Synaptics Security Advisory

Synaptics Fingerprint Driver – synaTEE.signed.dll Out-Of-Bounds Heap Write.

CVE: CVE-2021-3675

(Preliminary) CVSS: 5.5 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RC:R

Affected Drivers

File Description: Synaptics Fingerprint Driver Enclave

File Versions: All fingerprint driver versions that use synaTEE.signed.dll built prior to 26-Nov-2021 (see table below for details of fixed versions).

Impact

A carefully crafted command sent to the SGX Enclave of the driver can overwrite heap memory, causing a crash when the memory is freed, and potential confidentiality loss.

Background

synaTEE.signed.dll is an SGX enclave that performs on-host matching of fingerprint images to stored templates and other functions. It has an API that the fingerprint driver calls for this purpose.

Technical Details

An attacker-controlled host application can trigger an invalid memory access and potentially compromise the enclave's security.

At this time, the only verified consequence is overwriting 32-bits of the heap allocation header for an enclave-allocated memory block.

Since SGX is known to have exploit amplification potential, invalid memory accesses can often lead to arbitrary code execution, though at the present time no such exploit is confirmed in these drivers. This specific buffer vulnerability is guarded by a 64-bit token, but it affects only the upper half, so that only 32 bits have to be known, which may allow a brute force analysis to find an attack vector.

Acknowledgements

Synaptics would like to thank Tobias Cloosters <tobias.cloosters@uni-due.de> and Johannes Willbold <johannes.willbold@rub.de> for reporting this issue.

synaptics

Vulnerable/fixed version information

Vulnerable Driver Family	Fixed Version (and later)	Driver Date
5.1.xxx.26	5.1.340.26	07 Jan 2022
5.2.xxxx.26	5.2.3541.26	18 Mar 2022
5.2.2xx.26	5.2.229.26	18 Feb 2022
5.2.3xx.26	5.2.325.26	17 Dec 2021
5.3.xxxx.26	5.3.3543.26	04 Mar 2022
5.5.xx.1058	5.5.44.1058	21 Jan 2022
5.5.xx.1102	5.5.34.1102	20 Jan 2022
5.5.xx.1116	5.5.14.1116	20 Jan 2022
6.0.xx.1104	6.0.50.1104	17 Dec 2021
6.0.xx.1108	6.0.31.1108	26 Nov 2021
6.0.xx.1111	6.0.58.1111	15 Dec 2021

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 synaTEE.signed.dll but are not in one of these version number families, please contact your PC manufacturer.