New issue

Jump to bottom

Feishu Untrusted Search Path Vulnerability #1

Open liong007 opened this issue on Oct 3 · 0 comments

liong007 commented on Oct 3 • edited Owner

CVE-2021-3305
Exploit Title：Feishu Untrusted Search Path Vulnerability
Date：1/25/2021
Exploit Author：YuanLirong 袁利荣
Vendor Homepage: https://www.feishu.cn/
Software Link:
https://sf3-eecdn-tos.pstatp.com/obj/ee-appcenter/3cd560/Feishu-3.40.3.exe
Version: 3.40.3 and 3.41.3
Tested on:Windows 10
POC:
DLL hijacking point TextInputFramework.dll test script

1. Place the DLL hijacking test file TextInputFramework.dll in the same directory as Feishu-3.40.3.exe;
2. Click to execute Feishu-3.40.3.exe, and also execute TextInputFramework.dll to pop up the calculator.

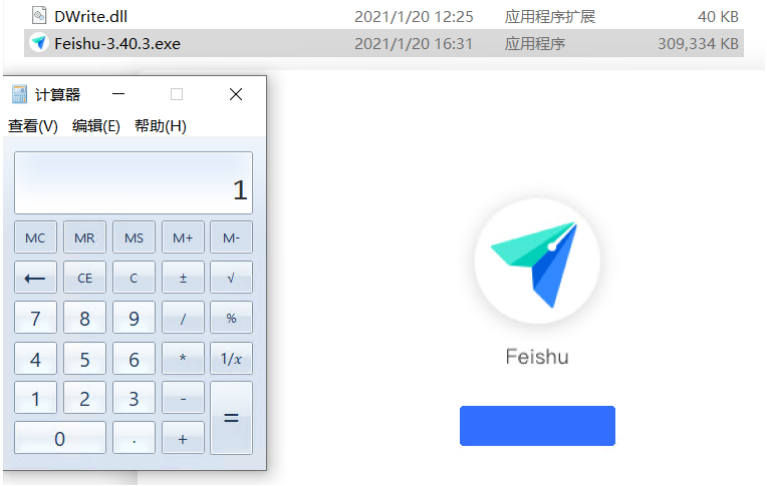
DLL hijacking point WindowsCodecs.dll test script

1. Put the DLL hijacking test file WindowsCodecs.dll in the same directory as Feishu-3.40.3.exe;
2. Click to execute Feishu-3.40.3.exe, and also execute WindowsCodecs.dll to pop up the calculator.

DLL hijacking point DWrite.dll test script

1. Put the DLL hijacking test file DWrite.dll in the same directory as Feishu-3.40.3.exe;

2. Click to execute Feishu-3.40.3.exe, and also execute DWrite.dll to pop up the calculator.



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant