Synaptics Security Advisory

*** UNSUPPORTED WHEN ASSIGNED ***

Synaptics Audio Driver: CxUIUSvc Service for UWP Application
Elevation of Privileges Vulnerability

This vulnerability only affects products that have reached End-of-Life and are no longer supported.

CVE: CVE-2024-9157

CVSS 3.1 score 7.8(High) /AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS 4.0 score 8.6(High) /AV:L/AC:L/AT:N/PR:L/UI:P/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H

Affected Drivers

All audio driver packages which include CxUIUSvc64.exe or CxUIUSvc32.exe are affected.

Impact

The CxUIUSvc service, by creating a named pipe without setting a security descriptor restricting access to the pipe, allows any user to send data to the service. A carefully crafted message allows a DLL to be loaded into a process running at elevated privilege.

Background

The CxUIUSvc service creates a named pipe and reads data sent by the connected client. If the data contains a specific header followed by path and filename of a DLL, the service loads that DLL.

Technical Details

An attacker creates a pipe client and connects to the server end of the named pipe created by the service. The pipe client then writes data, which contains the path to a malicious DLL, to the pipe. The service loads the DLL, which could be specified by a client running with low privileges.

The DLL specified by a local authenticated attacker is then running in a privileged process, resulting in an Elevation of Privileges vulnerability.

Acknowledgements

Synaptics would like to thank Harrison Neal for reporting this issue.

Vulnerable driver version information

Known Vulnerable Driver Families
9.0.282.xxx
9.0.285.xx
9.0.278.xxx

Vulnerable APO Driver	Updated APO Driver
1.4.0.80	1.4.0.81

This table is applicable to all known vulnerable PCs.