组织在保护敏感内部运作之际，与外部合作伙伴进行合作面临几个挑战。公司必须维护对其数据的主权，确保数据被拥有、控制和存放在可以自主和保密运行的私人实例中。同时，他们需要一个平台，允许外部实体（如联合运营和合作伙伴网络）对这些情报进行受控访问，以确保协作不会损害安全性。

现代网络安全的复杂性需要支持多种共享模型，从适应各种语言和格式的机器对机器交换，到人类可读数据的分发。访问以用户为中心的仪表板、综合报告和复杂的分析工具对于可操作的情报至关重要。任何平台还必须满足外部团队不同成熟度水平的需求，确保可用性和可访问性，无论他们的专业知识如何。其还必须与不同的基础设施和架构无缝集成，从而实现跨网络安全生态系统的威胁情报共享的通用且包容的方法。

有趣的是，当人们考虑威胁情报共享时，他们通常认为这是人与人之间的。然而，如上所述，共享也可以是机器对机器或机器可读和人类可读的。人类可读格式的优点是人类阅读时很容易理解。机器可读格式是专门为设备和机器设计的，因此该格式对于人类理解来说很复杂。机器可读格式对于机器来说编码起来更容易、更快捷。好消息是，机器可读格式的数据可以自动提取、并用于进一步处理，无需人工参与。

因此，威胁情报传输的整个概念就像一个由数据基础组成的金字塔，通过信息上升到知识并达到智慧的顶峰。我们在这里讨论的是如何将数据转化为理解、知识和智慧。

当某人刚接触某个角色和 / 或即将离开某个角色时，我们会谈论“知识转移”。“情报转移”略有不同，因为它可以帮助人们获取知识，但它会将其置于上下文之中，帮助个人学习，但它也可以通过上下文化和丰富的额外高保真数据，帮助机器更好地完成工作。要使这一切发挥作用，必须信任结果、信任数据和机器所学到的东西。安全团队必须对数据充满信心，他们必须相信数据告诉自己的内容，最终，安全团队必须相信自动化不会带来任何破坏。这说起来容易做起来难，因为去年的研究强调，人们对自动化的信任度很低，这是组织实现更多网络安全用例和流程自动化的主要障碍之一。

威胁情报共享的主要目标是帮助组织更好地了解最常见和最严重问题的风险，如 0day 威胁、高级持续性威胁和漏洞利用，并使他们能够就应对这些威胁做出明智的决策。借助自动化、详细、情境化的威胁情报，组织可以更好地预测恶意活动，并利用情报加快对已证实攻击的检测。威胁情报共享还可以促进组织和整个行业之间更多的协作关系。加强生态系统中的协作和对网络安全自动化的信任，将有助于赢得与网络对手的战斗。安

关于作者

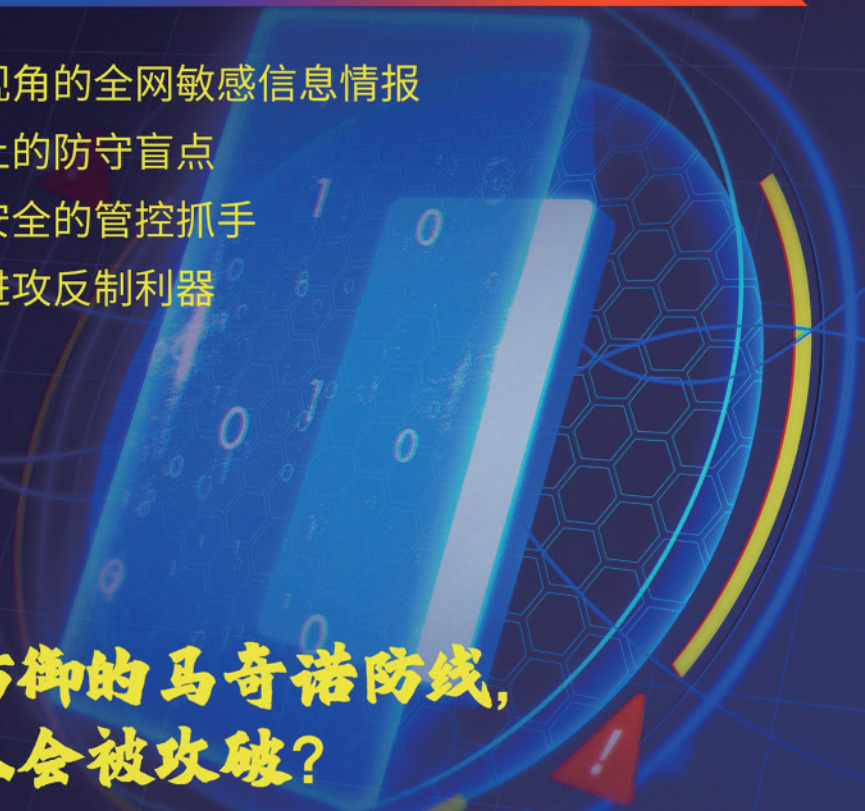
Marc Solomon

ThreatQuotient 的首席营销官。

奇安信

敏感信息泄露情报服务

- 攻击队视角的全网敏感信息情报
- 急需补上的防守盲点
- 供应链安全的管控抓手
- 预防性进攻反制利器



纵深防御的马奇诺防线，为什么会被攻破？

- 完整的防御体系，既要考虑正面防御，侧翼的情报收集和对抗也必不可少！
- 忽视全网视角的情报，是防守的重大盲点！

服务定位 SERVICE POSITIONING

- **攻击队视角**：使用渗透专家交付，不是简单的信息收集。
- **全网视角**：核心功能是从外部探测全互联网第三方应用中的敏感泄露数据；而非只关心自己的网络和应用。
- **情报级**：专家梳理的情报级信息，而不是简单数据抓取：给出利用思路和可能的攻击链，更有详细的整改建议。

奇安信安服团队

奇安信

新一代网络安全领军者

「零事故」安服团队重磅力作

900余次实战攻防演练的经验总结

从红队、蓝队、紫队视角全面解读攻防演练

扫码购买

奇安信连续三年位居
“中国网安产业竞争力50强”
第一名

6月20日，中国网络安全产业联盟（CCIA）
公布“2023年中国网安产业竞争力50强”榜单，
凭借扎实的技术实力和领先的市场表现，
奇安信连续三年高居榜单第一名。


奇安信科技集团股份有限公司

CCIA 50强

2023年中国网安产业竞争力50强

编号：CCIA-2023JZL-01

中国网络安全产业联盟

2023年6月

“2022年中国网安产业竞争力50强”榜单

TOP15	公司名称
1	**奇安信科技集团股份有限公司**
2	深信服科技股份有限公司
3	启明星辰信息技术集团股份有限公司
4	华为技术有限公司
5	天融信科技集团股份有限公司
6	绿盟科技集团股份有限公司
7	腾讯云计算（北京）有限责任公司
8	新华三技术有限公司
9	阿里云计算有限公司
10	杭州安恒信息技术股份有限公司
11	三六零数字安全科技集团有限公司
12	亚信安全科技股份有限公司
13	中电科网络安全科技股份有限公司
14	杭州迪普科技股份有限公司
15	山石网科通信技术股份有限公司