

...

 History

...

### Tested Environment

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

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

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

Demo:

- 
- The screenshot shows a Windows Virtual Machine window titled "win10-kali (based on Proxmox) (running) - Oracle VM VirtualBox". Inside the VM, a Kali Linux terminal is open with the following commands and output:
- ```

root@kali:~/Desktop# apt-get install dnsmasq
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
dnsmasq is already the newest version (2.8.4-3).
0 upgraded, 0 newly installed, 0 to remove and 0 not installed.

root@kali:~/Desktop# cp /etc/dnsmasq.conf /etc/dnsmasq.conf.bak
root@kali:~/Desktop# nano /etc/dnsmasq.conf
#
# This is a sample dnsmasq configuration file.  It contains several
# commented-out options.  To enable an option, uncomment the line.
# See also: http://thk-fs.org/files/dnsmasq/dnsmasq-tutorial.html
#
# Basic-configuration
#
# Listen on interface eth0
listen-address eth0

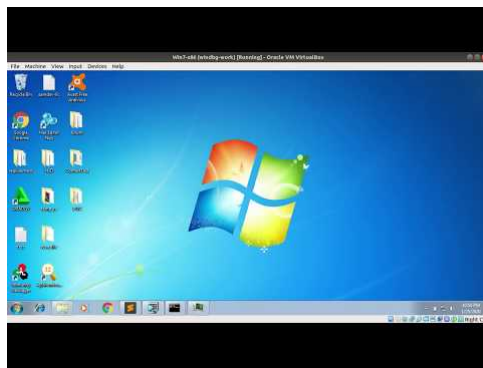
# Listen on the loopback interface
listen-address 127.0.0.1

# Use a dynamic list of nameservers
dynamic-servers=127.0.0.1:53,127.0.0.1:53

```
- The terminal window has a search bar at the bottom that says "Type here to search". The taskbar at the bottom of the VM shows various icons including a clock, network, volume, and application icons.

- 

- ### 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: Execute 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: Arbitrary 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

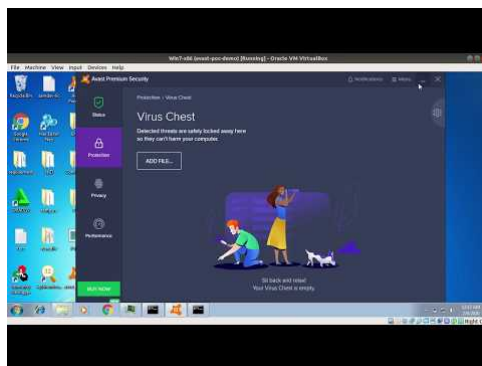
#### CVE-2020-10867: Perform Unauthorized action (task) from untrusted process

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



#### Credits:

- Umar Farook: [OSCE | Senior Security Analyst | Researcher](#)
- FOS Team : [Fools of Security](#)

#### Support !

Email address: [umarfarookmech712@gmail.com](mailto:umarfarookmech712@gmail.com) or [pingus@foolsofsecurity.com](mailto: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](#)