

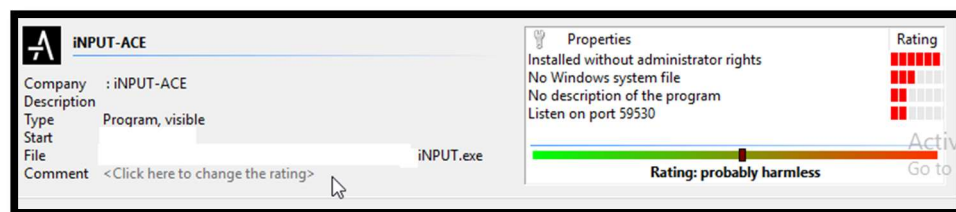
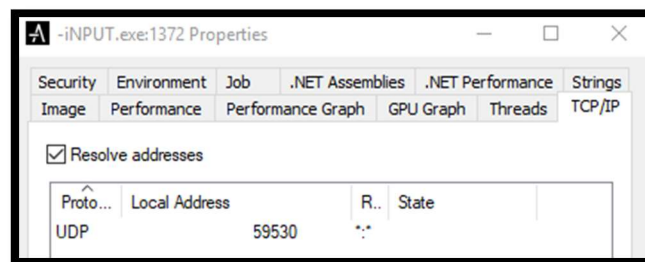
-INPUT-ACE Version 2.2.1

(Review)

Description: This is a review of the -iNPUT-ACE version 2.2.1. The software has a vulnerability that could lead to a denial-of-service (DoS) using a User Datagram Protocol (UDP) flood attack¹. Other types of attacks using UDP ports may be available.

1. UDP Flood Attack

1.1 The software relies in the use of an UDP port (e.g. 59530):



1.2 The port has an open status with a filtered status:



¹ https://en.wikipedia.org/wiki/UDP_flood_attack

1.3 Then it is possible to send packages to the target port (e.g. 59530) using strings (e.g. “xxx”):

```
UDP Flood uses
Enter target:
Enter target port (defaults to 80):
59530
Using Port 59530
Enter random string (data to send):
xxx

Starting UDP Flood.
```

1.4 Confirm the flood in the victim machine (Length:3):

[illegible]

1.5 To finally, suspend the software process and others under execution in the victim machine.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Suspended						
		81,080 K	148,932 K	4696		
Suspended						
		5,848 K	24,680 K	5184		
		5,188 K	22,308 K	2072		
		19,820 K	44,828 K	3968		
iNPUT.exe	Suspended	108,348 K	158,480 K	1372	iNPUT-ACE	

1.6 There is the possibility also to replicate the attack over a Transmission Control Protocol (TCP) as well by using the Remote Address and Remote Port information.

