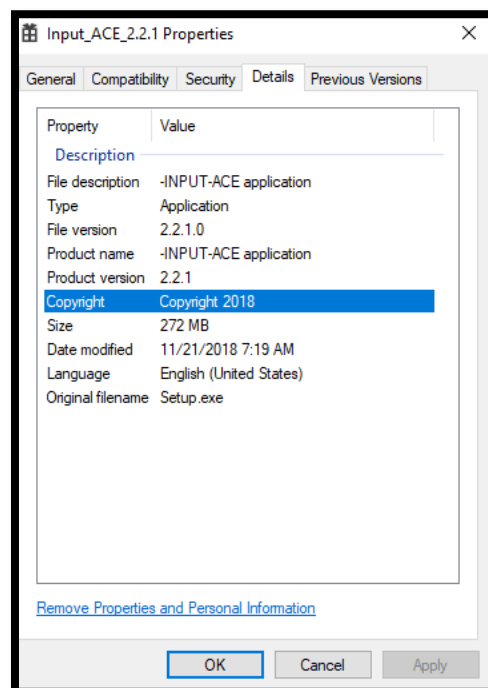


-INPUT-ACE Version 2.2.1

January 21st, 2019.

Description: This is an assessment of the -INPUT-ACE version 2.2.1. This evaluation found vulnerabilities related to a possible buffer overflow¹ and a denial-of-service (DoS) using a User Datagram Protocol (UDP) flood attack². The UDP flood attack targeted the specific port in use by the software, instead of a flood around random ports on a remote host. As a result, the software achieved a status “suspended”.

1. File identification:



¹ <https://security.radware.com/ddos-knowledge-center/ddospedia/buffer-overflow-attack/>

² https://en.wikipedia.org/wiki/UDP_flood_attack

2. General security indicators:

The dos-stub message is missing
The size of the resource (DATA.131) is bigger than the max (512000 bytes) threshold
The size of the resource (DATA.131) is bigger than the max (512000 bytes) threshold
The file contains another file (type: PKZIP, location: resources, file-offset: 0x0002B310)
The file references (1) blacklisted library
The file references (1) Windows built-in privilege(s)
The size (285944320 bytes) of the file is suspicious
The online scoring service is not reachable
The signature of the resource (FLAGS:132) is unknown
The file-ratio (99%) of the resources is suspicious
The file imports (5) anonymous function(s)
The file imports (34) blacklisted function(s)

2.1 The ASLR³ and DEP⁴ are enabled, however the CFG is disabled⁵.

address-space-layout-randomization (ASLR)	true
Code Integrity	false
data-execution-prevention (DEP)	true
Image Isolation	true
structured-exception-handling (SEH)	true
Image Bound	true
windows-driver-model (WDM)	false
terminal-server-aware	true
control-flow-guard (CFG)	false

2.2 Resources shows a compressed file:

file-offset ...	signature	non-standard	size (285773616 byt	file-ratio (99.94%)	md5	entropy
0x110B3B4C	Version	-	788	0.00 %	103C00A3979359D321798AF5E8BFFD2B	3.396
0x110B3278	String-table	-	1048	0.00 %	B3929F22874681B61A010F8F75F65FD1	3.426
0x110B3690	String-table	-	1138	0.00 %	8A1122B792CB09A177BB9C04E0BE76B8	3.322
0x110B3E60	Manifest	-	999	0.00 %	CBF1999E86CC16EECF938CD04AF0D4C6	5.320
0x110B3B04	Icon-group	-	34	0.00 %	E9EF6E365B9E8C9654A9ECE0C4EA75D0	2.374
0x110B3B28	Icon-group	-	34	0.00 %	CF3085EA1B910041CAF08EDC245B714A	2.492
0x110B1B58	Icon	-	744	0.00 %	9672B12784736875DE8A7A86503B8D7D	2.933
0x110B1E40	Icon	-	2216	0.00 %	FD881FE96555C23177AEA9A3369E20A6	2.147
0x110B26E8	Icon	-	744	0.00 %	9672B12784736875DE8A7A86503B8D7D	2.933
0x110B29D0	Icon	-	2216	0.00 %	FD881FE96555C23177AEA9A3369E20A6	2.147
0x110B1B4C	unknown	x	12	0.00 %	B68200A712BCEAD87897DECA6A51F2B0	1.947
0x0002B310	PKZIP	x	285763643	99.94 %	AC49C2D1FB98C3A0EE2D5387D59A3747	7.999

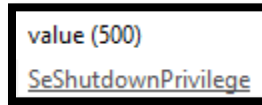
³ https://en.wikipedia.org/wiki/Address_space_layout_randomization

⁴ <https://support.microsoft.com/en-ca/help/875352/a-detailed-description-of-the-data-execution-prevention-dep-feature-in>

⁵ <https://docs.microsoft.com/en-us/windows/desktop/secbp/control-flow-guard>

2.3 Windows built-in privilege

In the strings, it is possible to locate one possible Windows built-in privilege constant: SeShutdownPrivilege⁶.



```
value (500)  
SeShutdownPrivilege
```

⁶ <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/shut-down-the-system>

3. Buffer Overflow

3.1 The buffer overflow was observed as following:

10:42:..	hINPUT.exe	1676	QueryAllInforma...C:\Users\input-ace\AppData\Local\INPUT\app-2.2.1\Autofac.dll	BUFFER OVERFLOW
10:42:..	hINPUT.exe	1676	QueryAllInforma...C:\Users\input-ace\AppData\Local\INPUT\app-2.2.1\Autofac.Extensions.DependencyInjection.dll	BUFFER OVERFLOW
10:42:..	hINPUT.exe	1676	QueryAllInforma...C:\Users\input-ace\AppData\Local\INPUT\app-2.2.1\System.Runtime.dll	BUFFER OVERFLOW
10:42:..	hINPUT.exe	1676	QueryAllInforma...C:\Users\input-ace\AppData\Local\INPUT\app-2.2.1\System.ComponentModel.dll	BUFFER OVERFLOW
10:42:..	hINPUT.exe	1676	QueryAllInforma...C:\Users\input-ace\AppData\Local\INPUT\app-2.2.1\System.Reflection.dll	BUFFER OVERFLOW
10:42:..	hINPUT.exe	1676	QueryAllInforma...C:\Users\input-ace\AppData\Local\INPUT\app-2.2.1\GalaSoft.MvvmLight.dll	BUFFER OVERFLOW
10:42:..	hINPUT.exe	1676	QueryAllInforma...C:\Users\input-ace\AppData\Local\INPUT\app-2.2.1\System.ObjectModel.dll	BUFFER OVERFLOW
10:42:..	hINPUT.exe	1676	QueryAllInforma...C:\Users\input-ace\AppData\Local\INPUT\app-2.2.1\MahApps.Metro.dll	BUFFER OVERFLOW
10:42:..	hINPUT.exe	1676	QueryAllInforma...C:\Users\input-ace\AppData\Local\INPUT\app-2.2.1\Newtonsoft.Json.dll	BUFFER OVERFLOW
10:42:..	hINPUT.exe	1676	QuerySecurityFile C:\Users\input-ace\AppData\Local\INPUT\app-2.2.1\Newtonsoft.Json.dll	BUFFER OVERFLOW
10:42:..	hINPUT.exe	1676	QueryAllInforma...C:\Users\input-ace\AppData\Local\INPUT\app-2.2.1\INPUT.Common.dll	BUFFER OVERFLOW
10:42:..	hINPUT.exe	1676	QueryAllInforma...C:\Users\input-ace\AppData\Local\INPUT\app-2.2.1\Telerik.Windows.Diagrams.Core.dll	BUFFER OVERFLOW
10:42:..	hINPUT.exe	1676	QueryAllInforma...C:\Users\input-ace\AppData\Local\INPUT\app-2.2.1\NLog.dll	BUFFER OVERFLOW
10:42:..	hINPUT.exe	1676	QueryAllInforma...C:\Users\input-ace\AppData\Local\INPUT\app-2.2.1\System.Windows.Interactivity.dll	BUFFER OVERFLOW
10:42:..	hINPUT.exe	1676	QueryAllInforma...C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.ComponentModel.DataAnnotations\v4...	BUFFER OVERFLOW
10:42:..	hINPUT.exe	1676	QueryAllInforma...C:\Users\input-ace\AppData\Local\INPUT\app-2.2.1\Telerik.Windows.Documents.dll	BUFFER OVERFLOW
10:42:..	hINPUT.exe	1676	QueryAllInforma...C:\Users\input-ace\AppData\Local\INPUT\app-2.2.1\OpenCvSharp.dll	BUFFER OVERFLOW
10:42:..	hINPUT.exe	1676	QueryAllInforma...C:\Users\input-ace\AppData\Local\INPUT\app-2.2.1\System.Net.Http.dll	BUFFER OVERFLOW
10:42:..	hINPUT.exe	1676	QueryAllInforma...C:\Users\input-ace\AppData\Local\INPUT\app-2.2.1\Microsoft.ApplicationInsights.dll	BUFFER OVERFLOW
10:42:..	hINPUT.exe	1676	QueryAllInforma...C:\Users\input-ace\AppData\Local\INPUT\app-2.2.1\Squirrel.dll	BUFFER OVERFLOW
10:42:..	hINPUT.exe	1676	QueryAllInforma...C:\Users\input-ace\AppData\Local\INPUT\app-2.2.1\Splat.dll	BUFFER OVERFLOW
10:42:..	hINPUT.exe	1676	QueryAllInforma...C:\Users\input-ace\AppData\Local\INPUT\app-2.2.1\DVParser.dll	BUFFER OVERFLOW
10:42:..	hINPUT.exe	1676	QueryAllInforma...C:\Users\input-ace\AppData\Local\INPUT\app-2.2.1\System.IO.Compression.dll	BUFFER OVERFLOW
10:42:..	hINPUT.exe	1676	QueryAllInforma...C:\Users\input-ace\AppData\Local\INPUT\app-2.2.1\Telerik.Windows.Controls.dll	BUFFER OVERFLOW
10:42:..	hINPUT.exe	1676	QueryAllInforma...C:\Users\input-ace\AppData\Local\INPUT\app-2.2.1\Telerik.Windows.Documents.Core.dll	BUFFER OVERFLOW
10:42:..	hINPUT.exe	1676	QueryAllInforma...C:\Users\input-ace\AppData\Local\INPUT\app-2.2.1\protobuf-net.dll	BUFFER OVERFLOW

Even with the CFG enabled.

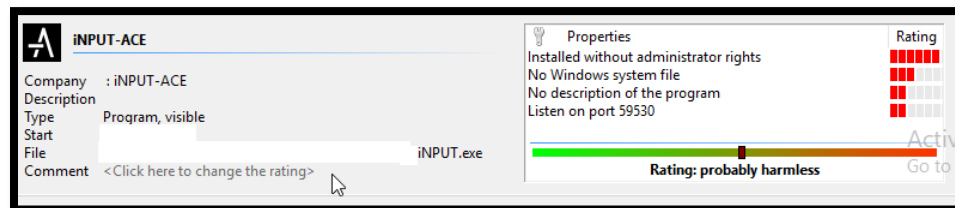
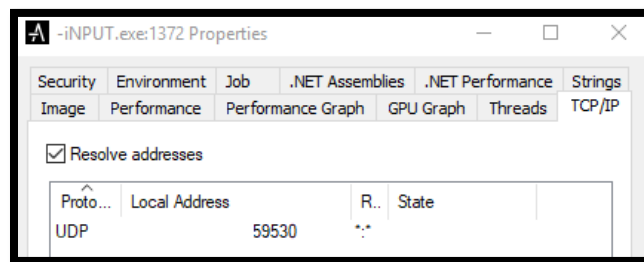
The screenshot shows the Windows Defender Security Center interface. The 'Exploit protection' section is active, displaying 'System settings' and 'Program settings'. Under 'Control flow guard (CFG)', the setting 'Ensures control flow integrity for indirect calls.' is shown with a dropdown menu set to 'Use default (On)'. Below this, 'Data Execution Prevention (DEP)' is also shown as 'On'. The 'Export settings' link is visible. In the background, the Task Manager window is open, showing the 'Process' tab with 'hINPUT.exe' selected, displaying its PID (1312), Private Bytes (97.876 K), Working Set (156.896 K), and Company Name (INPUT-ACE).

3.2 By checking the memory dump was observed some possible concerns that could be related to the buffer size⁷:

```
~/$ Input_ACE_2.2.1.exe
dump: bad read buffer size
```

4. UDP Flood Attack

4.1 The software relies in the use of an UDP port:



4.2 The port has an open status:

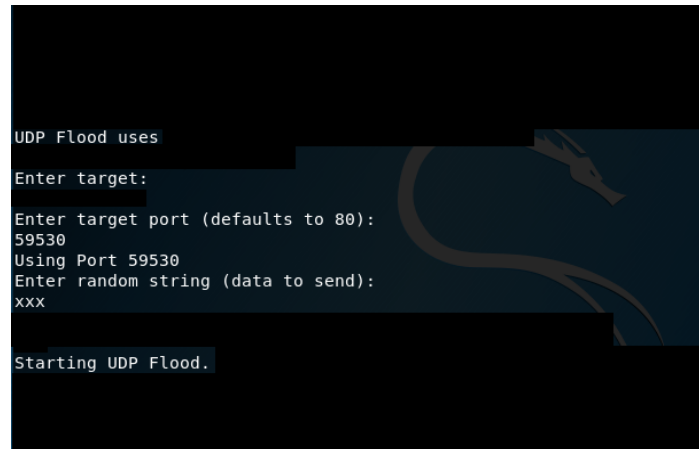
```
root@ :~# 59530
Starting

PORT      STATE      SERVICE
59530/udp open|filtered unknown
MAC Address:

13.60 seconds
root@ :~#
```

⁷ <https://cwe.mitre.org/data/definitions/131.html>

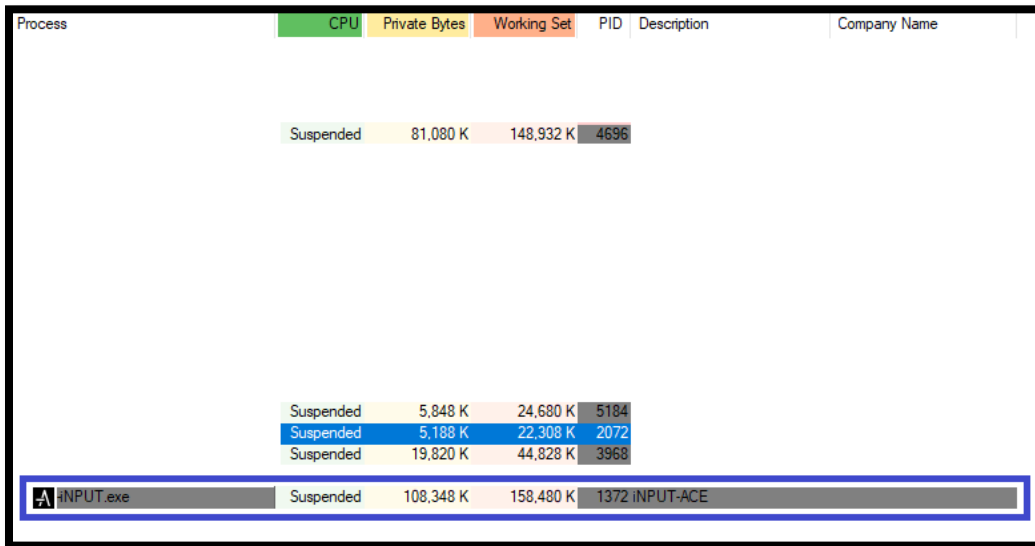
4.3 Then it is possible to send packages to this port:



4.4 Confirm the flood in the victim machine

The screenshot shows the Windows Task Manager application with the 'Performance' tab selected. The 'CPU' section is highlighted, showing 100% usage. Below this, a list of processes is displayed, with 'System Idle Process' at the top (0% CPU) and 'smss.exe' at the bottom (100% CPU). The 'smss.exe' process is highlighted in blue. The 'Details' pane on the right shows the 'smss.exe' process details, including its PID (4), PPID (0), and Name (smss.exe).

4.5 To finally, suspend the software process 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		
Suspended		5,188 K	22,308 K	2072		
Suspended		19,820 K	44,828 K	3968		
INPUT.exe	Suspended	108,348 K	158,480 K	1372	INPUT-ACE	

4.6 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.

