# Synaptics Security Advisory

Synaptics Fingerprint Driver: Service for Hardware Support App - Use After Free

CVE: CVE-2023-5447

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

## Affected Drivers

File Description: Synaptics Hardware Support App Service for Fingerprint Driver

File Versions: All versions of SynHsaService included in fingerprint driver packages built prior to 19-Aug-2023 (see table below for details of fixed versions).

## Impact

Missing lock check in SynHsaService may create a use-after-free condition which causes abnormal termination of the service, resulting in denial of service for the Synaptics Hardware Support App.

## Background

The Synaptics Pre-boot Manager for the Fingerprint Driver is a Hardware Support App which connects to the service. In the case of abnormal termination of the service, the most likely impact is denial of service condition for the Pre-boot Manager application.

## Technical Details

An attacker-controlled application which calls SynHsaService interface methods concurrently can cause a race condition, which triggers a use-after-free vulnerability, due to lack of using a lock when accessing and freeing a pointer.

At this time, the only verified consequence and most likely impact of an exploit leveraging this vulnerability is a crash of the service, resulting in denial of service for the Synaptics Hardware Support App.

### Acknowledgements

Synaptics would like to thank Aobo Wang of Chaitin Security Research Lab for reporting this issue.

## Vulnerable/fixed version information

| Vulnerable Driver Family | Fixed Version (and later) | Driver Date |
|---|---|---|
| 6.0.xxx.1105 | 6.0.64.1105 | 2023-08-13 |
| 6.0.xxx.1136 | 6.0.39.1136 | 2023-08-19 |

This table is applicable to all known vulnerable PCs. Drivers where the xxx values are lower than the corresponding sub-minor version number in the fixed version should be considered vulnerable. For any other drivers that contain SynHsaService (SynRPCServer.exe) but are not in one of these version number families, please contact your PC manufacturer.