Synaptics Security Advisory

Synaptics Fingerprint Drivers that use SGX

CVE: CVE-2019-18619

CVSS: 7.1 (high) CVSS: 3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

Affected Drivers

WBF drivers using an SGX enclave (which contain a synaTee component) - All versions prior to 2019-11-30. See table for specific driver version numbers affected.

Fixed driver versions properly validate parameters passed into the enclave.

Impact

Incorrect parameter validation in the synaTee component of Synaptics WBF drivers using an SGX enclave (all versions prior to 2019-11-15) allows a local user to execute arbitrary code in the enclave (that can compromise confidentiality of enclave data) via APIs that accept invalid pointers.

Background

Certain Synaptics Fingerprint Drivers (especially those which perform fingerprint matching on the host) employ Intel's Software Guard eXtensions (SGX) to protect fingerprint and other sensitive data. A commonly used software design pattern for calling SGX functions, present in Synaptics' drivers, was found to be vulnerable to attack.

Technical Details

A common technique in API design is to pass pointers to a "context" block of information for the command to be processed. While the SGX SDK can validate pointers in a command itself, embedded pointers inside structures in the data are not validated.

The Synaptics SGX enclave code did not validate these embedded pointers properly. This allows an attacker to write data to enclave memory, which can be used to trigger execution of the attacker's code in the context of the enclave.

Once the attacker's code is running in the enclave, it can read or modify all data that the enclave has access to, including encrypted data which it protects.

Acknowledgements

Synaptics would like to thank Tobias Cloosters, Michael Rodler, Lucas Davi (University of Duisburg-Essen) for reporting this issue.

Affected Drivers and Fixed Versions[1]

Affected Version	Corresponding Fixed Version
5.2.225.26	5.2.227.26
5.2.318.26	5.2.321.26
5.2.3530.26	5.2.3540.26
5.3.3539.26	5.3.3542.26
5.5.15.1102	5.5.26.1102
5.5.11.1106	5.5.18.1106
5.5.3.1116	5.5.8.1116
5.5.2734.1050	5.5.2739.1050
5.5.2811.1050	5.5.2817.1050
5.5.38.1058	5.5.40.1058
5.5.10.1093	5.5.11.1093
5.6.23.1000	5.6.24.1000
6.0.32.1104	6.0.38.1104
6.0.42.1107	6.0.43.1107
6.0.14.1108	6.0.16.1108

Affected Drivers without fixed versions as of 2020-07-10 (contact OEM for updates)

Affected Version
5.2.524.26
5.5.2734.1050
5.5.2811.1050
5.5.8.1096

[1] Version numbers are of the form 5.5.VV.PPPP or 5.[1, 2, 3].PPVV.26, where the P digits indicate a product ID, and the V digits increment for each version.