Realtek Semiconductor Corp.
No. 2, Innovation Road II,
Hsinchu Science Park, Hsinchu 300, Taiwan
Tel: +886-3-5780211; Fax: +886-3-5776047

Vulnerability Report

January 16, 2020

Realtek Audio Drivers for Windows – DLL preloading and potential Abuses (CVE-2019-19705)

Release Date
2019 Dec. 13th

Affected Projects
Realtek High definition audio driver

Affected Versions
Legacy (non-DCH type) driver 1.0.0.8855

CVE ID
CVE-2019-19705

Description
With Realtek High Definition Audio version 8855, the local user is able to gain privileges via a crafted DLL in the same folder as the running executable file.
The root cause is that Microsoft Visual Studio 2005 MFC is used in the named driver package (version 1.0.0.8855), which automatically loads a resource DLL. The VS2005 MFC uses a low-level function LdrLoadLibrary that also loads a code section, and thus there is a potential risk that unexpected code may be loaded.

Vulnerability Type
Insecure Permissions

Affected Component
Affected execution

Attack Type
Local

Impact Code Execution
True

Access Vector
Create a DLL with injection code and put it in the same folder of running execution file.

Realtek Semiconductor Corp.
No. 2, Innovation Road II,
Hsinchu Science Park, Hsinchu 300, Taiwan
Tel: +886-3-5780211; Fax: +886-3-5776047

Security Risk
High

Patch
Legacy (non-DCH) driver 1.0.0.8856