Se ha llevado a cabo una reciente investigación que ha descubierto diversas vulnerabilidades que podrían ser aprovechadas para eludir la autenticación de Windows Hello en las laptops Dell Inspiron 15, Lenovo ThinkPad T14 y Microsoft Surface Pro X.

Estas debilidades fueron identificadas por investigadores de Blackwing Intelligence, una firma especializada en seguridad de productos de hardware y software, así como en investigación ofensiva. Estos expertos encontraron fallos en los sensores de huellas digitales de Goodix, Synaptics y ELAN que están integrados en dichos dispositivos.

Un requisito para explotar estas vulnerabilidades en el lector de huellas digitales es que los usuarios de las laptops seleccionadas ya tengan configurada la autenticación mediante huellas digitales.

Los tres sensores de huellas digitales son de tipo *«match on chip»* (MoC), lo que implica que integran las funciones de coincidencia y otras funciones de gestión biométrica directamente en el circuito integrado del sensor.

A pesar de que MoC evita la reproducción de datos de huellas digitales almacenados para la coincidencia en el host, no impide que un sensor malicioso falsifique la comunicación legítima de un sensor con el host y declare falsamente que un usuario autorizado se ha autenticado con éxito, según indicaron los investigadores Jesse D'Aguanno y Timo Teräs.

El MoC tampoco evita la reproducción del tráfico previamente grabado entre el host y el sensor.

Aunque el Protocolo de Conexión Segura de Dispositivos (SDCP) creado por Microsoft tiene como objetivo resolver algunos de estos problemas mediante la creación de un canal seguro de extremo a extremo, los investigadores descubrieron un método novedoso que podría utilizarse para eludir estas protecciones y llevar a cabo ataques de adversario-en-el-medio (AitM).

Específicamente, se encontró que el sensor ELAN era vulnerable a una combinación de

suplantación de sensor debido a la falta de soporte de SDCP y la transmisión en texto claro de identificadores de seguridad (SIDs), lo que permitiría que cualquier dispositivo USB se hiciera pasar por el sensor de huellas digitales y afirmara que un usuario autorizado está iniciando sesión.

En el caso de Synaptics, no solo se descubrió que SDCP estaba apagado por defecto, sino que la implementación elegía depender de una pila personalizada defectuosa de Transport Layer Security (TLS) para asegurar las comunicaciones USB entre el controlador del host y el sensor, lo que podría utilizarse para eludir la autenticación biométrica.

La explotación del sensor Goodix, por otro lado, se aprovecha de una diferencia fundamental en las operaciones de inscripción realizadas en una máquina que tiene tanto Windows como Linux, aprovechando el hecho de que este último no admite SDCP para realizar las siguientes acciones:

1. Iniciar en Linux
2. Enumerar identificadores válidos
3. Inscribir la huella digital del atacante usando el mismo identificador que un usuario legítimo de Windows
4. Llevar a cabo un ataque de adversario-en-el-medio en la conexión entre el host y el sensor aprovechando la comunicación USB en texto claro
5. Iniciar en Windows
6. Intercepta y reescribe el paquete de configuración para apuntar a la base de datos de Linux usando nuestro ataque
7. Iniciar sesión como el usuario legítimo con la huella digital del atacante

Es importante destacar que aunque el sensor Goodix tiene bases de datos de plantillas de huellas digitales separadas para sistemas Windows y no Windows, el ataque es posible porque el controlador del host envía un paquete de configuración no autenticado al sensor para especificar qué base de datos usar durante la inicialización del sensor.

Para mitigar tales ataques, se recomienda que los fabricantes originales (OEMs) habiliten SDCP y se aseguren de que la implementación del sensor de huellas digitales sea auditada por expertos cualificados e independientes.

Esta no es la primera vez que la autenticación biométrica basada en Windows Hello ha sido vulnerada con éxito. En julio de 2021, Microsoft emitió parches para una vulnerabilidad de seguridad de severidad media (CVE-2021-34466, puntuación CVSS: 6.1) que podría permitir a un adversario falsificar el rostro de un objetivo y eludir la pantalla de inicio de sesión.

> *«Microsoft hizo un buen trabajo diseñando SDCP para proporcionar un canal seguro entre el host y los dispositivos biométricos, pero lamentablemente los fabricantes de dispositivos parecen malinterpretar algunos de los objetivos. Además, SDCP solo cubre un ámbito muy limitado de la operación típica de un dispositivo, mientras que la mayoría de los dispositivos tienen una superficie de ataque considerable expuesta que no está cubierta en absoluto por SDCP»,* afirmaron los investigadores.