

Document Number: NR-154525-TC

Version: Issue 1

# **Synaptics Security Advisory**

Synaptics-DisplayLink-privilege escalation vulnerability via a dynamic library sideloading -Internal Ref: PPDSYS-357

CVE: CVE-2023-4936

CVSS: 5.5 AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:H/A:L

CAPEC - CAPEC-184: Software Integrity Attack (Version 3.9)

#### Affected Drivers

File Description: Synaptics DisplayLink Installer

File Versions: Only the EXE variants of **DisplayLink USB Graphics Software for Windows** DisplayLink USB Graphics Software for Windows version 11.1 M1 and earlier,

 MSI and INF packages are not affected. This does -not- affect drivers loaded with Microsoft Windows Update (WU)

### **Impact**

It is possible to sideload a compromised DLL during the installation at elevated privilege.

## Background

The Synaptics /DisplayLink installer uses a standard installer executable setup.exe

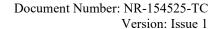
### **Technical Details**

An attacker creates folder with the same name as an executable but with .local suffix. Then create folders in that ".local" folder with the same name as folders in C:\Windows\WinSxS\x86\_microsoft.windows.common-controls\*. Then copy a malicious DLL into all of created folders as comctl32.dll.

If {executable\_name}.local folder/file is present next to executable, then DLL redirection mechanism kicks in and OS will look into \*.local folder when loading certain DLLs."

#### Acknowledgements

Synaptics would like to thank Krystian Nytko for reporting this issue.





# Vulnerable/fixed version information

Vulnerable Driver Family	Fixed Version (and later)	Driver Date
The EXE variants of all drivers	11.2M0	2023-10-06
prior to 11.2M0		

This table is applicable to all known PCs running Microsoft Windows OS. Drivers lower than fixed version should be considered vulnerable.