Multiple Vulnerability Disclosure in Avast AntiVirus (RPC Service)

Tested Environment

OS: Windows 7 Ultimate 32Bit (6.1, Build 7601), Windows 10 Pro 32Bit (10, Build 18363)
VM: Virtual Box

1. Windows 7 Ultimate 32Bit (6.1, Build 7601):

```
Avast Antivirus Type Avast Free AntiVirus
Avast Antivirus Version: 19.8.2393 (build 19.8.4793.545)
UI Version: 1.0.437
AvastSvc Service Version: 19.8.4793.0
```

2. Windows 10 Pro 32Bit (10, Build 18363)

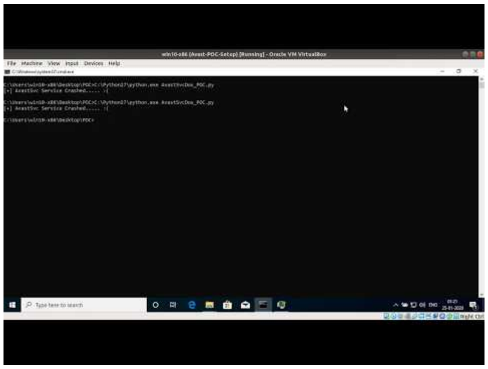
```
Avast Antivirus Type: Avast Free AntiVirus, Avast Premium Security
Avast Antivirus Version: 19.8.2393 (build 19.8.4257.552)
UI Version: 1.0.409
AvastSvc  Service Version: 19.8.4793.0
```

CVE-2020-10860: Arbitrary Memory Address Overwrite Vulnerability in the Avast Log Library

An issue was discovered in Avast Antivirus before 20. An Arbitrary Memory Address Overwrite vulnerability in the aswAvLog Log Library results in Denial of Service of the Avast Service (AvastSvc.exe).

Demo:

1. Free Avast Antivirus

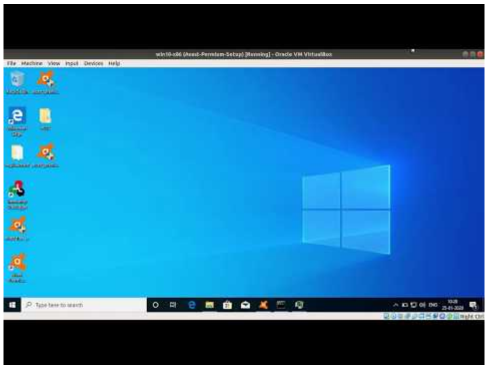

win10-x86 (Avast-POC-Setup) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
C:\Windows\system32\cmd.exe
Type here to search

```
C:\Users\win10-x86\Desktop\POC>C:\Python27\python.exe AvastSvcDos_POC.py
[+] AvastSvc Service Crashed..... :(

C:\Users\win10-x86\Desktop\POC>C:\Python27\python.exe AvastSvcDos_POC.py
[+] AvastSvc Service Crashed..... :(

C:\Users\win10-x86\Desktop\POC>
```

2. Premium Avast Antivirus


win10-x86 (Avast-Permium-Setup) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Type here to search

3. Disable SelfDefense Protection from untrusted application

[CVE-2020-10861](): Arbitrary File Deletion

An issue was discovered in Avast Antivirus before 20.The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to achieve Arbitrary File Deletion from Avast Program Path via RPC, when Self Defense is Enabled

CVE-2020-10862: Local Privilege Escalation (LPE)

An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to achieve Local Privilege Escalation (LPE) via RPC.

CVE-2020-10863: Execute TempShutDownMachine via RPC

An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to trigger a shutdown via RPC from a Low Integrity process via TempShutDownMachine.

CVE-2020-10864: Execcute Reboot via RPC

An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to trigger a reboot via RPC from a Low Integrity process.

CVE-2020-10865: Arbitary read/write Stats.ini file

An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to make arbitrary changes to the Components section of the Stats.ini file via RPC from a Low Integrity process

CVE-2020-10866: Enumerate Network Interface and access points

An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to enumerate the network interfaces and access points from a Low Integrity process via RPC

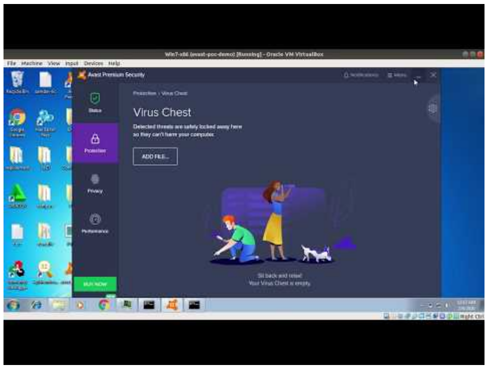
CVE-2020-10867: Perform Unauthorized action (task) from untrusted process

An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to bypass intended access restrictions on tasks from an untrusted process, when Self Defense is enabled.

CVE-2020-10868: Launch Repair app via RPC

An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to launch the Repair App RPC call from a Low Integrity process.

Demo



Virus Chest

Detected threats are safely locked away here so they can't harm your computer.

Sit back and relax! Your Virus Chest is empty.

Credits:

- Umar Farook: OSCE | Senior Security Analyst | Researcher
- FOS Team : Fools of Security

Support !

Email address: umarfarookmech712@gmail.com or pingus@foolsofsecurity.com
Youtube: Fools Of Security
Website: Fools Of Security Community

Reference:

Avast Release Notes
Free - AvastSvc Service (Arbitrary Memory Address Overwrite DOS)
Premium - AvastSvc Service (Arbitrary Memory Address Overwrite - DOS)
AvastSvc - Disable SelfDefense Protection from untrusted application
Local Privilege Escalation
Analysing RPC With Ghidra and Neo4 By xpnsec