Synaptics Security Advisory

Synaptics Fingerprint Driver: Encryption key derived from static host information

CVE: CVE-2023-6482

CVSS 3.1 score: 5.2(medium) /AV:P/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N

Affected Drivers

WBF device drivers which are deriving keys for encryption of pairing data from host static information – versions prior to 2023-12-01.

Impact

Decryption of pairing data allows the attacker to set up a TLS session with the fingerprint sensor and send restricted commands to the fingerprint sensor. This may allow an attacker, who has physical access to the sensor, to enroll a fingerprint into the template database.

Background

The communication channel between the fingerprint sensor and the WBF device driver is secured by TLS, to protect any sensitive data that is being sent between the sensor and the host device driver.

Technical Details

An attacker, who is reverse engineering the WBF device driver to extract encryption keys derived from static host information, can use those keys to decrypt data used by the TLS handshake between the driver and the sensor. After decrypting the data, the attacker monitors communication to reverse-engineer the TLS handshake.

The attacker then creates software which impersonates the Synaptics WBF device driver, sets up a secure TLS session with the fingerprint sensor, and sends restricted commands to the sensor.

While fingerprint sensors which store fingerprint templates and perform matching on the chip will not release templates or fingerprint images outside the sensor, it may be possible for the attacker to query the sensor database for limited information or enroll a fingerprint which could be used for identification if Windows Enhanced Sign-in Security is not enabled.

Vulnerable/fixed version information

Vulnerable Driver Family	Fixed Version (and later)	Driver Date
6.0.xx.1103	6.0.17.1103	2024/01/16

This table contains all vulnerable device driver families which have a fixed version. Drivers where the xx values are lower than the corresponding sub-minor version number in the fixed version should be considered vulnerable.