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	湖南西控自动化设备有限公司
价格	.00/件
规格参数	
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	15344432716 15386422716

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 materaial1(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(ChecksumSeed)，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 material3(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(TabulationHash),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 material2(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???????????PLCS7-1500?????

??????PLC S7-1500???????????????8???

?8 ???PLC????

????????PLC S7-1500???????????PLC?????PLC????9???

?9 ???PLC????