SIEMENS华东区安徽省阜阳市西门子（授权）一级总代理-西门子伺服电机一级总代理

产品名称	SIEMENS华东区安徽省阜阳市西门子（授权）一级总代理-西门子伺服电机一级总代理
公司名称	广东湘恒智能科技有限公司
价格	.00/件
规格参数	变频器:西门子代理商 触摸屏:西门子一级代理 伺服电机:西门子一级总代理
公司地址	惠州大亚湾澳头石化大道中480号太东天地花园2栋二单元9层01号房（仅限办公）（注册地址）
联系电话	18126392341 15267534595

产品详情

【二】三种攻击场景Team82研究人员为Evil PLC攻击确定了三种不同的攻击场景。其中包括将PLC武器化以实现初始访问、攻击移动集成商以及将PLC武器化为蜜罐。Claroty研究人员确定，攻击者可以使用武器化的PLC在内部网络上获得初步立足点，甚至进行横向移动。暴露在互联网上的PLC通常缺乏身份验证和授权等安全性，并通过Shodan和Censys搜索发现。能够以这种方式访问PLC的攻击者能够通过恶意下载程序修改参数或其行为和逻辑。机会主义攻击者识别面向互联网的PLC，使用商业工程师站软件连接到它们，并上传当前项目，其中包括来自PLC的代码和设置，Claroty博文然后，攻击者将修改项目的逻辑，并执行下载程序以更改 PLC
逻辑。此类事件的一个例子是2020对以色列供水系统的攻击，攻击者利用可访问的 PLC并试图向供水系统注入氯气。研究表明，攻击者可以使用面向互联网的PLC渗透整个OT网络的支点。攻击者不仅可以简单地连接到暴露的PLC并修改逻辑，还可以武装这些PLC并故意造成故障，将工程师引诱到他们那里。作为一种诊断方法，工程师将执行一个会危及他们机器的上传程序，这将促成攻击者在OT网络上站稳了脚跟。Claroty还发现，攻击者可以将系统集成商和承包商作为进入世界各地许多不同组织和站点的一种手段。现代OT管理通常涉及与许多不同网络和 PLC 交互的第三方工程师和承包商。在这种攻击场景中，系统集成商是PLC和工程师站之间的枢纽，负责监督众多OT网络。 研究人员说，攻击者会将PLC定位在一个远程、安全性较低的设施中，该设施已知由系统集成商或承包商管理。然后攻击者将PLC武器化并故意在PLC上造成故障。通过这样做，受害工程师将被引诱到PLC进行诊断。通过诊断过程，集成商将执行上传程序并让他们的机器受到威胁。他们补充说，在获得集成商机器的访问权限后，攻击者可以反过来攻击甚至武器化其他组织内部新访问的PLC，从而进一步扩大他们的控制范围。Claroty确定，防御者可以使用蜜罐PLC来吸引和攻击可能的攻击者，从而威慑和挫败潜在的攻击者。从防御的角度来看，攻击向量很有用，可以用来诱捕攻击者。鉴于攻击者经常使用与工程师相同的商业工具，防御者可以故意设置面向公众的武器化PLC，并允许攻击者与之交互。这些PLC将充当蜜罐，吸引攻击者与之交互。 然而，如果攻击者落入陷阱并在枚举过程中从诱饵PLC执行上传，则武器化代码将在攻击机器上执行。研究人员补充说，这种方法可用于在枚举的早期检测攻击，也可能阻止攻击者瞄准面向互联网的PLC，因为他们需要保护自己免受他们计划攻击的目标的侵害。Claroty表示，要达到100%的补丁级别，尤其是在关键基础设施中，并不容易，因此提供了额外的缓解措施，有助于降低Evil PLC攻击的风险。武器化是第一步，因此，研究人员建议尽可能限制对PLC的物理和网络访问。毫无疑问，此类设备不应从外部访问或在线公开。但内部访问也应jinxian于授权的工程师和操作员。Claroty建议落实网络分段和网络卫生，以确保与PLC的连接jinxian制对一小部分工程师站的访问，从而大大减少了网络中的攻击面。它还建议使用客户端身份验证来验证客户端和工程师站的身份。目前，一些供应商实施这样的通信协议，而不是允许任何工程师站与 PLC
通信，只有一组特定和预定义的工程师站能够与PLC交互，通过要求工程师站向PLC 出示证书。随着Evil PLC攻击向量向PLC执行下载/上传程序，监控OT网络流量并特别检测这些类型的事件非常重要，如果这样的程序在意外情况下发生，它可能表明有漏洞利用的企图。此外，随着攻击者和防御者进一步研究这种新的攻击向量，将会发现更多类似上面所示的漏洞，并且OT供应商将修补这些漏洞。与OT软件保持同步很重要，这将防止利用这些1-day漏洞的攻击。