西门子伺服电机授权代理商丨辽宁地区一级供应商

产品名称	西门子伺服电机授权代理商丨辽宁地区一级供应商
公司名称	上海乘晖科技集团有限公司
价格	.00/台
规格参数	西门子:西门子电机总代理 西门子电机:西门子电机总代理商 德国:西门子电机一级总代理
公司地址	上海市奉贤区驰华路775号2幢
联系电话	18674345958 18674345958

产品详情

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。

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

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。

西门子PLCs本地代码执行攻击发展历程

三、PLC沙箱逃逸

PLC的完整性对操作人员和工程师来说至关重要，而攻击者的目标就是通过隐藏于控制器上的代码和提升权限来破坏这种完整性。本次利用的漏洞CVE-2020-15782，绕过了PLC执行环境中的现有保护，包括工程代码通常会运行的沙箱。Claroty能够利用这个漏洞实现沙箱逃逸，以便直接访问内存，然后编写并注入shellcode来执行其对西门子1200/1500 PLC的攻击。

为了执行这种攻击，需要对PLC进行网络访问。此外，攻击者还需要PLC下载权限。自从TIA Portal V12以来，西门子提供了各种缓解控制，以限制用户网络和对PLC的读写访问，特别是口令保护机制。此外，从V17开始，西门子引入了在PLC、HMI和TIA Portal之间使用个人证书的TLS通信，这大大减少了潜在的攻击面。

3.PLC的通用结构（以S7 PLC为例）

为了理解Claroty的具体攻击，先要概述一个标准PLC的通用结构。它的CPU是一个16或32位微处理器，由一个内存芯片和集成电路组成，管理控制逻辑、过程监控和通信。CPU指导PLC执行控制指令，与其他设备通信，执行逻辑和算术操作，并执行内部诊断。它还运行内存例程，不断检查PLC，以避免编程错误，并确保内存没有损坏。逻辑运行在沙盒环境（有时也被称为“ 监狱 ”）中。传输到控制器的逻辑jinxian于供应商提供的特定内存区域和API。

以西门子S7 PLC为例，它运行在ADONIS内核和ARM或MIPS处理器上，有许多编程语言可用于配置控制器，包括语句列表(STL)、梯形图(LD)、功能框图(FBD)和结构化控制语言(SCL)。

不管何种输入源，PLC程序都会编译成MC7/MC7+字节码，这是一种低级别的代码表示。经工程站编译后-西门子TIA门户-代码块(MC7/MC7+格式)通过西门子的S7Comm/S7Comm+协议下载并安装到PLC中。然后，PLC中的MC7虚拟机将对代码块进行分派，并对字节码进行解释和执行。

PLC程序执行过程

如果不具备逆向工程能力，是不可能解码MC7/MC7+字节码的，因为西门子没有公开提供这种技术文档。因此，研究才必须用逆向工程分析MC7/MC7+字节码语言集，以便理解其内部机制并发现bug。

4.S7PLC沙箱逃逸

由于虚拟机限制了用户程序访问的资源，因此编译后的字节码只能用于访问操作系统允许的资源，而不能直接用于硬件操作。这是为了将用户和运行代码限制在一组被认为是安全且已定义的操作中。例如，操作系统将限制对受保护内存的任何直接访问，但会允许使用Siemens提供的标准库中的任何函数(例如ADD_I - Add Integer子例程)。换句话说，操作系统将用户代码“锁定”在一个沙盒/容器中，对资源、内存和功能的访问是有限的，这可能会破坏PLC和/或整个进程。

为了逃逸或“越狱”本地SIMATIC S7-1200和S7-1500沙箱，Claroty利用了其内存保护绕过漏洞。该漏洞使攻击者能够将任意数据和代码写入所谓的受保护的内存区域，或读取敏感数据以发动进一步攻击。

利用CVE-2020-15782实现沙箱逃逸

沙箱逃逸意味着攻击者可以从PLC上的任何地方读写，并可以用恶意代码修补内存中现有的VM操作码来实现对设备的ROOT权限操作。例如，Claroty能够直接将ARM/MIPS shellcode注入到内部操作系统结构中，这样当操作系统使用其选择的特定操作码时，恶意shellcode就会执行，从而远程执行代码。Claroty使用这种技术安装了一个内核级程序，它具有一些对操作系统完全隐藏的功能。

四、防范建议

4.缓解措施

西门子已经确定了以下具体的解决方案和缓解措施，并强烈建议客户采用它们来降低风险:

S7通信采用口令保护

通过S7-1200或S7-1500CPU的ENDIS_PW指令禁止客户端连接(这将阻塞远程客户端连接，即使客户端可以提供正确的口令)

使用显示配置额外的访问保护S7-1500 CPU(这将阻止远程客户端连接，即使客户端可以提供正确的口令)应用“纵深防御”，如工业操作指南第12ff页所述安全措施,特别是:

1.工厂安全:对关键部件的物理防护；

2.网络安全:确保PLC系统没有连接到不可信的网络；

3.系统完整性:配置、维护和保护设备应用适用的补偿饱和控制和使用内置的安全能力。

将整个解决方案更新到TIA Portal V17，并使用PLC、HMI和PG/PC之间的个人证书TLS通信

5.通用的安全建议

作为一种通用的安全措施，西门子强烈建议使用适当的保护机制对设备网络访问。为了在受保护的IT环境中运行设备，西门子建议按照西门子工业安全操作指南进行环境配置(https://www.siemens.com/cert/operational-guidelines-industrial-security)。

请按照产品手册中的建议操作。关于西门子工业安全的更多信息可以在https://www.siemens.com/industrialsecurity上找到。

五、小结

CVE-2020-15782漏洞可以绕过通常工程代码运行的沙箱，直接访问设备的内存，从而在西门子S7 PLC上获得本机代码执行。Claroty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，并可以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。需要特别注意的是，该漏洞如果被攻击者利用发起恶意攻击，将很难被检测发现。该项成果披露是西门子和Claroty公司紧密合作的结果，这有利于促进工业网络安全行业和工业设备供应商在漏洞披露方面的合作，也有利于整个工业生态系统的安全。