SIEMENS云南省昆明市西门子（授权）中国总代理-西门子西南地区一级总代理商

产品名称	SIEMENS云南省昆明市西门子（授权）中国总代理-西门子西南地区一级总代理商
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

????TIA?PLC?????????????????PLC?????????????????????????????????
??????????/?????????????????PLC??????????????

下面介绍密钥生成算法流程：

图6 密钥生成算法

主机(TIA)随机生成20字节的PreKey，使用类椭圆曲线加密算法和公钥加密PreKey，作为Keying materaial 1(对应图7中M3数据包的EG1、EG2)。

主机(TIA)根据PreKey计算KDF，并由此生成CEK(Checksum Encryption Key)，CS(Checksum Seed)，KEK(Key Encryption Key)。

主机(TIA)将Challenge和KDK相结合，使用AES-CTR加密算法和KEK进行加密，其结果作为Keying material 3(对应M3数据包中的EncryptedChallenge和EncryptedKDK)。

主机(TIA)用CS和Keying material 3进行哈希运算(Tabulation Hash),得到结果TB-HASH。

主机(TIA)使用AES-ECB算法和CEK来加密TB-HASH并得到结果Keying material

2(对应M3数据包中的EncryptedChecksum)。

图7 M3数据包结构

4.漏洞复现

???OMSp_core_managed.dll??stop???????????PLC S7-1500?????

??????PLC S7-1500??????????????????

?? ???PLC????

????????PLC S7-1500??????????PLC?????PLC????????

?? ???PLC????