唐山西门子低压电器一级总代理，变频器代理商

产品名称	唐山西门子低压电器一级总代理，变频器代理商
公司名称	上海跃韦科技集团有限公司
价格	.00/件
规格参数	西门子:西门子PLC模块.电机代理 全系列:西门子变频器通讯电缆代理 德国:西门子触摸屏DP接头代理
公司地址	上海市金山区吕巷镇溪北路59号5幢（三新经济小区）（注册地址）
联系电话	15821196730 15821196730

产品详情

我司长期***供应产品：西门子授权代理商优点详尽详细如下：

1、 SIMATIC，PLC、S7-200、S7-300、S7-400、S7-1200,S7-1500,S7-200SMART,S7-200CN,ET200

2、 逻辑思维控制器 LOGO！230RC、230RCO、230RCL、24RC、24RCL等

3、 SITOP 系列产品可调稳压电源 24V DC 1.3A、3A、10A、20A、40A

4、HMI 触摸液晶屏TD200 TD400C TP177,MP277 MP377SIEMENS 交、可调稳压电源传动系统

5、 变频调速器MICROMASTER系列产品：MM、MM420、MM430、MM440、G110，G120,V20,V90,ECO MIDASTER系列产品：MDV 6SE70系列产品（FC、VC、SC）

6、全源数据直流调速装置 6RA23、6RA24、6RA28、6RA70 系列产品SIEMENS 加工中心 直流伺服电机

7、840D、802S/C、802SL、828D 801D：6FC5210,6FC6247,6FC5357,6FC5211,6FC5200,6FC5510,

8、伺服驱动 ：6SN1123,6SN1145,6SN1146,6SN1118,6SN1110,6SN1124,6SN1125,6SN1128

工业网络安全公司Claroty研究人员近日发现了一个严重的漏洞，未经认证的远程攻击者可以利用这个漏洞攻击西门子旗下的可编程逻辑控制器(PLC)。该漏洞被编号为CVE-2020-15782，是一个高危的内存保护绕过漏洞，允许攻击者通过网络访问TCP 102端口在受保护的内存区域中写、读数据。这一远程可利用漏洞引发了研究者对西门子控制器安全问题的深入思考。

工业巨头西门子公司表示，该安全漏洞影响其SIMATIC S7-1200和S7-1500 cpu，可通过新的漏

洞远程攻击其PLC产品。西门子已经为一些受影响的设备发布了固件更新，并为尚未发布补丁的产品提供了变通方案。——西门子PLC产品

根据Claroty公司的说法，该漏洞可绕过通常工程代码运行的沙箱，直接访问设备内存，从而在西门子S7 PLC上获得本机代码执行。研究人员展示了攻击者如何绕过保护直接将shellcode写入受保护的内存中。沙箱逃逸意味着攻击者可以从PLC的任何地方读写，并可用恶意代码修补内存中现有的VM操作码，从而对设备进行Root权限的操作。重点强调的是，利用这一漏洞的攻击将很难被发现。

研究成果的披露是西门子和Claroty公司紧密关系的结果，这不仅促进了工业网络安全研究团队和供应商在漏洞披露方面的合作，也促进了整个工业生态系统的安全。西门子和Claroty之间的密切合作包括技术细节、攻击技术和缓解建议的交流，这些都有助于促成西门子及时发布更新补丁。西门子和Claroty希望，鉴于此漏洞的关键性质，用户应尽快更新S7-1200、S7-1500 CPU，以及其他受影响产品。

一、漏洞简介及受影响产品

1.漏洞概况

编号：CVE-2020-15782，在内存缓冲区范围内对操作的不当限制。CVSS v3.1得分:8.1。在zhiming漏洞网站vuldb.com上给的基本信息如下。

2.受影响产品

受影响的设备容易受到内存保护绕过而实施特定的操作。对TCP端口102进行网络访问的远程未经身份验证的攻击者可能会将任意数据和代码写入受保护的内存区域，或读取敏感数据以发动进一步攻击。

5月28日，西门子发布了警告SSA-434534，向用户通报该漏相关信息。西门子还发布了包括S7-1500、S7-1200的各种产品的更新，建议用户更新到***新版本以弥补漏洞。该公司表示，正在为尚未更新的产品准备进一步更新。西门子还提供了用户可用于降低风险的具体缓解措施。

二、西门子PLC本地代码执行的演进

CVE-2020-15782之所以受到如此关注，主要是这一漏洞的成功利用，将有可能将工业网络安全研究者对西门子控制器攻击研究提高到新层次，而攻击者实施成功攻击的限制则越少越易，原因就是该漏洞的条件太优越。

在可编程逻辑控制器(PLC)等工业控制系统上实现本机代码执行是那些gaoji水平高能力攻击者已经实现的***终目标。因为这些复杂的系统有许多内存保护，攻击者不仅为了能够运行他们选择的代码，而且还要不被发现，因此必须要跨越这些保护措施。

早期的攻击尝试需要对PLC的物理访问和连接，或者以工程师工作站为目标的技术和通向PLC的其他链接，以获得那种级别的代码执行。而此次Claroty公司利用一个新发现的漏洞，在西门子SIMATIC S7-1200和S7-1500 PLC cpu内绕过PLC沙箱，在内存保护区域运行本机代码，进一步提升了这种攻击思路的远程可行性。攻击者可以利用这个CVE-2020-15782漏洞，远程获取难以检测和删除的读写内存访问。

从攻击者的角度来看，PLC漏洞利用的***目标就是在PLC上实现不受限制和不被检测的代码执行。这意味着，能够将代码隐藏在PLC内部深处，而不被操作系统或任何诊断软件检测到。

多年来，鉴于西门子PLC在市场上的***地位，已经出现了许多在西门子PLC上实现这种能力的尝试。

首先，史上***zhuming的震网攻击（Stuxnet），它在旧的SIMATIC S7-300和S7-400上获得了用户级的代码执行。代码修改本身是通过操作本地step7项目文件来完成。然后，Stuxnet能够通过操纵本地工程站上的WinCC二进制文件来隐藏PLC上的代码更改。这样一来，恶意软件不仅可以偷偷地将自己安装在PLC上，而且当控制软件试图从PLC读取受感染的内存块时，还可以保护自己不受WInCC检测。当然，通过对其Windows操作系统的Microsoft更新和SSA-110665和SSA-027884中记录的西门子产品更新的组合，这个问题早已得到解决。

第二个经典型的PLC攻击，是2019年的Rogue7的攻击（出自论文Rogue7:Rogue Engineering-Station attacks on S7 Simatic PLCs）。《Rogue7》背后的研究人员能够创建一个流氓工程站，它可以伪装成TIA（TIA Portal是一系列无缝集成的自动化解决方案）通往PLC的门户，并注入任何有利于攻击者的信息。通过理解密码信息是如何交换的，他们能够将代码隐藏在用户内存中，而TIA工程站是看不见的。西门子部分解决了此问题，并提供了缓解措施，详见SSA-232418。

第三个，同在2019年，德国波鸿鲁尔大学(Ruhr University Bochum)安全研究***Ali Abbasi和Tobias Scharnowski介绍了他们如何通过物理攻击SIMATIC 1200来获得在西门子S7 PLC上的代码执行。他们使用UART（通用异步收发传输器（Universal Asynchronous Receiver/Transmitter)，通常称作UART。它将要传输的资料在串行通信与并行通信之间加以转换。 作为把并行输入信号转成串行输出信号的芯片，UART通常被集成于其他通讯接口的连结上。）物理连接来转储固件，并发现了一个漏洞链，使他们能够将代码隐藏在系统中更深的地方，并获得不受限制的代码执行。西门子在SSA-686531中解决了这个问题。

本次，claroty研究团队将这项研究向前推进了一大步，他们展示了一种新的复杂的远程攻击，它允许攻击者在西门子S7 PLC上获得本机代码执行。攻击目标是内核的深处，并避免了任何检测，因为能够逃离用户沙箱，并在受保护的内存区域中编写shellcode。CVE-2020-15782漏洞恰恰是促成PLC沙箱逃逸的关键条件。