Synaptics Security Advisory

Synaptics VFS75xx Fingerprint Sensors Equipped with External Flash

CVE: CVE-2019-18618

CVSS 3.1 Score: 6.3 **(**AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:L)

Affected Devices

All Synaptics VFS75xx equipped with external flash.

A table is provided of affected driver versions and corresponding fixed versions. As a general guideline, drivers with a major version number of 5 and a publication date prior to 2020-02 may be vulnerable.

Impact

Incorrect access control in the firmware of Synaptics VFS75xx family fingerprint sensors that include external flash (all versions prior to 2019-11-15) allows a local administrator or physical attacker to compromise the confidentiality of sensor data via injection of an unverified partition table.

Background

The VFS75xx series fingerprint sensors store fingerprint templates on the chip and perform matching without releasing template or fingerprint images outside the secured boundary of the chip in unencrypted form.

Technical Details

An attacker that can send commands to the device (which requires administrator or physical access) can craft a sequence of commands that resets the device (deleting all fingerprint templates and resetting encryption keys) and then installing a partition table with an invalid entry.

After doing this, the attacker can use the device APIs to read any data on the device, and write any data stored on the external flash.

While the user's fingerprint templates are deleted at the start of the process, the confidentiality loss is not completely under the attacker's control, but future fingerprint templates enrolled after the attack can be retrieved and decrypted. Furthermore, after a reset operation, an attacker could subsequently access data in the communications between the host and device as this vulnerability has compromised the fixed global keys used to secure the initial "pairing" operation.

Installing the updated drivers will patch the device to not accept unsigned partition tables. A sensor that is suffering from this exploit will become non-functional and will need to be manually factory reset in the BIOS or other location specified in the OEM's platform documentation after the update is installed.

Acknowledgements

Synaptics would like to thank Viktor Dragomiretskyy for reporting this issue.

Affected Drivers and Fixed Versions[1]

Affected Version (this version and lower)	Corresponding Fixed Version (or later)
5.1.337.26	5.1.338.26
5.2.320.26	5.2.321.26
5.2.3109.26	5.2.3110.26
5.2.3530.26	5.2.3540.26
5.2.5024.26	5.2.5026.26
5.3.3541.26	5.3.3542.26
5.5.35.1058	5.5.40.1058
5.5.17.1099	5.5.21.1099
5.5.17.1102	5.5.26.1102
5.5.10.1106	5.5.18.1106
5.5.4.1116	5.5.8.1116

Affected Drivers Without Fixed Versions as of 2020-07-10 (contact OEM to request update)

Affected Version (this version and lower)
5.1.3507.26
5.1.5.51
5.2.524.26
5.5.502.79
5.5.10.1100
5.5.2734.1050
5.5.2810.1050
5.5.512.1051
5.5.8.1092

[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.