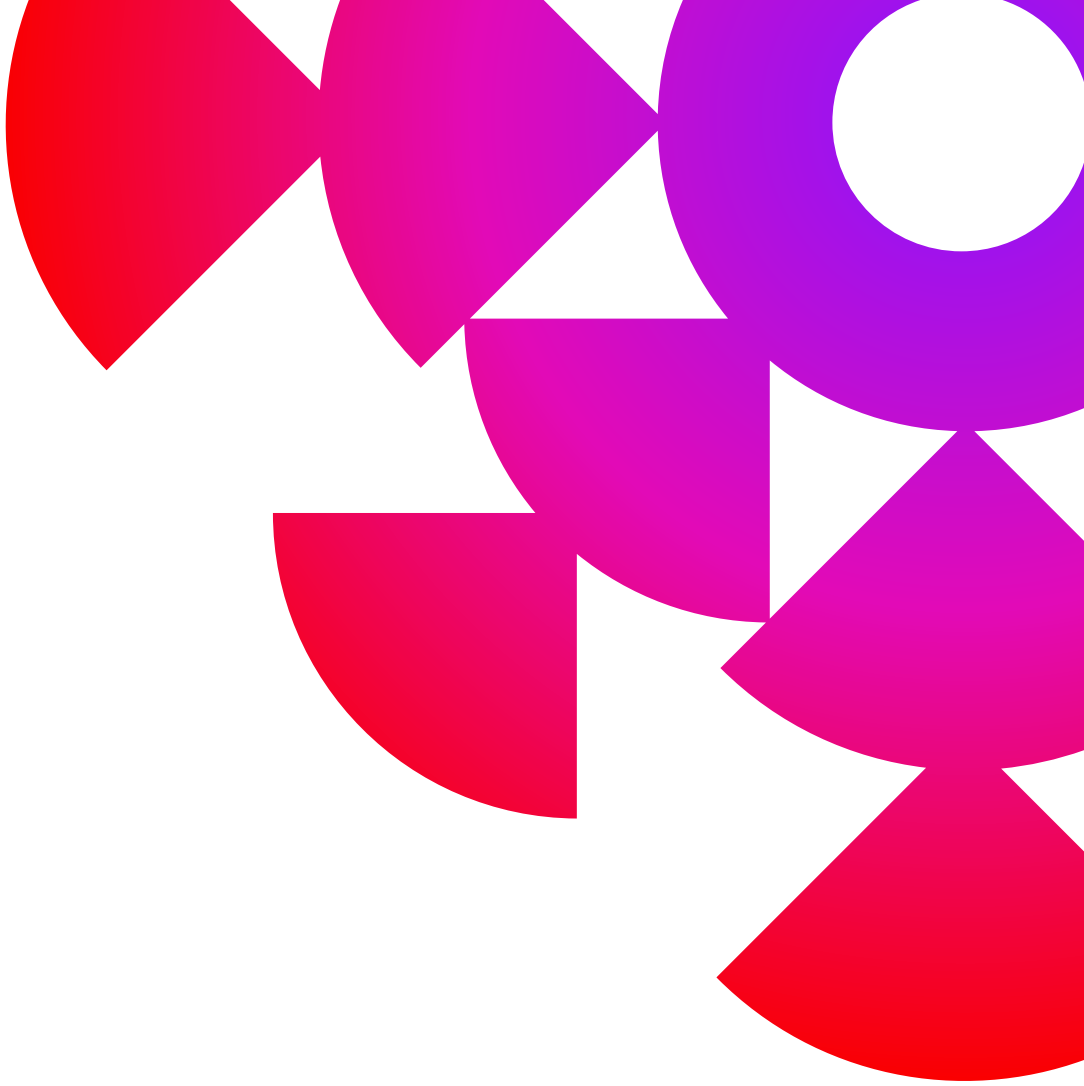


CLAROTY 半年度 ICS 风险和漏洞报告：2021 年下半年

Claroty Team82 编制

CLAROTY

目录

03 执行摘要

04 安全研究和披露趋势

05 ICS 漏洞带来的威胁和风险

08 值得关注的趋势

11 关于 Claroty Team82

12 对 Claroty 发现并在 2021 年下半年披露的 ICS 漏洞的评估

15 对 2021 年下半年披露的所有 ICS 漏洞的评估

24 缓解措施和修补措施

29 CVSS 信息

35 已利用的 CWE

37 与 2021 年下半年 ICS 风险和漏洞形势相关的关键事件

39 建议

41 致谢

41 关于 Claroty

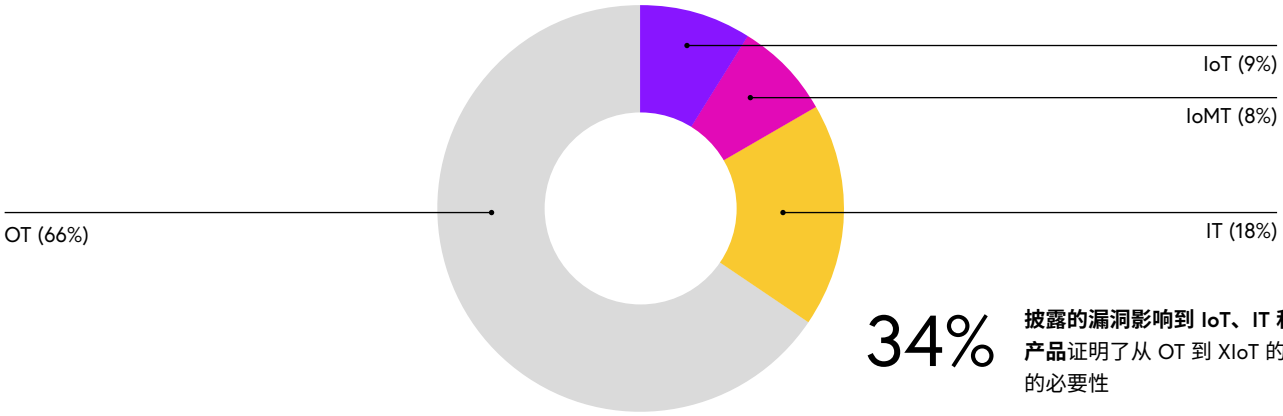
执行摘要

我们正在快速进入一个高度连接的信息物理系统成为常态的时代，IT、OT 和 IOT 安全管理之间的界限已经模糊，难以辨认。

所有这些都将连接到云并从云端进行管理，并且将处理海量的数据，以对性能进行微调，提供关键服务分析，并确保关键工业、医疗保健和企业流程的完整性。

这是扩展物联网 (XIoT) 的新范式，它增强了对及时、有用的漏洞信息的需求，以便更好地为风险决策提供信息。今天，Claroty 发布了第四份半年度 ICS 风险和漏洞报告。该报告由 Claroty 的研究部门 Team82 编制，旨在定义和分析与主要自动化产品和跨领域使用的联网设备有关的漏洞情况。

虽然与前六个月相比，2021 年下半年成为焦点的攻击数量有所减少，但这些事件只会助长决策者最终对 XIoT 网络安全的优先重视。从我们这份报告的分析中您还会看到，去年下半年披露和解决的联网物联网和医疗设备的漏洞，以及越来越多的 IT 漏洞比例，飙升至 34%。



34%

披露的漏洞影响到 IoT、IT 和 IoMT 产品证明了从 OT 到 XIoT 的安全的必要性

数字化转型以及 ICS 和 IT 基础设施的融合也在推动曾经单纯关注 OT 的研究人员将其工作扩展到 XIoT。

这表明，企业确实在融合安全管理系统下融合了运营技术、IT 和 IoT。因此，资产所有者和运营商必须全面了解其环境，以管理漏洞并减少风险。

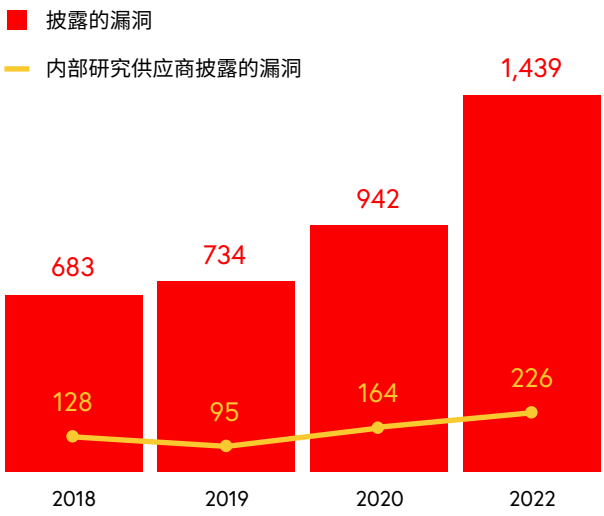
在这份报告中，Team82 全面审视了 2021 年下半年公开披露的 ICS 和 IoT 漏洞，包括 Team82 发现的漏洞以及受影响的供应商、独立安全研究人员和其他组织内部专家发现的漏洞。

我们敦促安全管理人员、资产所有者和运营商将这份报告作为一种资源，它不仅提供了关于工业设备中普遍存在的漏洞的数据，而且还提供了围绕这些漏洞的必要背景，以评估其各自环境中的风险。

我们来了解一下半年度 XIoT 风险和漏洞报告中的一些关键数据点：2021 年下半年：

安全研究和披露趋势

- 在 2021 年下半年，我们共计发布了 **797** 个 ICS 漏洞，这些漏洞影响了 **82** 家 ICS 供应商。其中 **21** 家受影响的供应商是新近受到影响的供应商，因为他们在过去几年中没有发表过披露信息。这 **21** 家受影响的供应商中，大多数属于自动化、制造业和医疗保健行业。
- 在 2021 年下半年，Team82 披露了 **110** 个漏洞，这些漏洞影响了 **16** 家自动化供应商。自成立以来，Team82 已经发现并向受影响的供应商报告了 **260** 多个漏洞。
- 数据显示，ICS 漏洞披露的数量和供应商所开展的内部研究披露的漏洞数量都在增加。巧合的是，开展内部研究的供应商数量增加了 **35%**。

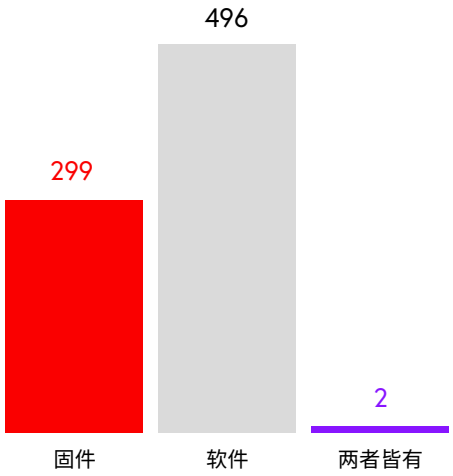


+110% **增加**
披露的漏洞

+76% **增加**
供应商开展的内部研究披露的漏洞数量

- 得益于西门子 CERT 团队开展的内部研究，西门子成为报告漏洞最多的供应商，达到 **251** 个，其次分别是施耐德电气、研华、台达电子和三菱。

- 在 2021 年下半年，大多数漏洞都会影响到下面的软件组件，鉴于软件的修补比固件更容易，防御者有能力在其环境中优先进行修补。

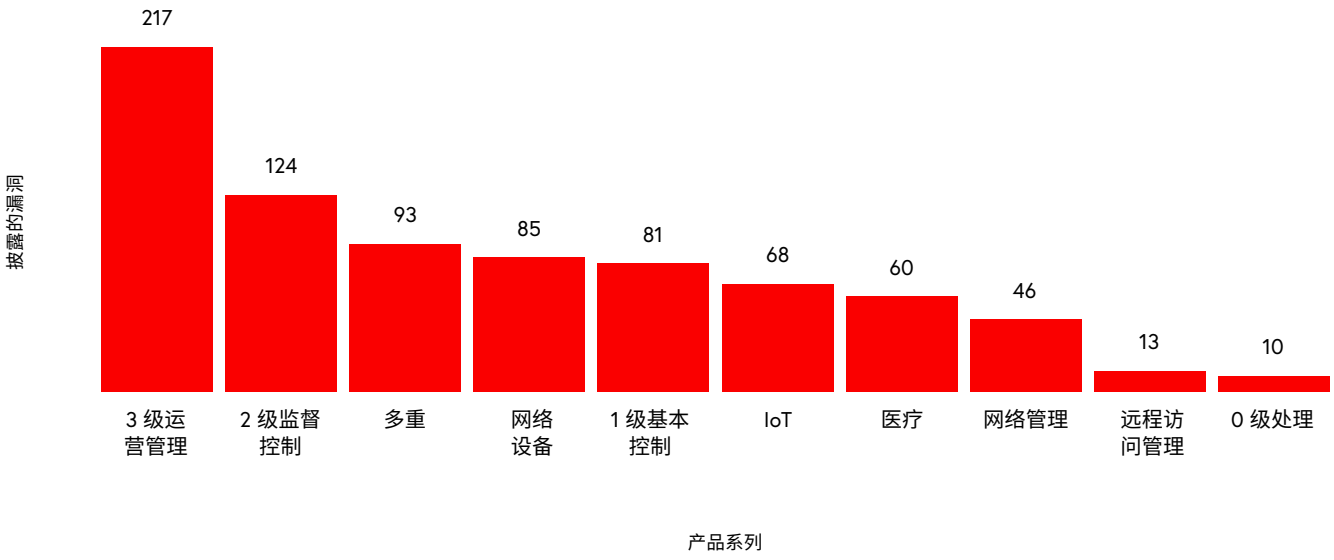


ICS 漏洞带来的威胁和风险

- 连续两份报告显示，符合运营管理（普渡模型的第 3 级）的产品受已披露漏洞的影响最大（217 个，或 27%），见下表。此级别的软件组件包括处于生产工作流程核心位置的服务器和数据库。这一级别的技术还会将从现场设备上收集的数据反馈给更高级别的业务系统，或在云端运行的系统。

  在基本控制（第 1 级）和监督控制（第 2 级）级别运行的产品受到 2021 年下半年披露的 25% 的漏洞影响（205 个）。处于基本控制级别的包括可编程逻辑控制器 (PLC)、远程终端设备 (RTU) 和其他监控 0 级设备的控制器，如泵、执行器、传感器等。处于监督控制级别的包括人机界面 (HMI)、SCADA 软件和其他用于监视和处理 1 级数据的工具。

受影响的产品系列



防御者必须了解针对工业网络和 IoT 设备的攻击者最常利用哪些威胁向量。对漏洞所在位置的适当可见性使组织能够正确修补或缓解软件和固件产生的问题，从避免网络和流程面临风险。

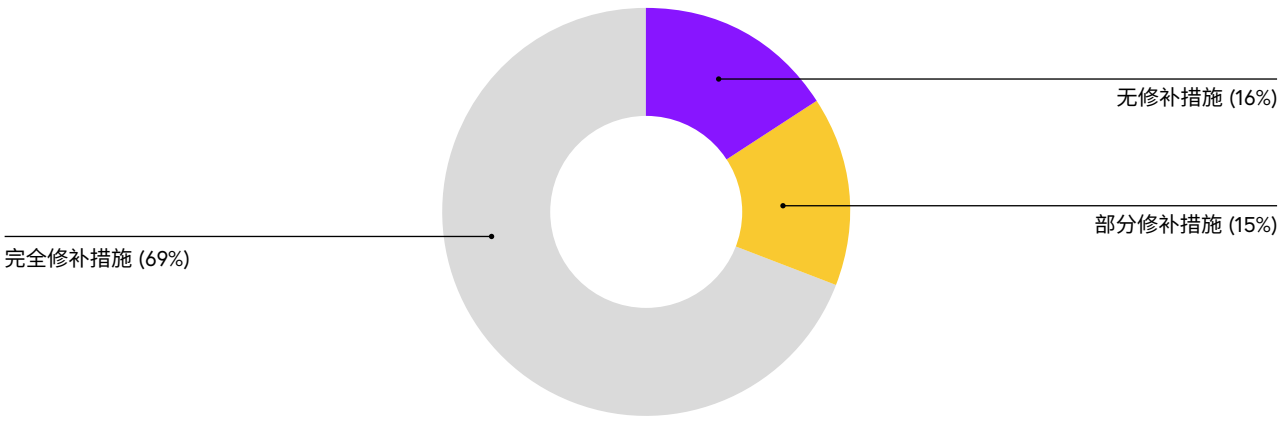
远程可利用漏洞：Team82 的数据显示，在所披露的漏洞中，有 63% 可能通过网络攻击向量被远程利用。这一数字比 2021 年上半年略上升 2%。

本地攻击向量：2021 年下半年，可在本地利用的漏洞的百分比下降到 31%。为利用这些漏洞，攻击者需要一个单独的网络访问向量，以便利用这些缺陷；这将包括用户互动，如网络钓鱼和垃圾邮件，以便在网络内获得最初立足点。

深度挖掘：**94%** 的运营管理信息通过本地攻击向量披露，需要用户互动才能利用，这加强了持续教育的必要性，以防止网络钓鱼攻击并阻止破坏性勒索软件攻击的浪潮。

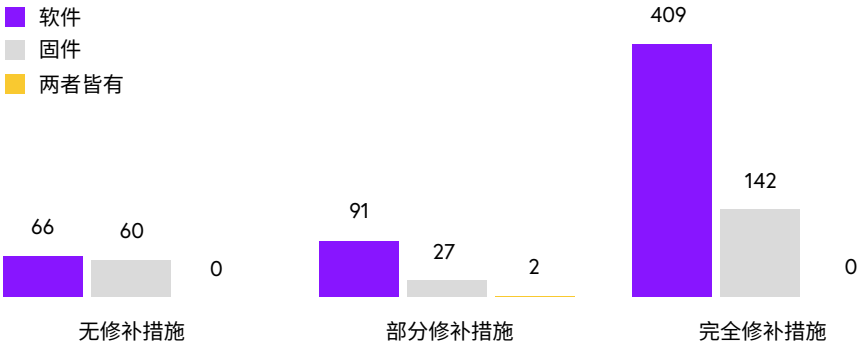
尽管很关键，但披露漏洞只是漏洞管理过程中的一个步骤。补丁和缓解措施对资产所有者、运营商和安全管理人员来说是最重要的。随着每天越来越多的联网设备上线，越来越多的系统可以公开访问，并提高了及时修复的紧迫性。

缓解措施和修补措施：由于许多众所周知的原因，更新工业控制系统或 SCADA 软件通常具有挑战性，者主要与正常运行时间和可用性要求有关。由于开发和实施更新所涉及的复杂性，固件更新也很困难。这些周期可能比传统的 IT 补丁管理要长得多，往往使缓解措施成为防御者的唯一修补选择。供应商和内部安全分析师及管理人员还必须优先跟踪报废产品以及更新可能具有挑战性或停机时间不可接受的产品中的漏洞。ICS 产品的保质期很长，随着漏洞（尤其是关键的远程代码执行或拒绝服务）的累积，风险会显著增加。



Team82 的数据与这些趋势相关：

按固件/软件划分的修补



74% **的完全修补漏洞**均基于软件。强调鉴于软件的修补比固件更容易，防御者有能力在其环境中优先进行修补。

62% **的部分修补或无修补漏洞**在被利用时可能导致远程代码执行或拒绝服务

- 大多数完全修补的漏洞均存在于普渡模型运营管理级别的产品中，其次是监督控制和网络管理。
- 对固件的修补措施较少。当它们由受影响的供应商提供时，网络设备固件的解决频率最大，其次是基本控制级别的产品，以及 IoT 设备。
- 报废的产品在工业环境中普遍存在；大多数组织都不愿淘汰监督关键流程的遗留系统。Team82 的数据显示，有 29 个漏洞影响了报废产品，并且没有计划对其进行修补。在所有情况下，受影响的供应商不再支持这些产品。
- 报废产品中 48% 的漏洞会影响到基本控制设备 (PLC、RTU)。这些缺陷中有近 60% 如果被利用，会使受影响的设备崩溃。

值得关注的趋势

云预测：保护 XIoT

扩展物联网 (XIoT) 是一个涵盖对我们生活至关重要的信息物理系统的总称。联网设备、操作技术、医疗保健系统等等正在迅速连接到网络和云端，这不仅是为了安全管理，也是为了数据分析、性能跟踪和增强等等。

这些效率对业务线所有者很有吸引力，而资产所有者和安全团队的工作就是要确保这些连接。这在许多方面都是一项挑战。

Team82 一直在积极研究云管理的 OT 设备的漏洞，不仅包括这些设备可能受到的影响，还包括云端的管理控制台。对于将 XIoT 连接到云端的企业来说，这可能是一个令人震惊的差距。

管理控制台的妥协很容易理解：利用云端的漏洞，您可以访问它所管理的所有账户和设备。然后，攻击者可以执行任何数量的利用，在从云端管理的设备上运行代码，这不仅可以完全控制一个终端设备，还可以进行横向网络移动，并有更多的有效载荷供其使用。同样，Team82 已经证明，有可能利用云端管理的 PLC 等设备的漏洞，并最终接管基于云的主机账户。

这些自上而下、自下而上类型的攻击是新出现的，并已被证明是有效的。它们通过将 PLC 等现场设备置于风险之中来威胁过程完整性，它们还威胁到数据完整性以及组织是否可以信任设备发送回云端数据上传。

监督融合 XIoT 环境的管理人员必须考虑一系列潜在的弱点以及如何远程或本地利用这些弱点。供应商和提供商等第三方合作伙伴的安全也必须得到妥善管理；一个能够访问敏感系统的受害供应商基本上将成为云端管理系统的一个后门。多租户主机也将成为基于云的 XIoT 系统的一大风险。从理论上讲，攻击者如果能够访问由服务供应商管理的主机系统，就能够将目标对准该主机上的任何一个虚拟实例，从而创造一个故障点。

这是 2022 年摆在 XIoT 运营商和所有者面前的风险管理方程式，他们必须权衡将 OT、IoT 和医疗设备管理放在云端的风险以及这样做将产生的商业和运营利益。

脆弱的供应链以及 SBOM 如何提供帮助

虽然 SolarWinds 在 2021 年初给技术所有者和运营商带来了冲击，但十二月披露的 Log4j 的关键漏洞表明了软件供应链是多么的脆弱，以及开源组件的可利用漏洞如何在瞬间将成千上万的公司和用户置于危险之中。

Log4j 是一个流行的开源 Apache 日志框架，包含一个很容易被利用的远程代码执行缺陷；Apache 软件基金会表示，有 2000 多家公司在使用 Log4j。使用 Log4j 的应用程序记录的恶意字符串会触发 JNDI（Java 命名和目录接口）查询，该查询将连接到攻击者控制的服务器并加载恶意的 Java 代码。

与许多其他供应商一样，自动化供应商使用 Log4j 作为跨 OT 域的组件，从而将许多工业流程置于风险之中。虽然 Log4j 很快得到了修补，但同样重要的是由此产生的关于软件供应链的讨论，以及确保在关键基础设施中安全使用开源组件。CISA 已经编制了一份受影响的供应商名单。

多年来，安全的软件开发一直是人们关注的焦点，然而，为开发人员提供安全性通常被视为满足最后期限和推动新应用程序和代码更新的障碍。

美国政府去年的一项行政命令在 2021 年下半年执行，特别要求加强软件供应链的安全。该命令明确指出，商业软件缺乏透明度和抵御攻击的能力，并要求增加控制措施，防止将可利用的漏洞引入代码。

除了确保审计信任关系，要求多因素认证、加密和事件监测外，该命令还坚持要求供应链供应商向组织提供软件物料清单 (SBOM)。SBOM 列出了用于构建和编译商业产品的软件组件——包括开源代码工具；它们类似于食品标签上的成分表。

很多时候，组织对备受欢迎的商业软件的组成部分视而不见，当 Log4j 等组件中的漏洞被披露时，安全团队会争先恐后地确定其暴露程度并确定补丁管理流程的优先级。然而，如果提供了 SBOM，用户不仅可以进行漏洞分析，还可以进行有助于评估产品风险的许可分析。机器可读的 SBOM 也很重要，它们可以整合到工具中，使工具能够被应用程序和系统查询。

预计在 2022 年，供应链安全将继续成为风险管理讨论的前沿和中心，而 SBOM 将成为这些讨论的一个重要组成部分。

全新勒索软件前沿

勒索软件和勒索攻击似乎从未消停过，当涉及到风险评估时，它们给资产所有者和运营商带来了很多思考。虽然 2021 年下半年没有发生极其重大的事件，但前六个月向威胁者证明，如果关键基础设施和 OT 资产采用易受攻击的 IT 技术，那么这些技术可能会影响关键流程和服务。

例如，Colonial Pipeline、JBS 和 NEW Cooperative 的事件在很大程度上是以盈利为目的的攻击，网络犯罪运营商已研究并了解了受害者支付高额赎金的意愿。在各案例中，攻击者都会索要数百万美元作为恢复系统的回报，Colonial 和 JBS 确实听从了攻击者的要求。

尤其是关键基础设施运营商，现在必须考虑勒索软件攻击是否可以掩盖更深层次的攻击。随着一月份俄罗斯和乌克兰之间的紧张局势加深，据报道，乌克兰的政府网站遭到了破坏性的恶意软件攻击。乌克兰的系统使用勒索软件作为一种误导策略，反而感染了 Wiper 恶意软件，导致受感染机器上的硬盘驱动器无法使用。这些类型的误导性攻击迫使防御者花费不必要的时间来处理他们认为是勒索软件的攻击，结果却发现这是一次影响更大的入侵。

在 2022 年，资产所有者和运营商应该意识到这类民族国家战术，以及活跃的冲突如何在网络上蔓延。随着冲突升级，用户应该拥有足够的威胁情报，以便及时了解用于针对其基础设施的策略、技术和程序。收紧防火墙规则、阻止网络邮件以应对网络钓鱼攻击、定期备份、离线和异地存储备份文件以及保护 OT 项目文件成为了地缘政治问题波及网络空间时要记住的关键策略。

关于 CLAROTY TEAM82

Claroty 的 Team82 是一个屡获殊荣的运营技术 (OT) 研究小组，以开发专有的 OT 相关威胁签名、OT 协议分析以及发现和披露工业控制系统 (ICS) 漏洞而闻名。Team82 致力于加强 OT 安全，并配有业界广泛使用的 ICS 测试实验室，与领先的工业自动化供应商密切合作，评估其产品的安全性。

迄今为止，Team82 已发现并披露了 **260** 多个 ICS 漏洞，其中 **110** 个在 2021 年下半年期间披露。

Team82 认识到了解 ICS 风险和漏洞形势，以及 Claroty 研究人员发现的漏洞如何适应这一情况的重要性，因此开发了一款自动收集和分析工具，从可信的开源获取 ICS 漏洞数据，包括国家漏洞数据库 (NVD)、工业控制系统网络应急响应小组 (ICS-CERT)、CERT@VDE、MITRE 以及工业自动化供应商施耐德电气和西门子。

该工具的成果揭示了与 ICS 漏洞有关的关键趋势和背景影响，它们对工业网络构成的风险，以及它们在不同供应商、产品、地域、时间段、关键性分数和影响等属性之间的变化。这些成果是本报告中研究和分析的基础。

第 1 部分：评估 CLAROTY 发现并在 2021 年下半年披露的 ICS 漏洞

Team82 在 2021 年下半年发现并披露了 110 个漏洞，使 Claroty 在 2021 年披露的漏洞数量达到 184 个。总体上看，Team82 已经披露了 260 多个影响 ICS 和 IoT 设备以及 OT 协议的漏洞。

Team82 在一些参数上优先考虑其工业控制系统研究，为 ICS 领域和安全社区提供最大的利益和贡献。Team82 与供应商和合作伙伴保持紧密沟通，并接受有关具体产品和版本的意见和要求。该团队的一些研究参数包括：

- 平台、设备或器材的通用性
- 攻击者在供应商修补之前发现并利用产品中的漏洞造成的潜在损害
- 有多少设备会受到漏洞影响
- Claroty 客户使用的产品

Team82 的研究考察了影响行业内众多部门的各种供应商和产品。由于这些参数，Claroty 还研究了第三方产品。Team82 在 2021 年下半年发现的 **110** 个漏洞影响到 16 家自动化和技术供应商。受影响的供应商和 ICS 产品类型细分如以下两张图表所示：

1.1 受影响的 ICS 供应商

受 Team82 在 2021 年下半年发现和披露的**110** 个漏洞影响的 **16** 家自动化和技术供应商的细分

供应商

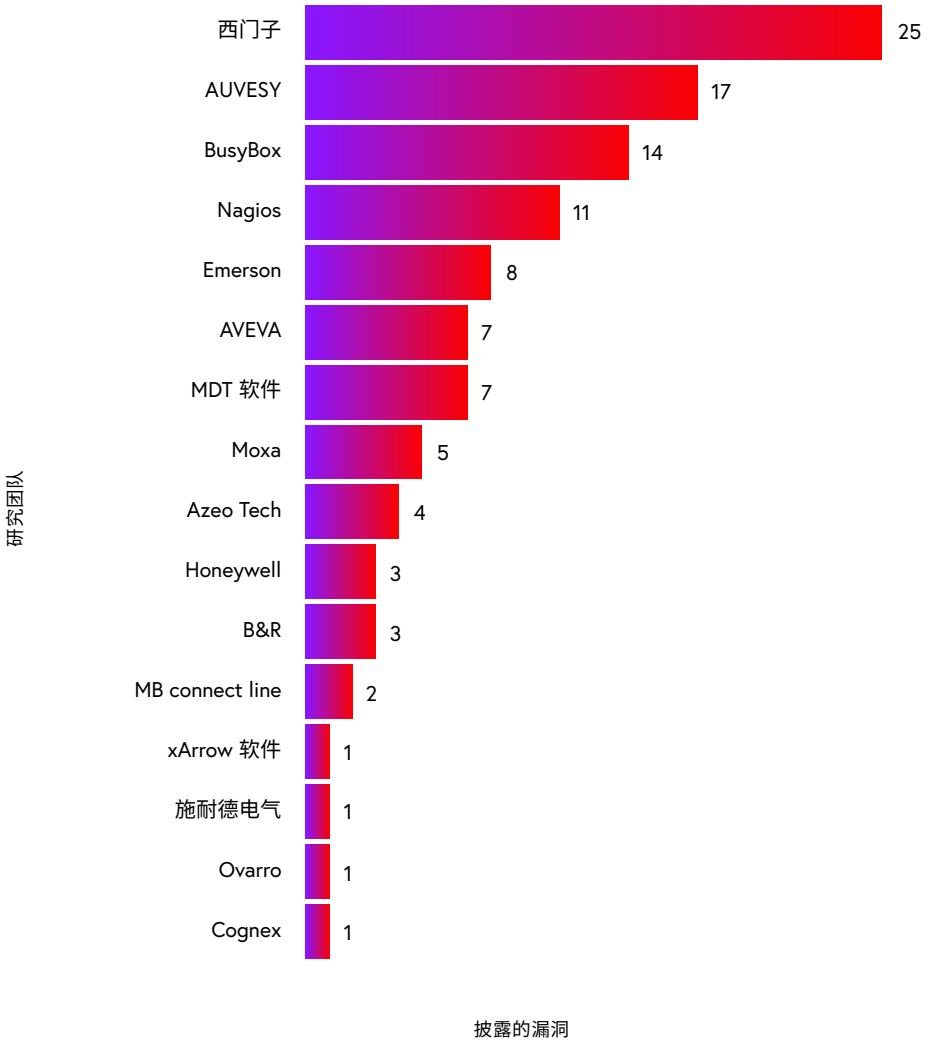


图 1.1：受 Team82 披露影响的供应商细分。

1.2 受影响的 ICS 产品类型

Team82 披露的漏洞基本上都是在普渡模型的第 3 级：运营管理上发现的。

目标产品系列

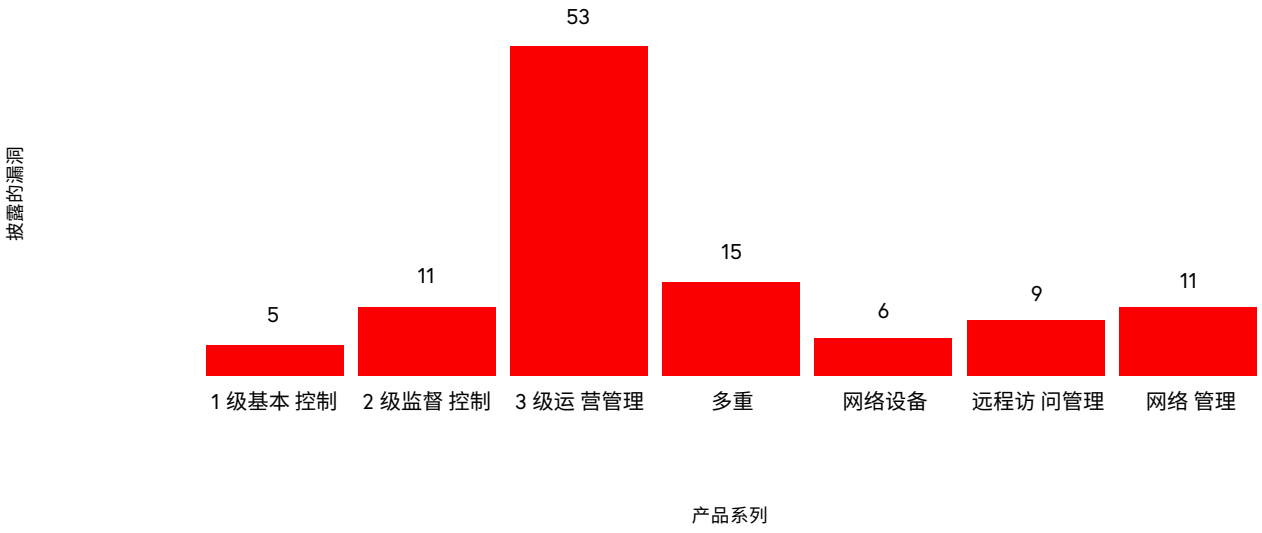


图 1.2：按产品系列类型划分的 Team82 发现的漏洞细分。

第 2 部分：对 2021 年下半年披露的所有 ICS 漏洞的评估

本节对 2021 年下半年发布的所有工业控制系统漏洞进行了统计分析和背景评估。

下面的数据包括 Team82 发现和披露的漏洞，以及其他研究人员、供应商和第三方在 2021 年下半年公开披露的所有其他漏洞。

2.1 ICS 漏洞的总数

在 2021 年下半年，共计发布了 797 个 ICS 漏洞，这些漏洞影响了 82 个 ICS 供应商。

发布的漏洞

797

已识别漏洞的总数

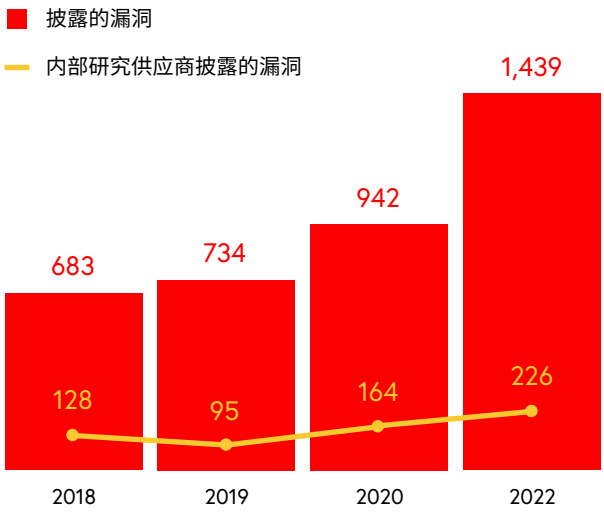
受影响的供应商

82

受影响供应商的总数

2.2 ICS 漏洞的年度比较

在过去四年中，漏洞披露的数量显著增加，表明人们认识的提高以及转向 OT 领域的安全研究人员数量的增加。



+110% **增加**
披露的漏洞

+76% **增加**
供应商开展的内部研究披露的漏洞数量

图 2.2a：每年披露的漏洞细分。

2.3 漏洞发现的起源，2021 年下半年

在 2021 年下半年，80% 披露的漏洞是由受影响供应商的外部来源发现的。外部来源包括一些研究机构、第三方公司、独立研究人员和学术界人士等。

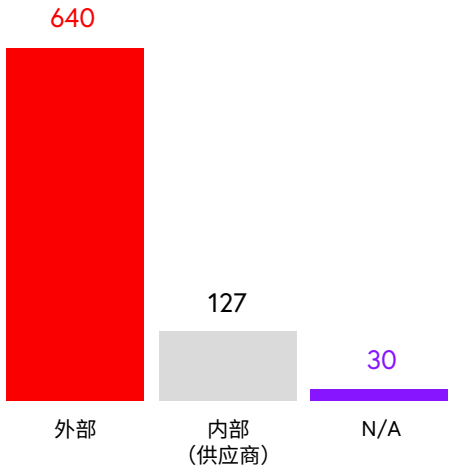
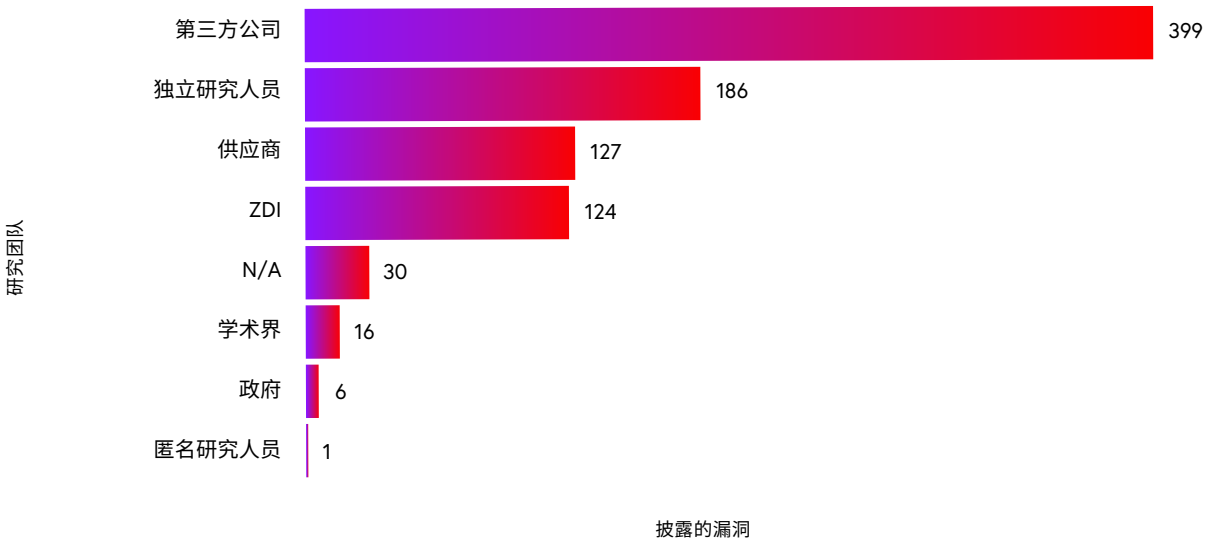


图 2.3a：按发现来源划分的漏洞细分。

下图细分了由第三方公司主导的外部来源披露的漏洞数量。在 2021 年下半年，这些来源发现了 **399** 个漏洞**(50%)**。这些披露的漏洞中有许多是由网络安全公司的研究人员发现的，这表明重点已经转移到将工业控制系统与 IT 和 IoT 安全研究并列。值得一提的是，有些披露是多个研究小组之间的合作，或者在其他情况下，不同的研究人员分别发现和披露同一个漏洞（在 2021 年下半年，这种情况的漏洞数量为 **92** 个）。



Team82 还指出，在 2021 年下半年，有 **55** 名新的研究人员报告了漏洞；下图中的数据按类型划分了这些新成员。

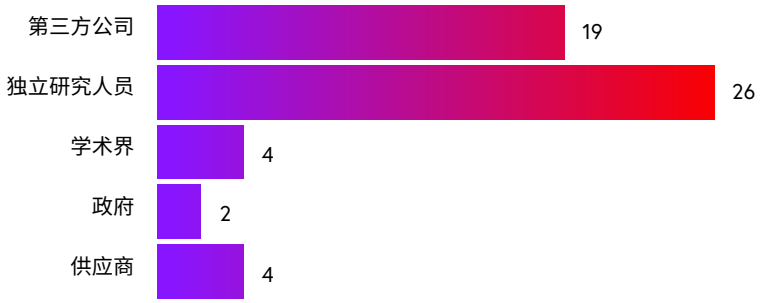


图 2.3c：报告 ICS 漏洞的新研究人员细分。

Team82 的数据表明，新的研究人员主要集中于市场领先的供应商，如西门子、施耐德电气和其他公司。其中 6 名新研究人员在 2021 年下半年介绍了 5 家新的受影响供应商。其余研究人员检查了以前受影响的供应商。应该注意的是，ICS 和 SCADA 设备和软件可能很难获得，而且价格昂贵，特别是对于新近活跃的研究人员来说。这也可能是关注市场领先的供应商的一个影响因素，他们的产品更容易获得。

2.4 受影响的 ICS 供应商

Team82 在我们的四份半年度报告中汇编了趋势数据，报告显示 2021 年受漏洞影响的供应商数量有所增加。

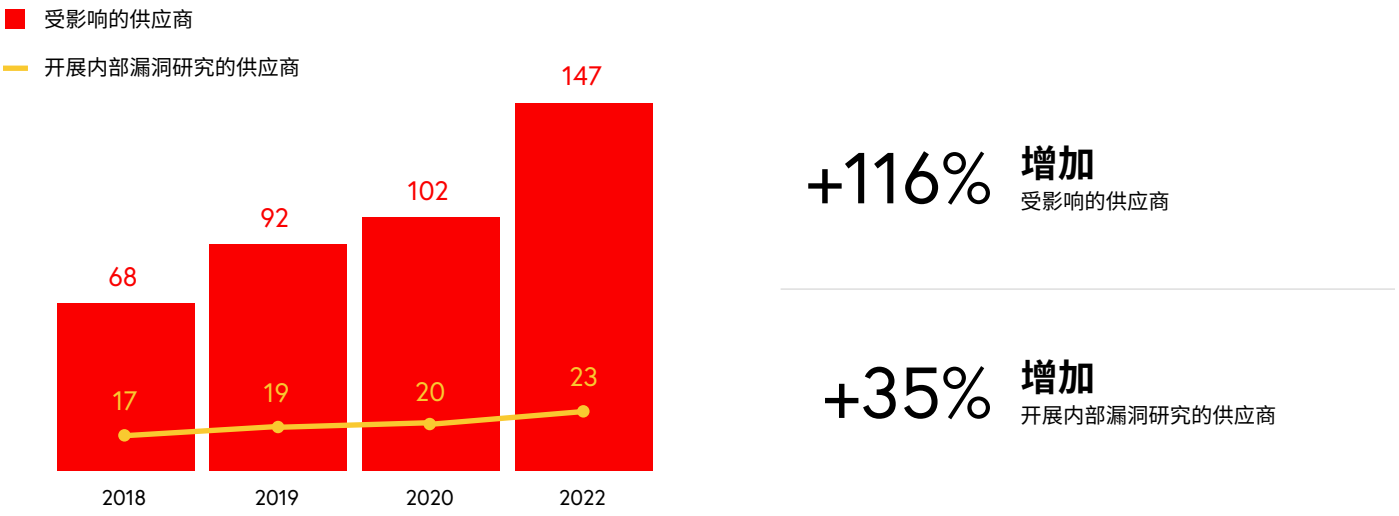


图 2.4a：每年受影响的供应商细分。

虽然 2021 年受漏洞影响的供应商数量发生显著增长，但了解这些数字背后的一些因素很重要。OT 和 ICS 内部的漏洞研究仍然是一门成熟的学科，Team82 的数据集还显示，开展内部漏洞和披露漏洞的供应商数量呈上升趋势。

大型供应商，如西门子公司、施耐德电气和 Rockwell Automation，都有成熟、完备的产品安全团队，其任务是向客户提供安全产品。Team82 与这些行业领先的自动化供应商以及许多其他正在制定和培养自己的内部安全和响应团队的供应商建立了研究合作伙伴关系。最终的结果是形成了一个基本上更安全的生态系统。

对于任何一家供应商来说，大量披露漏洞并非反映了其审查产品安全问题的能力。事实上，这些受影响的供应商为产品安全分配充足的专用资源并可能发现更多漏洞的情况可能正好相反。每个供应商的年龄、目录和安装基础也往往影响到影响产品的已披露漏洞的数量。

在目前的 Team82 数据集中，西门子是所有受影响供应商中报告漏洞最多的，达到 **251** 个，其中许多是作为西门子 CERT 团队开展的内部研究的一部分披露的），其次分别是施耐德电气、研华、台达电子和三菱。

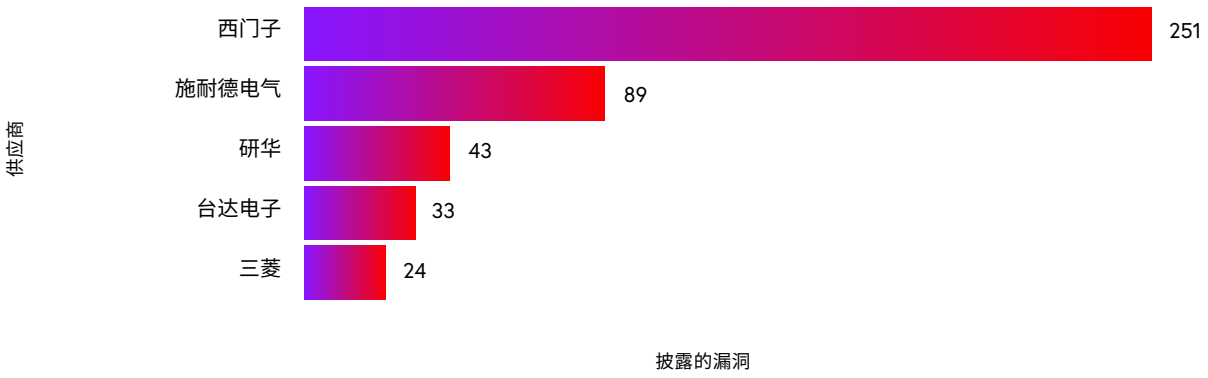


图 2.4a：每年受影响的供应商细分。

2.5 2021 年下半年首次披露漏洞的供应商

在 2021 年下半年期间，21 家产品之前未受到 ICS 漏洞影响的供应商受到至少一个 2021 年下半年披露的 ICS 漏洞的影响。

8 家此类供应商属于自动化行业，**4** 家属于医疗保健行业，另有 **4** 家属于制造业。

供应商	主要行业
AzeoTech	自动化
AUVESY	自动化
xArrow 软件	自动化
mySCADA	自动化
MDT 软件	自动化
Bachmann Electronic	自动化（可再生能源）
Cognex	自动化，制造业（机器视觉）
FANUC	自动化，制造业（机器人）
波士顿科学	医疗（医疗器材和设备）
瑞仕格医疗	医疗（药品供应链）
Fresenius Kabi	医疗（药品、生物技术）

供应商（续）	主要行业
Ypsomed	医疗（药品、生物技术）
Helmholz	工业通信
InHand Networks	工业 IoT
Annke	IoT（家庭和企业安全）
HCC Embedded	IoT（安全）
BusyBox	IT 技术
Nagios	IT 技术
Uffizio	IT 技术（GPS 追踪）
Trane	制造业
Xylem Inc.	制造业（水处理技术）

2.6 受影响的 ICS 产品

固件/软件

对于每个披露的漏洞，我们将易受攻击的组件标记为固件或软件。在有些情况下，一个漏洞会影响到几个组件，而这些组件则是固件和软件的组合。在 2021 年下半年，大多数漏洞都会影响到软件组件，鉴于软件的修补比固件更容易，防御者有能力在其环境中优先进行修补。

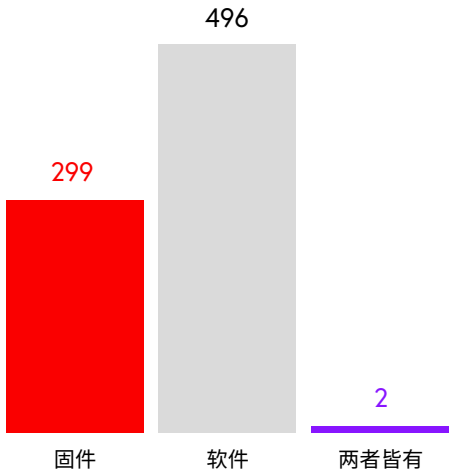


图 2.5a：软件和固件中所发现的漏洞细分。

产品系列类别

在研究产品系列内的固件和软件漏洞时，有一个更有趣的划分。重要的是要明白，虽然漏洞是在一个可以被归类为固件或软件的组件内发现的，但我们需要考虑到受其影响的产品。例如，可能有一个运行在 HMI 上的易受攻击的软件配置，或者可能有一个连接到泵的以太网模块。下图展示了受这些漏洞影响的产品系列，类别如下所示：

受影响的产品系列

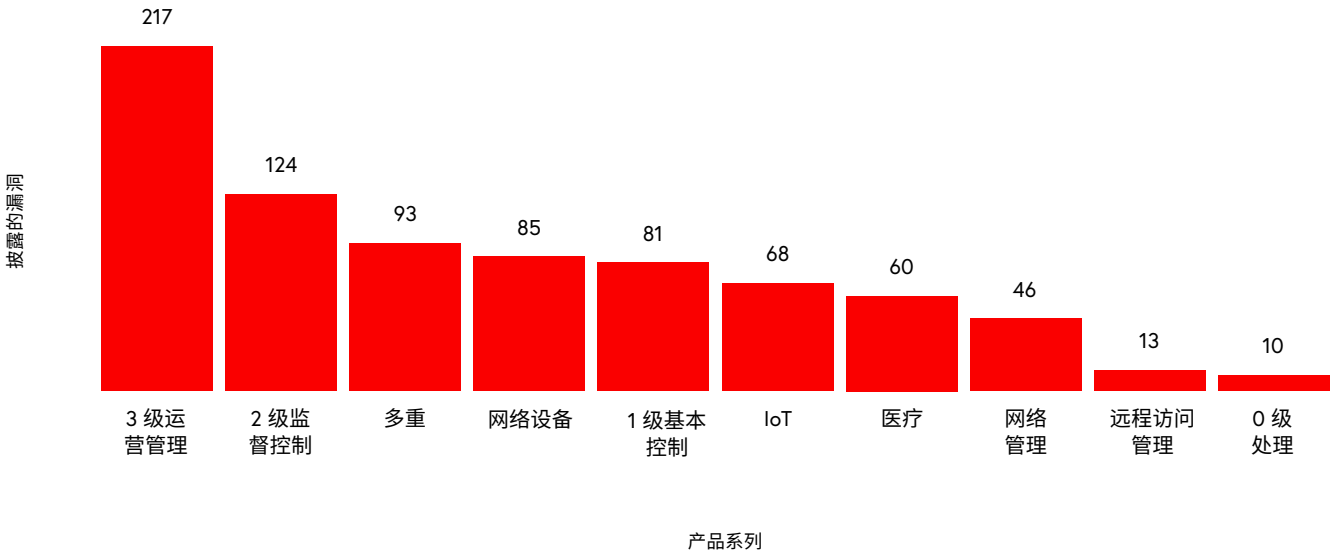


图 2.5b：受影响产品系列的细分。

由于 **27%** 的漏洞影响到普渡模型的运营管理级别（第 3 级），这解释了为什么我们看到许多漏洞影响软件组件。此外，发现的漏洞中有大约 **25%** 影响到普渡模型的基本控制（第 1 级）和监督控制（第 2 级）级别。当然，当影响到这些级别时，攻击者也可以达到更低的级别，并影响到进程本身，使其成为有吸引力的目标。

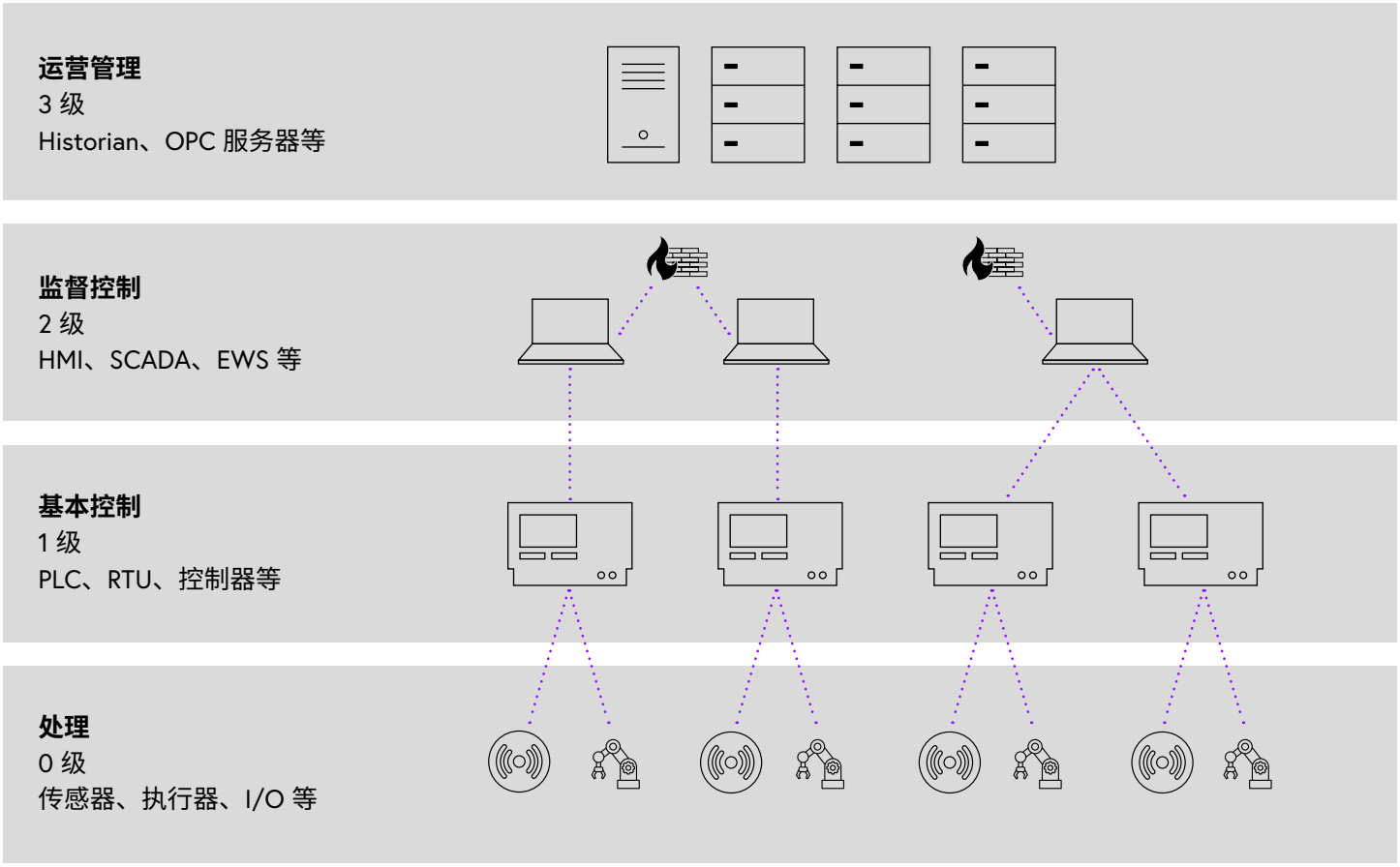


图 2.5c：工业控制系统的普渡模型。

我们要注意的是 “多重” 类别——该类别主要包含第三方组件漏洞，这些漏洞通常在每次披露中包含多个漏洞。它们通常会影响整个行业的许多供应商和产品。它强调，从可见性和风险评估开始，针对第三方漏洞采取保护和缓解措施是 OT 网络安全不可分割的一部分。

在查看每个类别时，您可以将影响它们的易受攻击的组件划分为固件、软件或两者皆有。大多数运营管理（第 3 级）和监督控制（第 2 级）漏洞都是基于软件的，而基本控制（第 1 级）漏洞大部分是基于固件的。由于无法随着时间的推移进行修补，尤其是在 1 级设备固件中，我们建议投资于分割、远程访问保护和监督控制级别的保护，因为它与基本控制级别相关联。

产品系列中的固件/软件划分

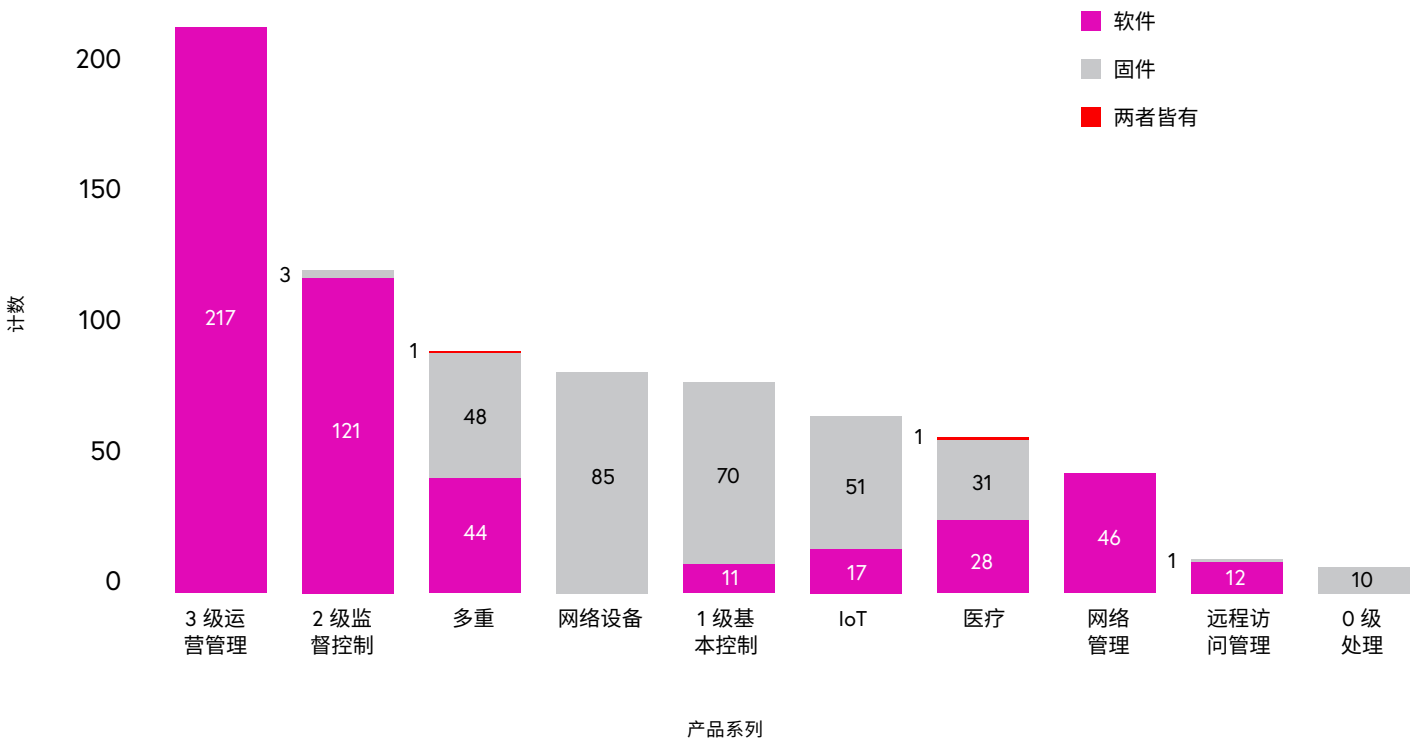


图 2.5d：按产品系列划分的固件和软件漏洞细分。

第 3 部分：缓解措施和修补措施

3.1 缓解措施

鉴于我们所述的关于软件和固件补丁的挑战，缓解措施往往是面向防御者开放的唯一修补方案。不过，尽管防御者依赖缓解措施，但来自行业组织（如 ICS-CERT）的供应商建议或提醒有时无法提供深度防御建议。

可行的建议很重要，如阻止特定的端口或更新过时的协议，但应该注意的是，在这些建议生效之前，必须做出基础性的实践。

Team82 围绕最重要的缓解措施的数据证实了这一点，如下所示。例如，网络分割是最重要的一步，应该是防御者先于我们列表上的其他选项考虑的优先事项，包括勒索软件意识（网络钓鱼缓解措施）、流量限制、基于用户和角色的政策，以及最小特权原则。

最重要的缓解措施

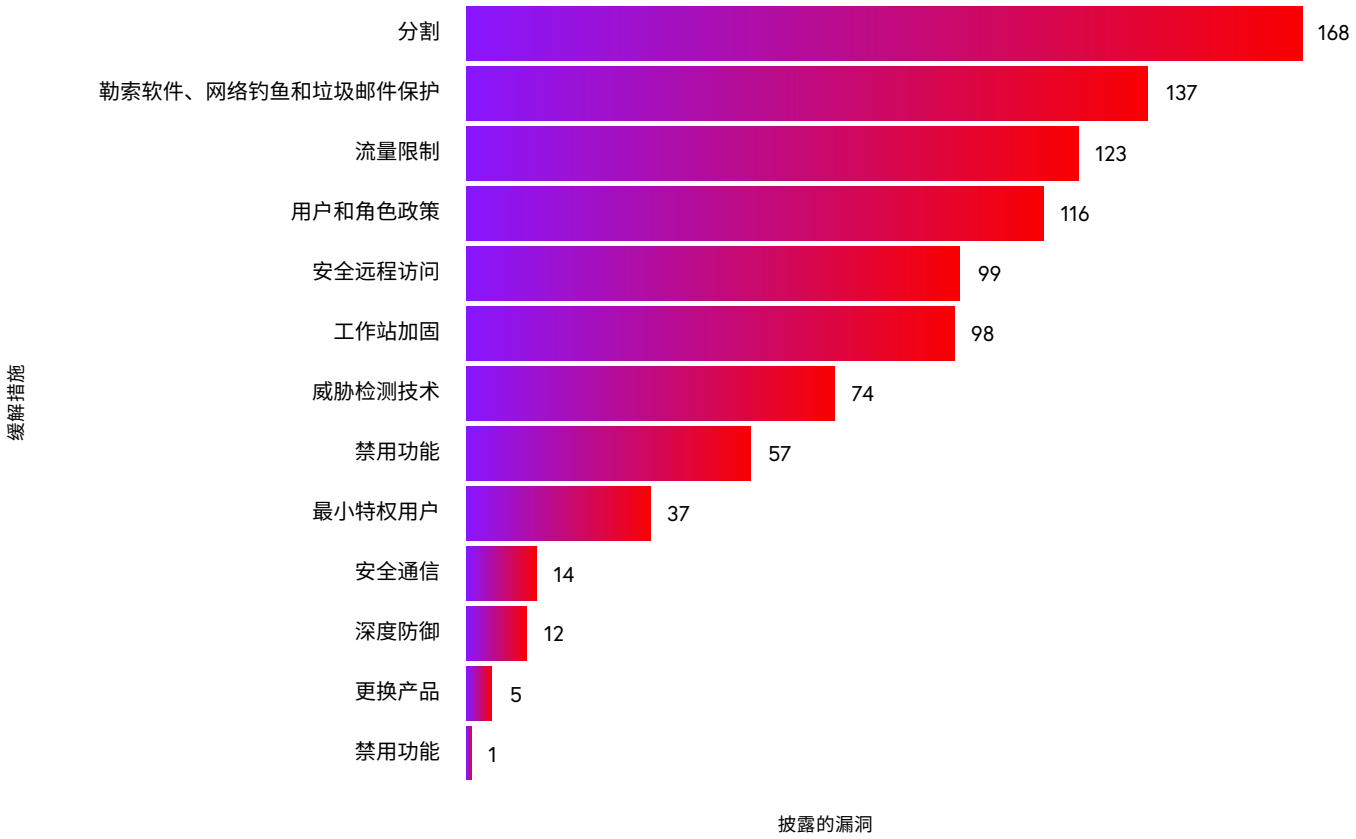


图 3.1a：最重要的缓解措施细分。

随着企业将数据、应用程序、基础设施和服务转移到云端，气隙系统已成为历史，边界逐渐模糊，网络分割成为一项重要的控制措施。这可能涉及虚拟分区，该分区允许针对工程和其他面向过程的功能量身定制的特定于区域的策略。探查流量和 OT 特定协议的能力对于防御异常行为也至关重要。

勒索软件、网络钓鱼和垃圾邮件保护紧随分割之后，成为重要的缓解措施。必须考虑到针对 IT 系统的勒索软件攻击，如对 NEW Cooperative、Colonial Pipeline 和 JBS Foods 的攻击，因为它们可以跨越到管理 OT 的系统，或迫使关键流程和服务关闭。与主系统分开维护和存储备份将在需要时启用数据恢复并帮助恢复运行。最后，提高员工对社会工程和网络钓鱼技术的认识至关重要，正如我们前面所提到，许多通过本地攻击向量利用的漏洞都依赖于用户互动。

3.2 修补措施

漏洞修补有三种形式：全面修补，即修复所有受影响的产品；部分修补，即并非修复所有受影响的产品；以及没有任何修补。

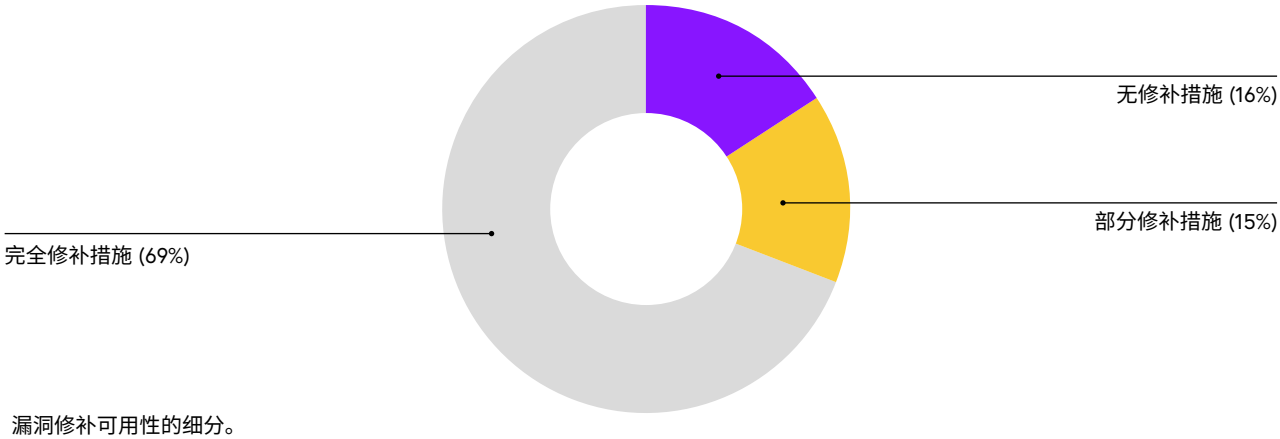
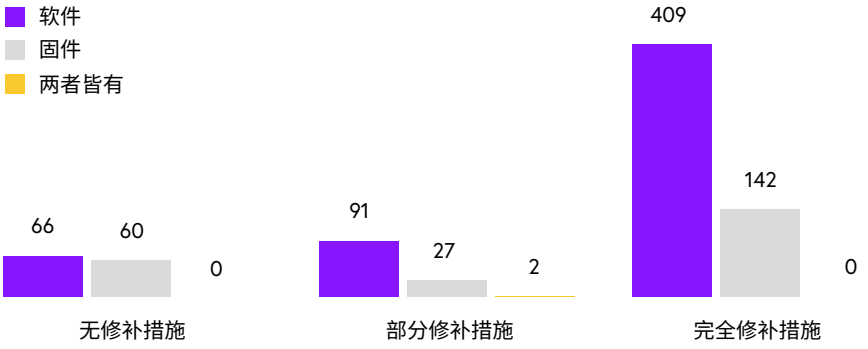


图 3.2a：漏洞修补可用性的细分。

按软件和固件细分漏洞修补，可以帮助安全从业人员创建战略性的修补和缓解计划。

按固件/软件划分的修补



74% **的完全修补漏洞**均基于软件。强调鉴于软件的修补比固件更容易，防御者有能力在其环境中优先进行修补。

62% **的部分修补或无修补漏洞**在被利用时可能导致远程代码执行或拒绝服务

图 3.2b：按固件/软件划分的漏洞修复可用性细分。

调查发生软件修复（部分或全部）的产品时发现，它们大多数处于第 3 级：运营管理，然后是第 2 级：监督控制和网络管理。

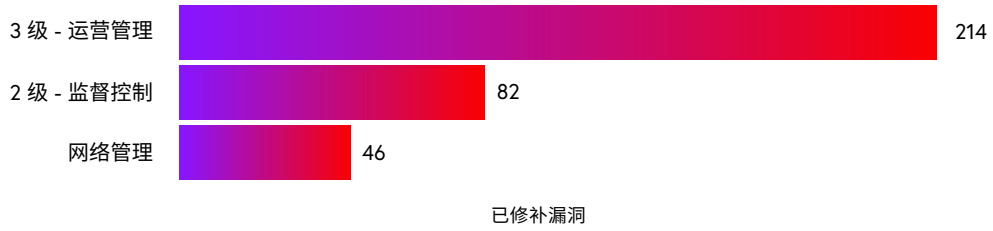


图 3.2c：按产品系列划分的前三大软件修补措施的可用性细分。

至于固件，似乎除了随着时间的推移无法更新之外，还存在可用修补解决方案较少的问题。当存在固件修补措施时（部分或全部），Team82 的数据显示其主要是针对网络设备，其次是基本控制（第 1 级）和 IoT。这表明，即使在固件中，也可能发生一些更新的优先级，因为更新网络设备，例如交换机，比升级 PLC 或 RTU 更容易，也更有可能。

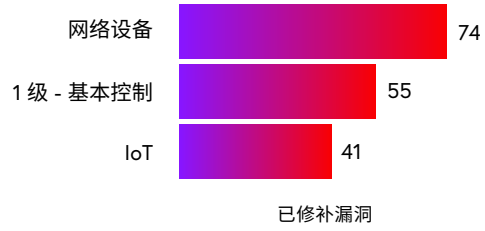


图 3.2d：按产品系列划分的前三大固件修补措施的可用性。

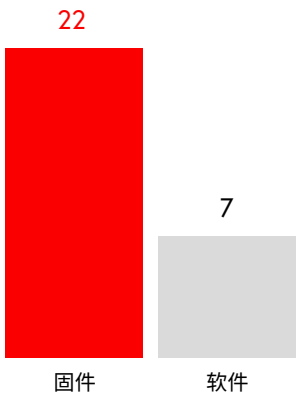
3.3 报废产品

29 个漏洞影响到报废产品，由于供应商不再支持这些产品，因此没有计划进行修补。

59% **影响报废的漏洞**可通过网络攻击向量远程利用

48% **影响报废的漏洞**处于 1 级——基本控制设备上，如：PLC、RTU 等

59% **影响报废的漏洞**被成功利用时，可能导致代码执行或拒绝服务



其他受影响的报废产品包括监督控制设备（第 2 级），其次是医疗和网络设备。

提及报废产品时，唯一的解决方案是缓解（在可能的情况下），直到更换。软件更新和修补比固件更新更容易；固件更新可能需要几个月或几年的时间来开发和分布。这一点以及修补方案较少的事实使人们认识到，防御者仍需主要依赖于缓解措施。

供应商和 CISO 必须追踪这种类型的技术负债。不受支持的产品中的漏洞与 ICS 产品的长保质期相冲突，并且可能会迅速累积。可能在更新具有挑战性的环境中运行的受支持产品也是如此，尤其是在停机时间不可接受的情况下。未修补的远程代码执行和拒绝服务缺陷会加大风险，通常会达到不可接受的程度。

第 4 部分：CVSS 信息

通用漏洞评分系统 (CVSS) 的基础指标组代表了一个漏洞在不同时间和用户环境下的恒定特征，包括两组指标：可利用性和影响。

4.1 可利用性指标

这些指标代表了漏洞可以被利用的技术手段和难度。

正如您在下图中所看到的，**63%** 的漏洞是通过网络攻击向量被利用的，并且是可以远程利用的。这强调了保护远程访问连接和面向互联网的 XIoT 设备的重要性。

至于具有本地攻击向量的漏洞：在其中 **31%** 的漏洞中，攻击者依靠用户互动来执行利用这些漏洞所需的操作。这包括社会工程技术，如网络钓鱼和垃圾邮件。对它们的认识和预防至关重要。事实上，利用此类技术的攻击正在增加，员工应遵守建议部分中详述的安全措施。

攻击向量分布

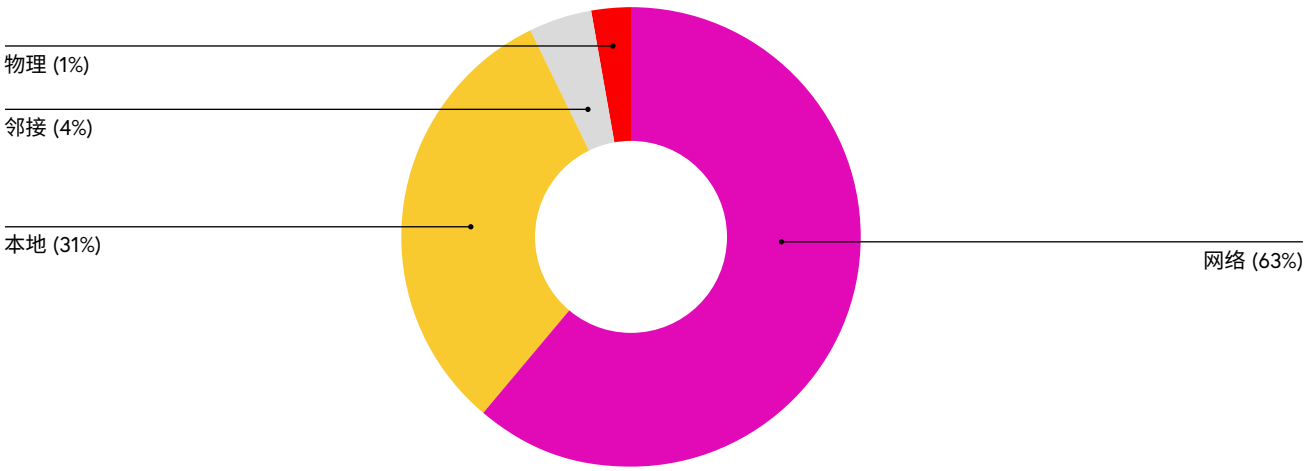


图 4.1a：与 ICS 漏洞有关的攻击向量

按产品系列划分的攻击向量

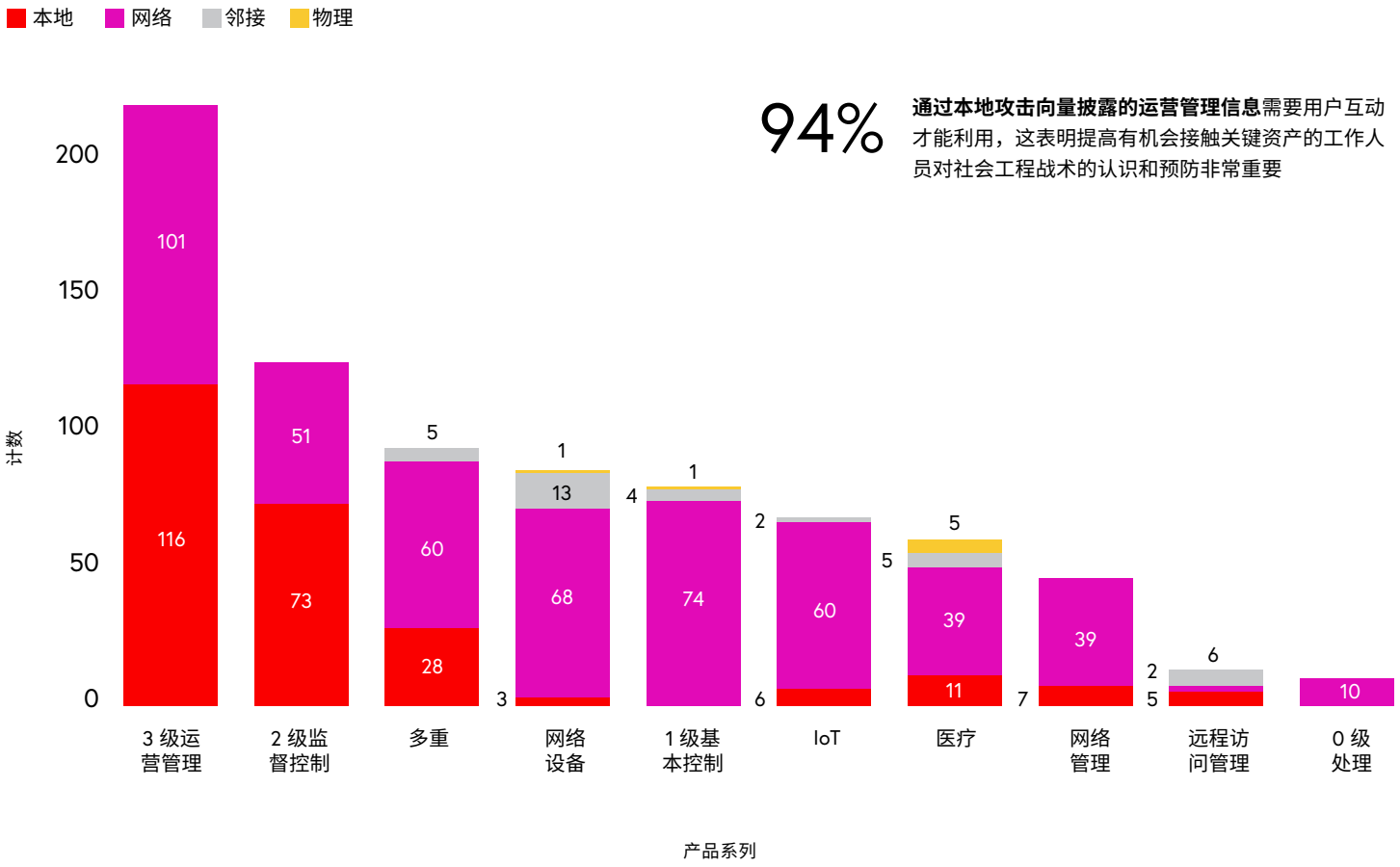
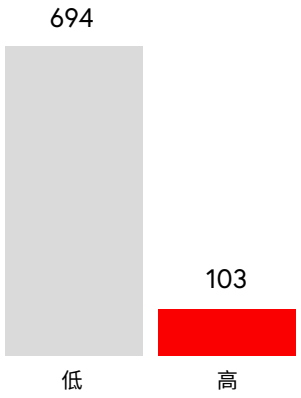


图 4.1b：按产品系列划分的攻击向量。

攻击的复杂度

该指标表示攻击者无法控制的条件，必须存在这些条件他们才能够利用该漏洞。例如，成功的攻击可能取决于攻击者收集的关于配置设置的知识。



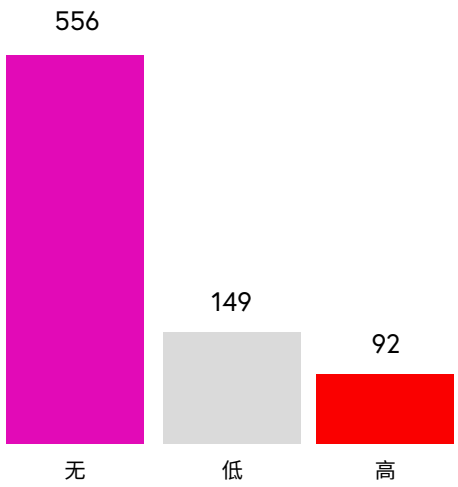
87% **的漏洞复杂度较低**，这意味着这些漏洞不需要特殊条件，攻击者每次都能取得成功。

图 4.1c：根据 CVSS 评分划分的攻击复杂度。

4.2 所需特权

该指标代表攻击者在成功利用该漏洞之前必须拥有的特权水平。

所需 CVSS 特权



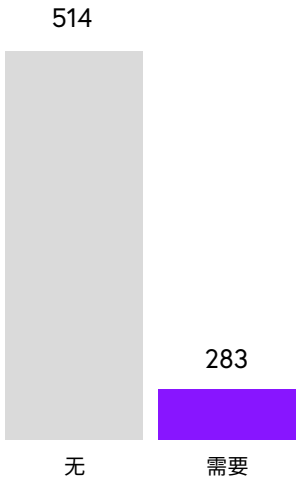
70% **的漏洞复杂度较低**，这意味着这些漏洞不需要特殊条件，攻击者每次都能取得成功。

图 4.2a：利用漏洞所需的权限。

用户互动

该指标表示攻击者为了利用漏洞，对独立用户或用户所发起进程的参与的依赖性。

CVSS 用户互动



64% **的漏洞不需要用户互动**，这意味着攻击者不需要依赖于参与独立用户或用户所发起的进程来利用该漏洞。

图 4.2b：利用漏洞所需的用户互动。

4.3 影响指标

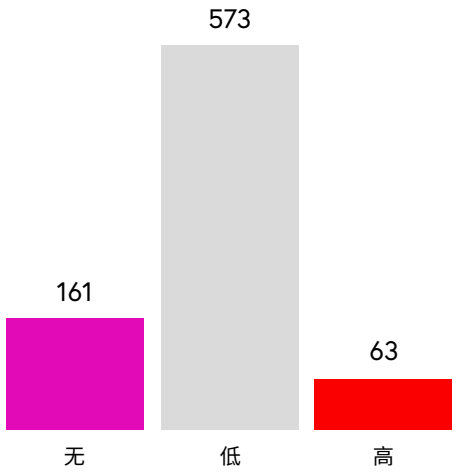
这些指标代表了成功利用每个漏洞的直接后果。CVSS 系统根据 CIA 三要素（保密性、完整性和可用性）来衡量影响。虽然在技术上与任何类型的网络都有关，但 CIA 三要素并不包括通常来说 OT 网络两个最重要的风险变量：可靠性和安全性。

这意味着 CVSS 并没有完全考虑到 ICS 漏洞的潜在影响，这些漏洞可以被用来造成实际伤害。在以下章节中，您可以了解到保密性和完整性作为风险变量在 OT 网络中的相关性较小。因此，ICS 防御者需要进一步评估漏洞的严重性，而不仅仅是其 CVSS 分数。

保密性

该指标表示由于成功利用漏洞而对信息资源的保密性产生的影响。

CVSS 保密性



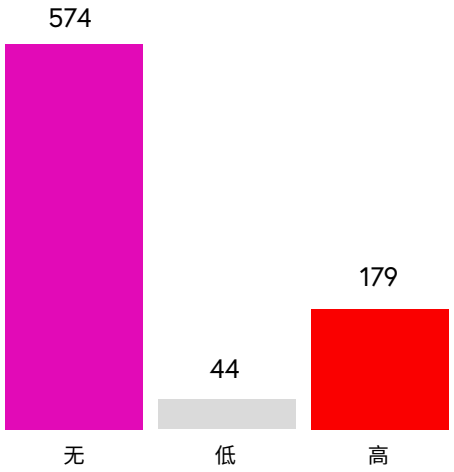
92% **的漏洞对保密性的影响很低或没有影响**注意，虽然保密性在 IT 安全中很重要，但在 OT 网络中，这一风险变量并不那么重要。

图 4.3a：对保密性的影响。

完整性

该指标表示由于成功利用漏洞而对信息完整性产生的影响。

CVSS 完整性



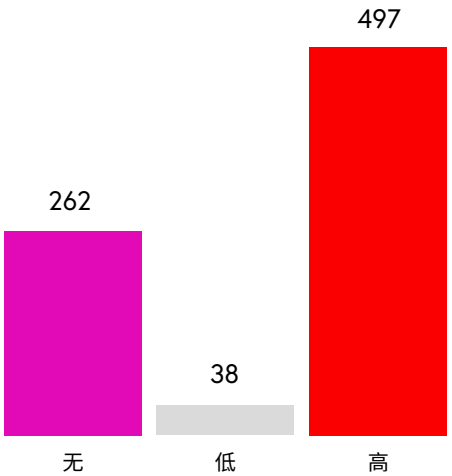
72% **的漏洞对完整性毫无影响**这表明虽然信息的完整性在 IT 安全中很重要，但在 OT 网络中它是一个较小的风险变量。

图 4.3b：对完整性的影响。

可用性

该指标表示由于成功利用漏洞而对受影响组件的可用性产生的影响。

CVSS 可用性



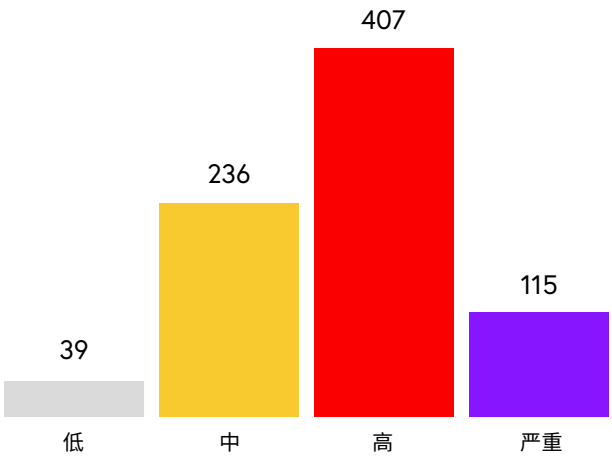
62% **的漏洞对可用性的影响较高**这意味着完全失去了可用性，导致拒绝访问资源。或者，可用性部分丧失，但也很重要——例如，拒绝创建新连接的能力。

图 4.3c：对可用性的影响。

4.5 CVSS 分数

上面提到的所有指标都经过测量并计算成最终的 CVSS 分数，该分数代表了漏洞的严重程度。分数范围划分为四类：低、中、高和严重。

CVSS 类别划分



65% **的漏洞被归类为“高”或“严重”类别**这反映了 ICS 安全研究人员的广泛趋势，即专注于识别具有最大潜在影响的漏洞，以最大限度降低危害

图 4.5a：按严重性划分的 CVSS 分数细分。

CVSS 的类别划分也与之前的发现相一致，即大多数漏洞并不复杂，无需权限，也不依赖于用户互动，并且可能会导致完全丧失可用性。

第 5 部分：已利用的 CWE

Team82 的数据集中排名前五的最普遍常见弱点和枚举 (CWE) 在 MITRE 公司 2021 年 CWE 25 大最危险软件错误名单中也名列前茅。这些漏洞相对容易被利用，可导致对手遭受严重破坏。

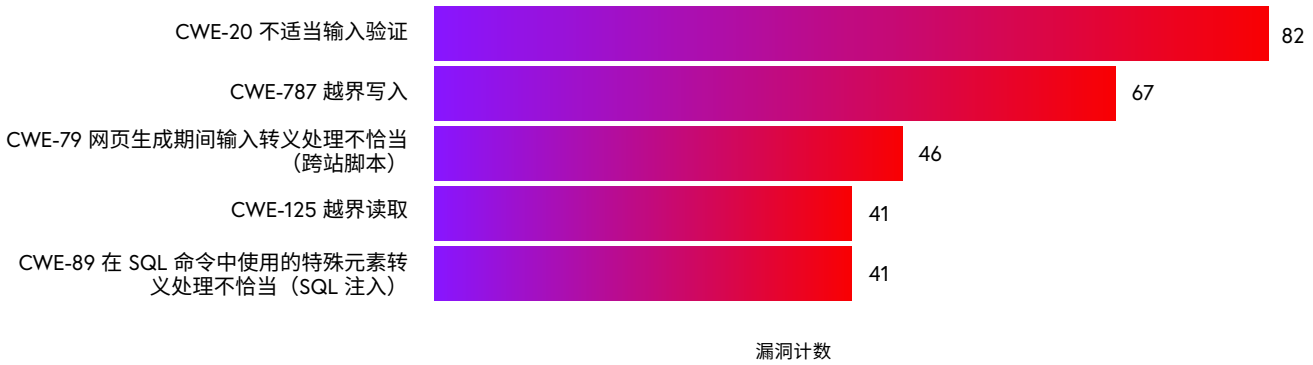


图 5a：前五大最普遍的 CWE 细分。

CWE 是一个软件漏洞的分类系统，是确定 CVSS 分数严重程度的基础，也是为了进一步强调锁定软件开发实践和早期实施安全措施的必要性。

长期以来，我们一直提醒要注意简单的编码错误，如输入验证、与缓冲区有关的内存漏洞和 SQL 注入。然而，这些仍然困扰着软件开发，这也反映在 Team82 的数据集中。好消息是，所有这些 CWE 的占比——除 CWE-20——已证明 2021 年下半年发生的漏洞比去年上半年少。不适当输入验证漏洞是异常值，出现在 10% 的漏洞中，高于 2021 年上半年的 4%。

CWE-787 和 CWE-125，越界读取和越界写入漏洞分别在 MITRE 的"25 大"名单中排名第 1 和第 3。它们造成了一系列后果，从数据损坏和代码执行，到拒绝服务攻击。

CWE-79 和 CWE-20 是输入和转义处理漏洞，在 MITRE 名单中分别排名第 2 和第 4。两者都允许攻击者改变控制流、修改内存、读取应用程序数据、绕过保护机制、执行代码，或使设备和进程崩溃。

CWE-89 在 MITRE 名单中排名第 6。它是指未能转义处理可用于修改 SQL 命令的特殊元素，并导致攻击者能够读取和修改应用数据并绕过保护机制。

基于 CWE 的 ICS 漏洞的潜在影响

下图说明了 2021 年下半年发布的基于 CWE 的 ICS 漏洞的普遍潜在影响，反映了远程代码执行作为 OT 安全研究界主要关注领域的突出地位。

在远程代码执行的背后是清晰的第二层潜在影响：导致拒绝服务的情况发生、绕过保护机制，并允许对手读取应用数据和修改内存。

按影响程度划分的漏洞数量前 10 名

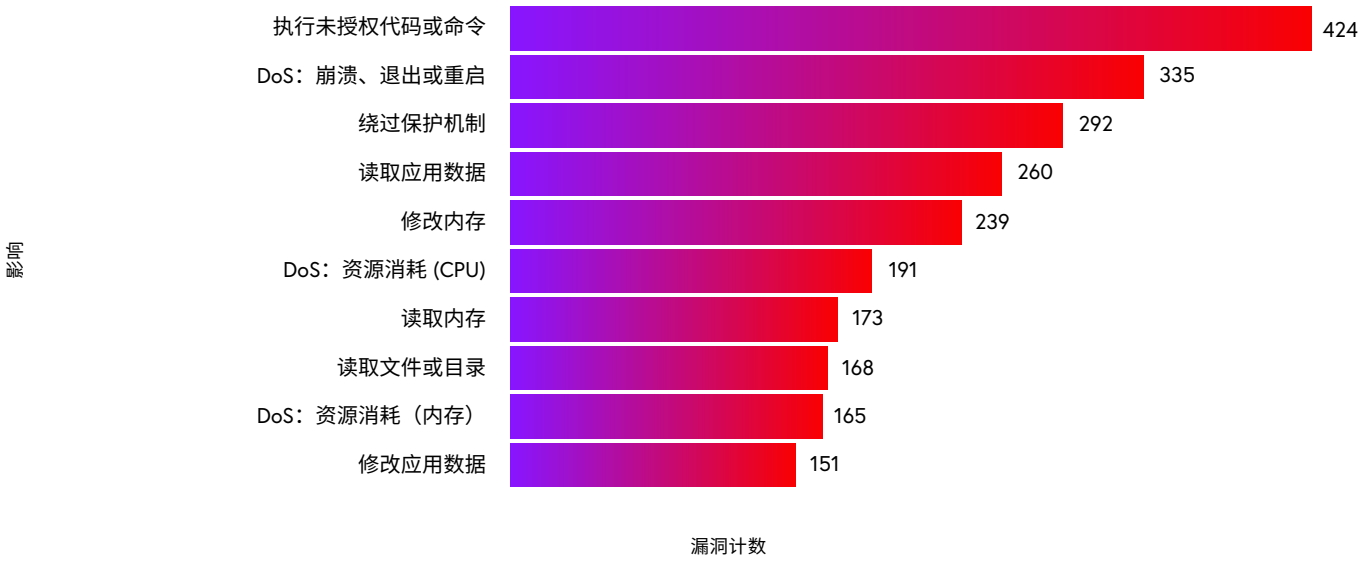


图 5a：按 CWE 影响划分的漏洞数量细分。

在针对基本控制设备（第 1 级）的披露中，我们发现：

53% 可能导致代码执行

51% 可能导致拒绝服务

图 5b：对 1 级——基本控制设备的影响。

安全研究人员和攻击者都对 PLC 和 RTU 等设备的远程代码执行漏洞垂涎三尺。保护这些难以打补丁或更新的设备免受基于网络的攻击（这些漏洞中有 91% 可被远程利用）需要第三方安全保护。

第 6 部分：与 2021 年下半年 ICS 风险和漏洞形势相关的关键事件

据 Team82 评估，在 2021 年下半年期间，以下事件和趋势可能在一定程度上促成了 ICS 风险和漏洞形势。

TARDIGRADE 生物制造业恶意软件攻击

据生物经济信息共享和分析中心 (BIO-ISAC) 称，绰号为 Tardigrade 的多态恶意软件攻击在生物制造公司中广泛传播。这些攻击的目的旨在窃取知识产权和私人研究。

Tardigrade 的代码根据其环境而改变，以避免被发现。它有别于其他多态恶意软件，因为它能够从内存中重新编译其加载程序，并且不留下签名，使其探测更加复杂。

该恶意软件可通过许多向量传递，包括钓鱼邮件，并使用被称为 SmokeLoader 或 Dofoil 的恶意软件加载程序，将模块注入被攻击的机器。它还创建了一个后门连接，允许从攻击者的服务器上下载文件和命令，部署额外的攻击模块，并在网络上保持隐蔽。

由于专利研究，生物制造公司一直吸引着间谍活动的注意，甚至自 COVID-19 开始以来更是如此，因为该领域正在持续研发疫苗和治疗方案。因此，该行业的安全从业人员应保持警惕。

如需有关 Tardigrade 生物制造业恶意软件攻击的更多信息，请参考：
https://claroty.com/2021/11/24/blog-research-what-you-should-know-about-the-tardigrade-biomanufacturing-malware-attacks/

LOG4J 漏洞

在广受欢迎的基于 Java 的开源 Apache 日志框架 Log4J 中发现了一个零日漏洞。该漏洞 (CVE-2021-44228) 被称为 Log4Shell，远程未认证的攻击者可以使用特制的字符串在受影响的应用程序和服务上执行代码，从而滥用该漏洞。根据 CISA 编制的名单，目前已有超过 100 家已知的受影响供应商，其中超过 20 家为 ICS 供应商。

随着补丁和更新的出现，更多的漏洞被发现，使得以前的修复措施在某些非默认的情况下不再完整。次级漏洞可能导致

DoS 条件、信息泄露和代码执行，因为攻击者可以利用 JNDI 查询模式制作恶意输入数据。

这些漏洞影响了工业供应商，因为日志工具被用于许多部署在 OT 网络中的应用程序，导致许多供应商发布补丁、缓解措施或受影响产品的清单。

如需有关 Log4J 漏洞的更多信息，请参考：
https://claroty.com/2021/12/14/blog-research-what-you-need-to-know-about-the-log4j-zero-day-vulnerability/

NEW COOPERATIVE 勒索软件攻击

九月，NEW Cooperative，一个在爱荷华州有 60 个经营点的农民合作社，在遭受勒索软件攻击后关闭了其业务。据称，这次攻击是由负责 Colonial Pipeline 攻击的勒索软件即服务运营商 DarkSide 的一个分支 BlackMatter 执行的。据报道，BlackMatter 要求支付 590 万美元的赎金，并威胁称，如果五天内不支付，赎金将翻倍。此外，据称 BlackMatter 从 NEW Cooperative 窃取了 1000GB 的数据，并威胁要将其泄露出去。

在与 BlackMatter 的聊天会话中，NEW Cooperative 表示，40% 的粮食生产都在其软件上运行，1100 万只动物的喂养计划也依赖它们，这意味着停产可能会迅速摧毁粮食供应链。

NEW Cooperative 表示，他们主动关闭系统以控制攻击，这与今年早些时候 Colonial Pipeline 和 JBS 食品公司在破坏性的勒索软件攻击后采用的策略类似。

粮食供应链所涉及的公司应该保护自己，确保对所有系统和流程的完整可见性，同时确保持续监测可能由针对性或机会性攻击造成的任何威胁。准确的资产清单是正确管理漏洞的第一步，以确保关键系统达到当前的修补水平，并在适当的时候进行补偿性控制。

如需有关 NEW Cooperative 攻击的跟多信息，请参考：
https://www.claroty.com/2021/09/21/blog-food-supply-chain-latest-ransomware-target/

第 7 部分：建议

Team82 建议采取这些安全措施，以应对我们在本报告中分享的漏洞趋势。

网络分割

随着气隙系统工业设备成为过去，更多的设备连接到互联网并通过云端进行管理，我们必须优先考虑网络分割等深入防御措施。我们建议网络管理员：

- 对网络进行虚拟分割，并以可远程管理的方式进行配置
- 创建针对工程和其他面向流程的功能的特定区域政策。
- 保留探查流量和 OT 特定协议的能力，以检测和抵御异常行为。

勒索软件、网络钓鱼和垃圾邮件保护

远程工作的增加加大了对电子邮件作为重要沟通机制的依赖。因此，这些情况也增加了员工成为网络钓鱼或垃圾邮件攻击目标的风险，从而增加了勒索软件和其他恶意软件感染的风险。我们鼓励安全从业人员和所有员工：

- 不要从不信任的来源打开电子邮件或下载软件
- 不要点击未知发件人发来的电子邮件中的链接或附件
- 不要通过电子邮件向任何人提供密码、个人或财务信息（敏感信息也用于双重勒索）
- 始终验证电子邮件发件人的电子邮件地址、姓名和域
- 经常备份重要文件，并将其与主系统分开存储
- 使用防病毒、反垃圾邮件和反间谍软件保护设备
- 立即向相应的安全或 IT 人员报告网络钓鱼电子邮件
- 执行多因素身份验证

远程访问连接保护

即使世界开始摆脱 COVID-19 大流行期间的限制，远程工作也是新常态。随着组织适应增加的与公司资源的远程连接，他们必须以安全的方式这样做。在 OT 环境和关键基础设施中，这一点至关重要，因为操作人员和工程师需要对工业资产进行安全的远程访问，以确保流程的可用性和安全性。我们鼓励安全从业人员：

- 验证 VPN 版本是否已修补并更新到最新版本
- 监控远程连接，尤其是与 OT 网络和 ICS 设备的远程连接
- 实施精细的用户访问权限和管理控制

保护运营管理和监督控制

2021 年下半年披露的大多数 ICS 和 SCADA 漏洞影响了第 3 级：运营管理（Historian、OPC 服务器等），紧随其后的是第 2 级：监督控制（HMI、SCADA 和工程工作站）。

大多数运营管理和监督控制漏洞都是基于软件的，而基本控制漏洞大部分是基于固件的。由于无法随着时间的推移打补丁，特别是 1 级设备固件，我们建议投资于分割、远程访问保护，以及更好地保护运营管理和监督控制级别，因为它们提供了对基本控制级别的访问权限，并最终对流程本身进行保护。其他建议包括：

- 使用加密、访问控制列表和适合 OT 网络的适当远程访问技术等机制来保护远程访问连接。
- 保持资产库存和细分。
- 评估风险并确定关键补丁的优先次序。
- 确保设备有密码保护，并执行严格的密码卫生措施。
- 实施细化的基于角色和政策的管理访问。
- 正如我们所看到的，大多数基于本地攻击矢量的 2 级漏洞都依赖于用户互动，坚持最佳实践来防御社会工程技术。

致谢

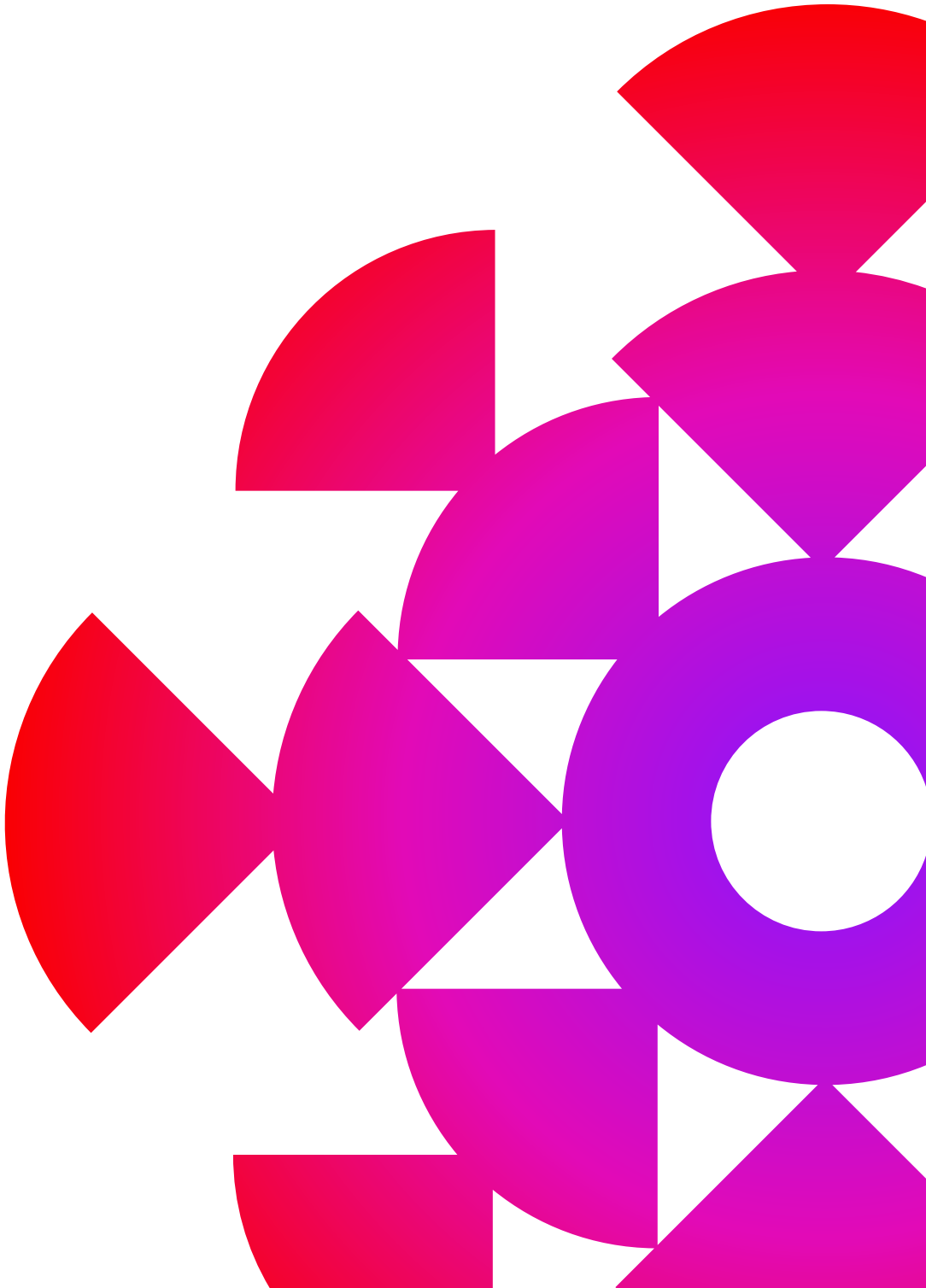
本报告的第一作者是 Claroty 安全研究员 Chen Fradkin。

其他为本报告作出贡献的人员包括：Claroty 公司安全研究团队负责人 Rotem Mesika，创新总监 Nadav Erez，漏洞研究团队负责人 Sharon Brizinov，以及 Claroty 公司研究副总裁 Amir Preminger。特别感谢整个 Claroty 研究团队为本报告的各个方面和研究工作提供了卓越的支持，为报告提供了动力。

关于 CLAROTY

Claroty 使企业能够确保工业 (OT)、医疗保健 (IoMT) 和企业 (IoT) 环境中信息物理系统的安全：扩展物联网 (XIoT)。该公司的统一平台与客户的现有基础设施相整合，为可见性、风险和漏洞管理、威胁检测和安全远程访问提供了全方位的控制。Claroty 由全球最大的投资公司和工业自动化供应商提供支持，被全球数以百计的组织部署于数千个地点。公司总部设在纽约市，在欧洲、亚太和拉丁美洲都有分公司。

如需了解更多信息，请访问 www.claroty.com。



CLAROTY