



# S7

📅 2021-09-01 | 📁 Challenge , 2021 , 工业信息安全技能大赛 , 巡回赛-杭州站

Challenge | 2021 | 工业信息安全技能大赛 | 巡回赛-杭州站 | S7

[点击此处](#)获得更好的阅读体验

## WriteUp来源

来自 **Venom** 战队

## 题目描述

工业协议中存在异常数据。请通过流量中的数据找寻 flag，flag形式为 flag{}。提交时请提交括号内内容。

## 题目考点

- 流量分析
- S7Comm协议

## 解题思路

过滤 `s7comm-plus.data.function == createobject`，发现有写操作

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

s7comm-plus.data.function == createobject

	Destination	Protocol	Length	Info
52	192.168.103.26	S7COMM-PLUS	370	+60132 Ver:[V3] Seq=421 [Req CreateObject] Unknown (962) Cl
5	192.168.103.252	S7COMM-PLUS	130	+60132 Ver:[V3] Seq=421 [Res CreateObject] Retval=OK ObjId=
52	192.168.103.26	S7COMM-PLUS	206	+60132 Ver:[V3] Seq=436 [Req CreateObject] Unknown (923) Se
5	192.168.103.252	S7COMM-PLUS	125	+60132 Ver:[V3] Seq=436 [Res CreateObject] Retval=OK ObjId=
52	192.168.103.26	S7COMM-PLUS	370	+60132 Ver:[V3] Seq=437 [Req CreateObject] Unknown (962) Cl
5	192.168.103.252	S7COMM-PLUS	130	+60132 Ver:[V3] Seq=437 [Res CreateObject] Retval=OK ObjId=
52	192.168.103.26	S7COMM-PLUS	208	+60132 Ver:[V3] Seq=456 [Req CreateObject] Unknown (923) Se
5	192.168.103.252	S7COMM-PLUS	125	+60132 Ver:[V3] Seq=456 [Res CreateObject] Retval=OK ObjId=
52	192.168.103.26	S7COMM-PLUS	370	+60132 Ver:[V3] Seq=457 [Req CreateObject] Unknown (962) Cl
5	192.168.103.252	S7COMM-PLUS	130	+60132 Ver:[V3] Seq=457 [Res CreateObject] Retval=OK ObjId=
52	192.168.103.26	S7COMM-PLUS	208	+60132 Ver:[V3] Seq=473 [Req CreateObject] Unknown (923) Se
5	192.168.103.252	S7COMM-PLUS	125	+60132 Ver:[V3] Seq=473 [Res CreateObject] Retval=OK ObjId=

Element Tag-Id: Start of Object (0xa1)  
Relation Id: DynObjX7.255.49210  
Class Id: SessionTisJob.Class\_Rid  
> Class Flags: 0x00000000  
Attribute Id: None  
▼ Attribute  
Element Tag-Id: Attribute (0xa3)  
> Item Value: ID=ObjectVariableTypeName (WString) = TisModifyJob\_22  
▼ Attribute  
Element Tag-Id: Attribute (0xa3)  
> Item Value: ID=AbstractTisJob.Request (Blob) = 0x401432038c10040305d0040a0606040000794c  
▼ Attribute  
Element Tag-Id: Attribute (0xa3)  
> Item Value: ID=AbstractTisJob.Trigger (Blob) = 0x11030000167e38e4a03100  
Element Tag-Id: Terminating Object (0xa2)  
Data unknown: 00000000  
> Trailer: Protocol version=V3

0000	72 03 00 8b 20 53 22 76 10 83 eb dd c5 51 ba 72	r... S"v .....Q..r
0010	1b cb e3 34 33 31 a4 1d b7 75 fe 23 b4 ea 77 ff	...431.. .u.#...w.
0020	16 7f d8 97 4c 31 00 00 04 ca 00 00 01 d9 00 00	....L1.. ....
0030	03 9b 36 00 00 03 9b 00 04 00 00 00 00 82 7b	..6..... .....{
0040	a1 7f ff c0 3a 95 15 00 00 a3 81 69 00 15 0f 54	..... .i...T
0050	69 73 4d 6f 64 69 66 79 4a 6f 62 5f 32 32 a3 95	isModify Job_22..
0060	05 00 14 00 13 40 14 32 03 8c 10 04 03 05 d0 04	.....@.2 .....
0070	0a 06 06 04 00 00 70 4c a3 95 06 00 14 00 0b 11	.....pL .....
0080	03 00 00 16 7e 38 e4 a0 31 00 a2 00 00 00 00 72	.....8.. 1.....r
0090	03 00 00	...

CTFHub

添加过滤条件 `s7comm-plus.data.opcode == 0x31` , 筛选写操作数据

https://writeup.ctfhub.com/Challenge/2021/工业信息安全技能大赛/巡回赛-杭州站/mJg7zCJ4CgQiDCWgwmyShU.html

2/4

文件(F) 编辑(E) 视图(V) 刷新(S) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(I) 帮助(H)

s7comm-plus.data.function == createobject and s7comm-plus.data.opcode == 0x31

Time	Source	Destination	Protocol	Length	Info
22016 93.088417	192.168.103.252	192.168.103.26	S7COMM-PLUS	273	+60132 Ver:[V3] Seq=247 [Req CreateObject] Unknown (923) Se
22020 93.132414	192.168.103.252	192.168.103.26	S7COMM-PLUS	372	+60132 Ver:[V3] Seq=248 [Req CreateObject] Unknown (962) Cl
24112 118.266988	192.168.103.252	192.168.103.26	S7COMM-PLUS	298	+60136 Ver:[V1] Seq=1 [Req CreateObject] ObjectServerSessio
24640 122.277213	192.168.103.252	192.168.103.26	S7COMM-PLUS	379	+60136 Ver:[V3] (S7COMM-PLUS reassembled) Seq=23 [Req Creati
24657 122.386349	192.168.103.252	192.168.103.26	S7COMM-PLUS/XML	748	+60136 Ver:[V3] (S7COMM-PLUS reassembled) Seq=25 [Req Creati
24674 122.544026	192.168.103.252	192.168.103.26	S7COMM-PLUS	1514	+60136 Ver:[V3] (S7COMM-PLUS inner fragment)   +60136 Ver:[
25610 131.584110	192.168.103.252	192.168.103.26	S7COMM-PLUS	273	+60132 Ver:[V3] Seq=306 [Req CreateObject] Unknown (923) Se
25614 131.624042	192.168.103.252	192.168.103.26	S7COMM-PLUS	372	+60132 Ver:[V3] Seq=307 [Req CreateObject] Unknown (962) Cl
27002 144.225998	192.168.103.252	192.168.103.26	S7COMM-PLUS	208	+60132 Ver:[V3] Seq=355 [Req CreateObject] Unknown (923) Se
27019 144.288793	192.168.103.252	192.168.103.26	S7COMM-PLUS	370	+60132 Ver:[V3] Seq=356 [Req CreateObject] Unknown (962) Cl
27540 150.165196	192.168.103.252	192.168.103.26	S7COMM-PLUS	208	+60132 Ver:[V3] Seq=381 [Req CreateObject] Unknown (923) Se
27547 150.206087	192.168.103.252	192.168.103.26	S7COMM-PLUS	370	+60132 Ver:[V3] Seq=382 [Req CreateObject] Unknown (962) Cl

Element Tag-Id: Start of Object (0xa1)  
Relation Id: DynObjX7.255.49192  
Class Id: SessionTisJob.Class\_Rid  
Class Flags: 0x00000000  
Attribute Id: None  
Attribute  
Element Tag-Id: Attribute (0xa3)  
Item Value: ID=ObjectVariableTypeName (WString) = TisModifyJob\_16  
Attribute  
Element Tag-Id: Attribute (0xa3)  
Item Value: ID=AbstractTisJob.Request (Blob) = 0x401432038c10040305d0040606060400005a6d  
ID Number: AbstractTisJob.Request  
Datatype flags: 0x00  
Datatype: Blob (0x14)  
Blob root ID: None  
Blob size: 19  
Value: 401432038c10040305d0040606060400005a6d

72 03 00 8b 20 6c 95 59 d2 d1 45 31 fa 7c 8a 01 r... 1.Y ..E1.|..  
30 d1 3b 15 17 bc b0 d5 62 f2 a1 cc b3 1c be c9 0.;.... b.....  
9e f0 f3 f6 d3 31 00 00 04 ca 00 00 01 63 00 00 .....1.. ....c..  
03 9b 36 00 00 03 9b 00 04 00 00 00 00 82 11 .....6.....  
a1 7f ff c0 28 95 15 00 00 a3 81 69 00 15 0f 54 ....(.. ..i...T  
69 73 4d 6f 64 69 66 79 4a 6f 62 5f 31 36 a3 95 isModify Job\_16..  
05 00 14 00 13 40 14 32 03 8c 10 04 03 05 d0 04 .....0..2.....  
06 06 06 04 00 00 5a 6d a3 95 06 00 14 00 0b 11 .....Zm.....  
03 00 00 10 7e 38 e4 a0 31 00 a2 00 00 00 00 72 .....8.. 1.....r  
03 00 00 .....

CTFHub

得到字符串 ZmxhZ3s5d3pLc0x0bVdmWVduTk00fQ

Base解密得到flag

## Flag

1 flag{9wzKsLtmWfYWnNM4}

本文作者：CTFHub

本文链接：<https://writeup.ctfhub.com/Challenge/2021/工业信息安全技能大赛/巡回赛-杭州站/mJg7zCJ4CgQiDCWgwmyShU.html>

版权声明： 本博客所有文章除特别声明外，均采用 [CC BY-NC-SA](#) 许可协议。 转载请注明出处！

# Challenge

# 2021

# 工业信息安全技能大赛

# 巡回赛-杭州站

© 2019 – 2022 ❤ CTFHub  
由 [Hexo](#) & [NexT.Gemini](#) 强力驱动