CLAROTY

TEAM82

Cyberworld
科明大局

解决 CPS 身份危机

全新的 CPS 资产信息数字库
解决整个行业中产品标识符不一致的问题

引言

网络化物理系统（CPS, Cyber Physical Systems）资产因满足不同客户和地区的需求，呈现出多种多样的变体和配置。虽然每一家医疗设备制造商（MDM, Medical Device Manufacturer）或原始设备制造商（OEM, Original Equipment Manufacturer）在物理世界中都有完善的方法来精确识别每个变体，但他们在网络世界中的命名规则是事后才考虑的。

由于同一资产在信息收集方式不同的情况下会报告出不一致的别名，负责保护 CPS 的安全团队和网络管理员在进行公共漏洞和暴露（CVE, common vulnerability and exposure）归因时，会出现不完全匹配的情况，从而削弱他们准确评估环境中网络风险范围和修复措施的能力。

Claroty Team82 研究团队基于数据对该问题进行了分析，揭示了问题的严重程度，并展示了现有产品信息的差异。分析还表明，需要一个集中式存储库，用于提供 OEM 和 MDM 的默认配置、当前厂商批准的补丁级别、设备出厂时是否带有默认凭证或已知凭证，并有助于识别阻碍“最后一公里修复（Last-mile remediation）”的风险。

例如：同一产品系列的可编程逻辑控制器（PLC, Programmable Logic Controllers），可能会因配置不同的网络接口卡（NIC, Network Interface Cards）、模块、中央处理器（CPU, Central Processing Units）而引入各自的软件和固件漏洞、不安全的配置。主动和被动的流量收集方法也可能因信息来源和所使用的协议不同，获得不同的标识符，这使得信息的关联变得困难。

这种差异还会进一步影响到 CVE 机构，它们依赖受影响厂商提供的信息来编写安全公告；一些内部设备映射可能随着时间推移未得到 MDM、OEM 的完善，许多公告缺乏相关的上下文，安全团队难以全面理解哪些产品、版本、配置可能受到新报告漏洞的影响。

数据不一致的情况，比如操作系统名称和版本存在多个或缺失，或型号前缀各不相同，通常需要安全和网络团队手动操作，从各自供应商提供的资源中拼凑出完整的信息。

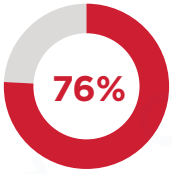
例如：在 Claroty 的数据集中，可以看到一些 OEM 产品代码和型号从未在 CVE 公告中发布。厂商的产品目录可能会列出产品名称及其支持的大量型号，但这些信息在 CVE 公告中依然不完整，导致安全团队只能根据现有信息推断某设备是否易受特定 CVE 的影响。

因此，同一资产可能会存在多重漏洞，具体取决于设备的设置方式以及漏洞是否仅影响特定配置的产品。

主要发现

基于一个包含 1,700 万个 CPS 资产的数据集，Claroty Team82 研究团队得出以下结论：

88% 的 CPS 资产在数据采集过程中未传输精确的产品代码。



76% 的设备传输的产品代码与厂商的官方记录不一致。

为了解决设备数据碎片化问题，并推动整体 CPS 风险的降低，Claroty Team82 研究团队结合自身在协议研究方面的经验，以及基于 AI 自动化数据集分析，填补了部分数据空白，纠正了数据不一致之处，并显著提升了资产可视化。

- 对于一家大型工业自动化厂商，Claroty 的映射准确率流程取得了显著改进，产品代码识别率从 **4%** 提升到 **83%** 。
- 在成功匹配新的产品代码后，**56%** 的设备收到了针对陈旧固件的全新或更新的安全建议。
- 因此，Claroty 能够把漏洞识别的准确率提升 **25%** 。

用户在处理与漏洞“最后一公里修复”相关的复杂流程时，很容易陷入困境。最终，资产所有者如何才能确保软件补丁、固件更新、补偿性控制的实际操作工作已经完成，并且风险得到了降低？

本报告探讨了资产可视化的细微差别及其对整体 CPS 防护的影响，剖析了 CPS 资产识别的核心挑战，并介绍了一种基于 AI 的设备信息映射方法，该方法能显著提升资产可视化。

命名规则不一致

产品代码是设备识别的重要标准，但在 OT 和医疗物联网（IoMT, Internet of Medical Things）协议中，它们很少以数字形式提供。在 Claroty 的数据集中，Claroty Team82 研究团队发现 **88%** 的 CPS 资产未传输产品代码；其他命名规则不一致，例如型号名称和产品编号与厂商目录不匹配，这让现场资产的完整识别变得复杂。

另外，Claroty Team82 研究团队发现，许多 CPS 设备不会定期传输操作系统（OS）名称或版本，这可能会给希望将此信息与已知漏洞关联的组织造成重大的风险管理缺口。因此，大多数安全团队无法将漏洞与特定资产完全对应起来，从而造成安全盲点、延长遭受攻击的时间、修复不彻底。

41% 41% 的 CPS 设备未提供操作系统版本信息。

24% 24% 的 CPS 设备未提供操作系统名称信息。

单个资产，多个别名

Claroty Team82 研究团队分析的工业控制系统（ICS, Industrial Control Systems）和传统医疗设备揭示了准确识别资产的另一项挑战：比如，一个存在漏洞的控制器，会因所使用的协议或数据采集方法不同而拥有多个别名。

这些别名可以是产品系列名称（在 Claroty 的数据集中，超过四分之三的设备存在多个名称变体）、型号、版本等标识符。此外，同一受影响的控制器在 NVD 公告、厂商自身的安全公告、OEM 与 MDM 的产品目录中所列出的信息也可能不一致。

安全团队通常需要从众多来源推断设备的产品系列、型号或版本信息，原因很简单：产品代码很少被传输给安全工具进行关联分析。

33% 33% 的型号因所使用的协议或集成方式不同，存在多个名称变体。

76% 76% 的设备型号名称与厂商名称不一致。

Claroty CPS Library：解决“最后一公里修复”的难题

“最后一公里修复（Last-mile remediation）”对安全团队来说是一个重大难题，因为目前没有一个集中式存储库，能够提供经过认证的 OEM 和 MDM 补丁级别，以便他们确认其资产是否确实受到某个 CVE 影响。当前，这需要安全团队手动访问厂商资源，并将可能受影响的产品与厂商目录进行匹配。在一个拥有数十家 CPS 资产供应商的企业中，这是一项耗时且成本高昂的过程，必须定期安排执行。

如果缺乏充分的可视化和设备识别能力，企业根本无法全面管理风险暴露。如果厂商没有标准化的方法来识别型号和组件级别的产品，这个问题就会层层蔓延，最终导致漏洞公告出现不一致的情况：资产与漏洞的匹配不完全，CVE 归因也不一致。

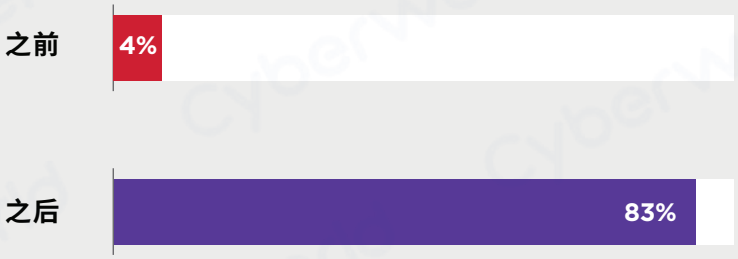
与此同时，CPS 面临着严峻的补丁挑战，包括 OT、ICS、医疗系统、医疗设备，这让许多企业的风险暴露窗口长时间处于开放状态。例如，在美国，医疗设备的更新若涉及网络安全，必须经过美国食品药品监督管理局（FDA）的审查和批准。此外，MDM 要求设备只能在特定的补丁级别下运行，这又增加了复杂性。这种情况在一些运行于 CPS 环境中的复杂工业自动化系统中也同样存在。例如，一些 OEM 要求控制系统和其他连接的资产只能在特定的补丁级别下运行。

集中式存储库能够提供必要的标识符，让企业能够正确地把资产与漏洞匹配，从而克服“最后一公里修复”中的挑战。

Claroty Team82 研究团队分析了一家大型 OEM 的设备目录，并结合 Claroty 的 OT 协议知识，运用 AI 技术填补了数据空白，修正了缺失数据，从而提高了映射和识别准确率。

这项工作使其资产的映射准确率提高了 **83%** 。

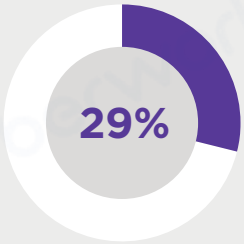
提升某 OEM 的映射准确性



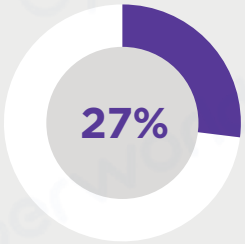
仅 4% 的设备被识别出来。

使用 CPS Library 后，83% 的设备被成功识别。

在此基础上，为所分析的 56% 的设备环境中陈旧固件，提供全新或更新的建议。



29% 的设备收到了针对先前未知固件的新修复建议。



在特定型号的新固件版本发布后，有 27% 的设备收到了更新的修复建议。

让漏洞评估变得更加准确。

假阴性率降低 15%

通过提高映射精度，
识别出以前未曾发现的漏洞。

假阳性率降低 10%

改进设备与漏洞匹配。

AI 助力 CPS 产品代码映射

Claroty 的 CPS Library 解决了 CPS 安全中复杂且现实的问题：如何可靠地把发现的资产映射到厂商提供的权威产品代码。这是实现精确资产、漏洞和风险暴露识别的基础，也是风险管理策略的核心。

Claroty 解决方案不仅仅是简单的查找，而是融合了多源数据采集、证据图谱建模（evidence graph modeling）、强大的统计集成学习、CPS专家的校准，在真实的运行环境中充分展现 Claroty 深厚的数据科学专业知识。

构建证据图谱（Evidence Graph）：真实（Ground Truth）校准

Claroty的方法首先从网络流量、厂商目录、配置管理记录、安全公告中系统性地收集资产数据。这些多样化的输入数据相互关联，形成一个全面的“证据图谱”，该图谱模拟了所有可能的关系，包括别名、系列、属性、替代项（replacements）、旧代码。

关键在于，标记由 CPS 专家精心整理和验证的特定“真实（ground truth）”连接。这些连接成为 Claroty 的 AI Agents 学习、重新训练并实时调整其映射策略的校准点，保证每次推断都以实际现场数据为基准，而不是以通用的模板为基础。

多智能体 AI (Multi-Agent AI)：专业化的 CPS 智能

在 CPS Library 中，Claroty 部署了多个服务于 CPS 的 AI Agent。可以想象成，一群拥有多年经验的 CPS 专家正在处理数据，他们各自专注于设备识别的不同方面：

自然语言处理模型（NLP Models）：解析混合格式、源自协议的命名字符串、软件标记和代码片段。

统计推理器（Statistical Reasoners）：运用置信度评分和复杂的统计测试来权衡证据、区分信号与噪声，并利用从“真实（ground truth）”校准中获得的经验关系。

领域引导的 CPS 规则（Domain-Guided CPS Rules）：实施经过现场验证的逻辑，识别硬件代际、固件兼容性、更换周期等细微差别，确保不会将“外观相似”的资产错误分类。

随着新的“真实（ground truth）”数据不断进入证据图谱，所有 Agent 都会持续进行重新校准，形成一个闭环系统，确保在现实世界中的可靠性并持续改进。

集成方法：数据科学专业知识的实践应用

在厂商产品代码映射中嘈杂且相互矛盾的现实环境下，单一模型不足以胜任。以下是 Claroty 的集成系统如何树立新的标准：

加权投票与噪声校准

为了整合所有结果，Claroty 采用了一种名为集成学习（ensemble learning）的数据科学技术。Claroty 架构中的每个 AI Agent 或模型都具备专门的优势，但也存在各自的盲点，例如难以处理模糊的目录条目、有限的协议上下文、某些设备类型的数据稀疏性（data sparsity）。

鉴于此，Claroty 的集成方法不仅仅是简单的聚合，而是主动弥补每个 Agent 知识的不足。让多个不同的模型共同参与，每个模型采用不同的视角、数据源和推理方法，降低因单一模型主导决策而带来的风险。

在“白噪声（white noise）”区域，例如数据不完整或相互矛盾的区域，这种方法尤为有效，因为集成共识有助于抑制随机或无方向性误差。最终结果是输出更加稳健：集成系统填补了各个模型盲点造成的空白，最大限度地降低了模糊或噪声数据环境下的错误率，这充分展现了 Claroty 在数据科学方面的深厚造诣，以及在应对现实世界 CPS 复杂性方面的实践经验。

基于实际情况、经专家验证的共识

集成系统做出的每一个决策最终都基于证据图谱的“真实（ground truth）”关联，这使得整个过程既具有统计上的稳健性，又具有实际操作上的可靠性。这种“校准共识（calibrated consensus）”意味着 Claroty 的建议与实际操作人员在现场遇到的情况相符，而不仅仅是理论上的最优解。

验证与持续改进

模糊不清或置信度较低的映射会被标记出来，以便由专家进行人工审核。人工基准测试、反馈循环、数据丰富化进一步优化了 AI 模型，确保在新环境中持续提高准确性和可靠性。对误差分布的统计分析有助于针对未来版本中最具影响力的整理工作。

总结

由于产品信息通过各种通信协议传输方式的不一致，安全团队在 CVE 归因和全面了解其 CPS 环境中的风险方面面临着巨大挑战。这导致在把缺失或繁杂的命名规则与漏洞和固件级别进行对应时出现空白。

Claroty Team82 研究团队利用 AI 和数据分析的方法对该问题进行了分析，揭示了现有产品的信息差异。厂商产品代码很少以数字形式提供。其他资产信息，例如操作系统、版本、补丁级别、默认配置等，也必须从不同的 OEM 和 MDM 资源中手动收集。

安全团队在尝试把 CVE 信息与其环境中的资产进行匹配时，不得不处理各种不同的型号名称和产品配置。CPS 资产的模块化特性也意味着某些漏洞仅存在于特定配置中，这进一步加剧了这项工作的复杂性。这些多重别名常常迫使用户从众多来源推断产品信息的准确性。同时，CVE 信息也不完整，因为它依赖于同样不一致的产品信息。

Claroty Team82 研究团队针对资产映射准确性问题提出的新方法取得了显著成效。结合 AI 技术与 OT 协议经验，提高了一家 OEM 产品目录的资产识别准确率；为所分析的 56% 的设备环境中陈旧固件，提供全新或更新的建议，并减少资产与漏洞匹配中的误报和漏报。

关于 Claroty

Claroty 凭借无与伦比的、以工业为主的平台重新定义了网络化物理系统 (Cyber Physical Systems, CPS) 防护。Claroty 平台旨在保护关键任务型基础设施，提供市场上最深入的资产可视化、最广泛的 CPS 安全解决方案，涵盖了风险管理、网络防护、安全访问、威胁检测，可以在云端使用 Claroty xDome，也可以在本地部署 Claroty CTD。Claroty 平台以屡获殊荣的威胁研究和技术联盟为后盾，帮助企业有效降低 CPS 风险，提供最快的价值实现时间 (TTV) 和更低的总拥有成本 (TCO) 。在全球范围内，已有数百家企业在数千个站点部署了Claroty。

关于 Team82

Team82 是 Claroty 的研究团队，曾多次获奖，以研究威胁、分析 OT 和医疗协议、发现与披露工业、医疗、商业漏洞而闻名。Team82 致力提升 CPS 网络安全，拥有业内规模最大的测试实验室，并与行业领先的供应商紧密合作，评估其产品的安全性。截至 2025 年 11 月，Team82 已披露了 710 个漏洞。