西门子DOS攻击事件

发表于 2021-01-25 更新于 2021-02-21 分类于 Challenge ， 2019 ， 工业信息安全技能大赛 ， 哈尔滨站
Challenge | 2019 | 工业信息安全技能大赛 | 哈尔滨站 | 西门子DOS攻击事件

点击此处获得更好的阅读体验

WriteUp来源

https://www.cnpanda.net/ctf/415.html

shuaitong提供补充

题目描述

> *样本中包含针对西门子工控设备的DOS攻击模式，请分析出发送怎样的UDP数据会使设备宕机。flag格式flag{}*

题目考点

- *CVE-2015-5374*

解题思路

使用IDA反汇编题目文件，发现可疑字符串crash，共两处引用

从该文件无法得到题目要求的UDP数据流

搜索西门子Dos攻击事件，找到了这篇文章https://zhuanlan.zhihu.com/p/27428923

经过分析得知题目中给的是Launcher模块，题目要求是宕机，根据文章中

> *攻击者武器库中的另一工具是拒绝服务（DoS）工具，可以用来对付西门子SIPROTEC设备，该工具利用了CVE-2015-5374漏洞，目标是使设备无法响应。一旦漏洞被成功利用，目标机器将会停止任何命令响应，直到手动重启。*

留意到此处代码，确定题目文件为Industroyer工控恶意软件Launcher模块。而其中的udp包发生在利用DOS攻击漏洞CVE-2015-5374阶段，去GitHub搜索了CVE-2015-5374的Payload，从而得到最终答案。

Flag

```
1 flag{1149000000000000000000000000000289E}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2019/工业信息安全技能大赛/哈尔滨站/fcHcoYAb9CbRpbUkkv62p3.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # 2019 # 工业信息安全技能大赛 # 哈尔滨站
黑客的大意
Tesla工业APP分析