温州地区西门子模块代理

产品名称	温州地区西门子模块代理
公司名称	浔之漫智控技术（上海）有限公司
价格	.00/件
规格参数	
公司地址	上海市松江区广富林路4855弄88号3楼
联系电话	158****1992 158****1992

产品详情

温州地区西门子模块代理

西门子2018年5月15日发布安全公告通知客户，其部分 SIMATIC S7-400 CPU
受严重的拒绝服务（DoS）漏洞影响，该漏洞编号为CVE-2018-4850，CVSS（V3.0）评分7.5分。

SIMATIC S7-400

SIMATIC S7-400 是西门子旗下的可编程逻辑控制器（PLC），专门用于工业环境中的过程控制。该产品广泛应用在汽车、机械设备制造、建筑设计、钢铁、发电配电、化工、仓储、食品和制药行业。西门子的PLC产品在我国也有着广泛的应用。

漏洞原理

漏洞原因在于受影响的 CPU 未正确验证 S7 通信数据包，从而允许远程攻击者触发 DoS
条件，可致系统进入并保持 DEFECT 模式，必须手动重启才能恢复。

攻击者成功利用该漏洞的前提是能够将特质的 S7 恶意通信数据包发送至 CPU
的通信接口，包括以太网、PROFIBUS
和多点接口（MPI）。值得注意的是，攻击者无需用户交互或获取特权就能利用该漏洞。

西门子指出，该漏洞可能会造成 CPU 的核心功能出现拒绝服务状态，从而影响系统的可用性。截至安全公告发布之时，西门子称未发现公开已知的利用案例。

影响范围

受影响的产品及版本为：

SIMATIC S7-400 (incl. F) CPU 硬件版本4.0及以下所有版本；

SIMATIC S7-400 (incl. F) CPU硬件版本5.0：所有5.2版本以下的所有固件版本；

SIMATIC S7-400H CPU硬件版本4.5及以下所有版本。

建议受影响的用户分别更新到硬件版本5.0、5.2和6.0。西门子表示，受影响的 SIMATIC S7-400 CPU 硬件版本已停产或已被淘汰。西门子建议客户升级到新版本或采用其提供的应对举措。

鉴于 DoS 漏洞会对工业环境造成严重的风险，建议组织机构尽快更新。

缓解建议

1. SIMATIC S7-400（含F）CPU模块硬件版本在

v4.0及以下版本

2. SIMATIC S7-400（含F）CPU模块硬件版本低于v5.0或

所有固件版本低于v5.2

3. SIMATIC S7-400H CPU模块硬件版本在v4.5及以下版本

补充建议

1.避免将控制设备或操作站暴露在互联网中，应用隔离设备确保外界无法从互联网直接访问工业设备。

2.远程设备与控制系统间部署工业网闸，并确保工业控制系统与办公信息网络完全分离。

3.操作站部署主机防护系统，避免其成为网络攻击的中转跳板。

4.必须进行远程访问时，请使用安全方法，例如使用虚拟专用网络（VPN），并同时确保VPN自身的安全性。

西门子S7-1500系列

其替代400系列的任务眼看就要完成。但是西门子那么多400库存不能眼看着砸在自己手里，所以只能用限制功能的方式来逐步完成1500的换代工作，所以在以前的1500版本中，是不支持冗余组态的。

西门子S7-400系列

情况在2018年下半年开始有所转机，西门子盘算了一下自己的400差不多库存销售完了，对自己可爱伶俐的小儿子开始更加溺宠了，连出了好几个型号来扩充其产品线，更是在新型号中破天荒的加入了冗余组态。

西门子S7-1500冗余配置

这是多么值得庆祝，多么值得欢呼的消息。曾经多少个项目跟业主签约的冗余系统只能含泪用400系列来完成，多么希望用博途来完成设计组态的任务而不得，只能默默地晚上加班加点的改写Step

7的程序块。现在终于跟以前说拜拜，开始享受博途编程带来的便利。

本次新增的产品型号有：CPU1513R、 CPU1515R和CPU1517H这三种，其中CPU1513R、CPU1515R适用于中小型项目，CPU1517H适用于大型项目，当然价格也是不菲。

在这三种型号中，CPU1513R 和 CPU1515R一般适用于中小型项目。冗余组态时其中一个CPU模块失效，备用CPU模块就会自动接管控制功能，可以做到快速切换，以防止数据丢失，防止控制失效。PROFINET总线的冗余组态通讯方式还可以提高设备的可用性。

西门子那些支持Profinet S2冗余控制功能的现场远程IO设备（例如ET 200SP/MP）通过PROFINET连接到冗余CPU结构中，构成PROFINET冗余通讯，即便是网络发生了中断的情况，现场设备也能继续工作而不会出现错误。

这三种型号中的CPU1517H性能更强，适用于大型项目的应用。该CPU有专用的光纤同步模块，可以实现冗余系统的快速、平滑切换。在以后，CPU1517H还将会支持PROFINET冗余网络。

CPU6ES7 211-0AA23-0XB0 CPU221 DC/DC/DC,6输入/4输出6ES7 211-0BA23-0XB0
CPU221 继电器输出,6输入/4输出6ES7 212-1AB23-0XB8
CPU222 DC/DC/DC,8输入/6输出6ES7 212-1BB23-0XB8
CPU222 继电器输出,8输入/6输出6ES7 214-1AD23-0XB8
CPU224 DC/DC/DC,14输入/10输出6ES7 214-1BD23-0XB8
CPU224 继电器输出,14输入/10输出6ES7 214-2AD23-0XB8
CPU224XP DC/DC/DC,14DI/10DO,2AI/1AO(PNP)6ES7 214-2AS23-0XB8
CPU224XPsi DC/DC/DC,14DI/10DO,2AI/1AO(NPN)6ES7 214-2BD23-0XB8
CPU224XP 继电器输出,14DI/10DO,2AI/1AO6ES7 216-2AD23-0XB8
CPU226 DC/DC/DC,24输入/16输出6ES7 216-2BD23-0XB8 CPU226 继电器输出,24输入/16输出