西门子S7-300,轨道西门子代理商

产品名称	西门子S7-300,轨道西门子代理商
公司名称	湖南西控自动化设备有限公司
价格	.00/件
规格参数	西门子:S7300 PLC:6ES73901AE800AA0 德国:轨道=480MM
公司地址	中国（湖南）自由贸易试验区长沙片区开元东路1306号开阳智能制造产业园（一期）4#栋301
联系电话	17838383235 17838383235

产品详情

使用西门子工控系统的注意了，已经暴露了15个安全漏洞

网络安全研究人员披露了西门子 SINEC 网络管理系统 (NMS) 中 15 个安全漏洞的详细信息，其中一些可能被攻击者混合使用，以在受影响的系统上实现远程代码执行。

工业安全公司 Claroty在一份新报告中表示：“ 这些漏洞如果被利用，会给网络上的西门子设备带来许多风险，包括拒绝服务攻击、凭据泄漏和在某些情况下远程执行代码。 ”

值得庆幸的是，2021年10月12日，西门子在 V1.0 SP2 版本更新中解决了上述所有的安全漏洞（从 CVE-2021-33722 到 CVE-2021-33736）。西门子在一份报告中写到，严重的漏洞可能允许经过身份验证的远程攻击者，在某些条件下以系统特权在系统上执行任意代码。

威胁大的漏洞编号是CVE-2021-33723（CVSS 评分：8.8），它允许攻击者将权限升级至管理员账号，病号可以与路径遍历漏洞 CVE-2021-33722（CVSS 评分：7.2）想结合，终实现远程任意代码执行。

此外，还有一个需要注意的是 SQL 注入漏洞，漏洞编号（CVE-2021-33729，CVSS 分数：8.8），通过该漏洞，经过身份验证的攻击者可以在本地数据库中执行任意命令。

Claroty 的 Noam Moshe认为，SINEC在网络拓扑中处于至关重要的中心位置，因为它需要访问凭据、加密密钥和其他授予它的管理员访问权限，以便管理网络中的设备。

从攻击者的角度来看，这种攻击是利用合法凭证和网络工具进行恶意活访问、活动和控制，而SINEC将攻击者置于以下主要位置：侦察、横向移动和特权升级。