passtheticket Update pearsonvue-readme.md History

1 contributor

43 lines (31 sloc) | 1.51 KB

Pearson Vue VTS 2.3.1911 Installer - VUEApplicationWrapper Unquoted Service Path (CVE-2020-36154)

The Application Wrapper is the component that automates the Pearson VUE Testing System. The Wrapper is a scheduler that runs in the background on the test center's server. VUEApplicationWrapper service has an unquoted service path vulnerability and insecure file permissions on "\Pearson VUE" directory that allows to overwrite by everyone so that unauthorized local user can leverage privileges to VUEService user that has administrative rights.

Exploit: https://www.exploit-db.com/exploits/49143

```
#Detection of unquoted service path:

C:\Users\VUEService>wmic service get name, pathname, displayname, startmode| findstr /i "Auto" | findstr /i /v "C:\Windows\\" |
findstr /i "Pearson" |findstr /i /v """
VUE Application Wrapper
VUEApplicationWrapper C:\Pearson VUE\VUE
Testing System\bin\VUEWrapper.exe
Auto

C:\Users\VUEService>sc qc VUEApplicationWrapper
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: VUEApplicationWrapper
TYPE : 10 WIN32_OWN_PROCESS
START_TYPE : 2 AUTO_START
ERROR_CONTROL : 1 NORMAL
BINARY_PATH_NAME : C:\Pearson VUE\VUE TestingSystem\bin\VUEWrapper.exe
LOAD_ORDER_GROUP :
TAG : 0
DISPLAY_NAME : VUE Application Wrapper
DEPENDENCIES : lanmanworkstation
SERVICE_START_NAME : .\VUEService


#Detection of insecure file permissions:

PS C:\Users\VUEService> Get-Acl -Path "c:\Pearson Vue\"


Directory: C:\


Path Owner Access
---- ----- ------
Pearson Vue BUILTIN\Administrators Everyone Allow FullControl...
```