

| | | | |
|--------------|---|--|---|
| Nro. Alerta: | AL-2023-057 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR |  |
| TLP: |  | | |
| Fecha: | 04-dic-2023 | Fallas en los sensores de huellas dactilares | Pág.: 1 of 8 |


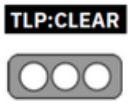
I. DATOS GENERALES:

| | |
|---------------------------|---|
| Clase de alerta: | Vulnerabilidad |
| Tipo de incidente: | Múltiples vulnerabilidades podrían explotarse para evitar la autenticación de Windows Hello en las computadoras portátiles Dell Inspiron 15, Lenovo ThinkPad T14 y Microsoft Surface Pro X por fallas en los sensores de huellas dactilares de Goodix, Synaptics y ELAN que están integrados en los dispositivos. |
| Nivel de riesgo: | Alto |

II. ALERTA



Figura 1.- Nuevas fallas en los sensores de huellas dactilares permiten a los atacantes eludir el inicio de sesión de Windows Hello

| | | | |
|--------------|---|--|---|
| Nro. Alerta: | AL-2023-057 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR |  |
| TLP: |  | | |
| Fecha: | 04-dic-2023 | Fallas en los sensores de huellas dactilares | Pág.: 2 of 8 |

III. INTRODUCCIÓN

Windows Hello es una forma más personal y segura de obtener acceso inmediato a los dispositivos Windows 10 mediante un PIN, el reconocimiento facial y en este caso particular a través de la huella digital.

Blackwing Intelligence es una empresa de seguridad cibernética que se especializa en seguridad de productos de hardware y software de alta gama e investigación ofensiva; Jesse D'Agunno (@0x30n) y Timo Teräs (@terastimo) evaluaron a pedido de Microsoft's Offensive Research and Security Engineering (MORSE), respecto a la seguridad de los tres principales sensores de huellas dactilares integrados en las computadoras portátiles Dell Inspiron 15, Lenovo ThinkPad T14 y Microsoft Surface Pro Type Cover with Fingerprint ID (for Surface Pro 8 / X) y utilizados para la autenticación de huellas dactilares de Windows Hello; la investigación reveló múltiples vulnerabilidades, lo que permitió omitir por completo la autenticación de Windows Hello en las tres computadoras portátiles.

En la investigación se utilizó ingeniería inversa de software y hardware para solucionar fallas de implementación criptográfica en un TLS personalizado, descifrar y reimplantar protocolos propietarios para lograr eludir por completo la autenticación de Windows Hello en las tres computadoras portátiles, objetivos de investigación; adicional se investigó varios métodos de "ataque de presentación"; estos son los ataques más tradicionales contra las tecnologías biométricas, como extraer huellas dactilares latentes de superficies, crear huellas dactilares falsas, etc. utilizando métodos probados y verdaderos, así como enfoques más novedosos que utilizan la impresión 3D y otras tecnologías.

Un requisito previo para las vulnerabilidades del lector de huellas digitales es que los usuarios de las computadoras portátiles objetivo tengan la autenticación de huellas digitales ya configurada; los tres sensores de huellas dactilares son un tipo de sensor llamado "match on chip" (MoC), que integra la coincidencia y otras funciones de gestión biométrica directamente en el circuito integrado del sensor.

| | | | |
|--------------|---|--|---|
| Nro. Alerta: | AL-2023-057 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR |  |
| TLP: |  | | |
| Fecha: | 04-dic-2023 | Fallas en los sensores de huellas dactilares | V 1.1 Pág.: 3 of 8 |

Los investigadores Jesse D'Aguanno y Timo Teräs indicaron que "Si bien MoC evita la reproducción de datos de huellas dactilares almacenados en el host para su comparación, no impide, en sí mismo, que un sensor malicioso falsifique la comunicación de un sensor legítimo con el host y afirme falsamente que un usuario autorizado se ha autenticado exitosamente".

IV. VECTOR DE ATAQUE:

- Ataques de presentación

Estos son los ataques más tradicionales contra las tecnologías biométricas, como extraer huellas dactilares latentes de superficies, crear huellas dactilares falsas; utilizando métodos probados y verdaderos, así como enfoques más novedosos que utilizan la impresión 3D y otras tecnologías.


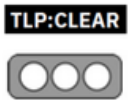
V. IMPACTO:

El MoC tampoco impide 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 aliviar algunos de estos problemas mediante la creación de un canal seguro de extremo a extremo, los investigadores descubrieron un método novedoso que podría usarse para eludir estas protecciones y organizar ataques del adversario en el medio (AitM).

Específicamente, se descubrió que el sensor ELAN era vulnerable a una combinación de suplantación de sensor derivada de la falta de compatibilidad con SDCP y la transmisión de texto sin cifrar de identificadores de seguridad (SID), permitiendo así que cualquier dispositivo USB se haga pasar por el sensor de huellas digitales y afirme que un usuario autorizado está iniciando sesión.



| | | | |
|--------------|---|---|---|
| Nro. Alerta: | AL-2023-057 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR ALERTAS DE SEGURIDAD |  |
| TLP: |  | | V 1.1 |
| Fecha: | 04-dic-2023 | Fallas en los sensores de huellas dactilares | Pág.: 4 of 8 |

En el caso de Synaptics, no solo se descubrió que SDCP estaba desactivado de forma predeterminada, sino que la implementación optó por confiar en una pila de Seguridad de la capa de transporte (TLS) personalizada y defectuosa para asegurar las comunicaciones USB entre el controlador host y el sensor que podrían usarse como arma para eludir autenticación biométrica.

VI. INDICADORES DE COMPROMISO

Vulneraciones en la seguridad de los tres principales sensores de huellas dactilares integrados utilizados para Windows Hello integrado por los fabricantes de portátiles OEM.

Las computadoras portátiles objetivo fueron:

- Dell Inspiron 15
- Lenovo ThinkPad T14
- Funda con teclado para Microsoft Surface Pro con identificación de huellas dactilares (para Surface Pro 8/X)

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

- Arrancar en Linux
- Enumerar identificaciones válidas
- Registre la huella digital del atacante utilizando la misma identificación que un usuario legítimo de Windows
- MitM la conexión entre el host y el sensor aprovechando la comunicación USB de texto sin cifrar
- Arrancar en Windows

| | | | |
|--------------|---|--|--|
| Nro. Alerta: | AL-2023-057 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR |  ALERTAS DE SEGURIDAD |
| TLP: |  | | |
| Fecha: | 04-dic-2023 | Fallas en los sensores de huellas dactilares | Pág.: 5 of 8 |

- Intercepte y reescriba el paquete de configuración para que apunte a la base de datos de Linux usando nuestro MitM
- Inicie sesión como usuario legítimo con la impresión del atacante

Vale la pena señalar que si bien el sensor Goodix tiene bases de datos de plantillas de huellas dactilares separadas para sistemas Windows y no Windows, el ataque es posible debido al hecho de que el controlador del host envía un paquete de configuración no autenticado al sensor para especificar qué base de datos usar durante el sensor de inicialización.

VII. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- La autenticación biométrica puede ser muy útil para permitir a los usuarios iniciar sesión cómodamente. Esto es especialmente útil en escenarios móviles, ya que permite al usuario elegir una contraseña larga para protegerse contra el descifrado de sus datos, mientras le permite acceder a su dispositivo durante todo el día sin el inconveniente de ingresando la contraseña larga. También es clave para un futuro de autenticación de dispositivos sin contraseña.
- Microsoft hizo un buen trabajo al diseñar SDP para proporcionar un canal seguro entre el host y los dispositivos biométricos, pero desafortunadamente los fabricantes de dispositivos parecen malinterpretar algunos de los objetivos. Además, SDP solo cubre un alcance muy limitado del funcionamiento de un dispositivo típico, mientras que la mayoría de los dispositivos tienen expuesta una superficie de ataque considerable que no está cubierta por SDP en absoluto.
- Asegúrese de que SDP esté habilitado. (No ayuda si no está encendido)
- Haga que un tercero experto calificado audite su implementación.



| | | | |
|--------------|---|---|--|
| Nro. Alerta: | AL-2023-057 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR ALERTAS DE SEGURIDAD |  V 1.1 |
| TLP: |  | | |
| Fecha: | 04-dic-2023 | Fallas en los sensores de huellas dactilares | Pág.: 6 of 8 |

- Seguridad del firmware: Aunque todo el firmware de los sensores puede estar cifrado, la calidad del código podría ser deficiente en general. Según las pruebas por los expertos, existe una alta probabilidad de que los sensores sean vulnerables a la corrupción de la memoria.
- Funcionalidad oculta: hay muchas funciones que no se utilizan directamente en el funcionamiento normal, incluida la depuración y otros comandos. Es probable que existan otras vulnerabilidades lógicas ocultas bajo la superficie. Ataques directos al hardware (JTAG, decapping, acceso al almacenamiento, fallas, análisis de energía, etc.). No hay protección si un atacante puede escribir directamente en la base de datos o extraer secretos del dispositivo. Ataques de canal lateral para revelar secretos (claves específicas del dispositivo, claves de descifrado de firmware, etc.)

En general se debe considerar las siguientes recomendaciones:

- Instalar actualizaciones disponibles en medios oficiales del proveedor, previo análisis del impacto que podría provocar en los servicios críticos para el negocio de la organización.
- Realizar copias de respaldo de seguridad periódicas, de la información crítica para evitar la pérdida de la misma.
- Actualizar el sistema operativo de los equipos a las últimas versiones.
- No abrir, manipular, o interactuar, con correos electrónicos altamente sospechosos que lleguen a las bandejas de correo o mensaje en redes sociales.
- Otorgar privilegios de usuario al mínimo dependiendo del tipo de labor a realizar.
- Implementar técnicas de navegación segura en toda la Institución/Organización, como por ejemplo visita únicamente de sitios con certificados SSL, y, de origen no sospechoso.
- Bloquear el acceso de usuarios, a dispositivos de almacenamiento externo, ajenos a la Institución/Organización, a través de políticas de seguridad adecuadas.



| | | | |
|--------------|---|--|---|
| Nro. Alerta: | AL-2023-057 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR |  |
| TLP: |  | | |
| Fecha: | 04-dic-2023 | Fallas en los sensores de huellas dactilares | Pág.: 7 of 8 |

- Implementar y monitorear, plataformas de seguridad perimetral para identificar posible tráfico malicioso tanto a nivel interno como externo a la infraestructura de red de la organización/Institución
- Descargar programas, archivos y actualizaciones, solamente desde fuentes oficiales y verificadas.
- Cerrar todo tipo de conexión/protocolo de acceso remoto a infraestructuras críticas en la Organización/Institución, en el caso de requerir su implementación, realizarlo bajo estrictas normas de seguridad apalancados en plataformas de seguridad perimetral y, uso de una VPN.
- Tener actualizado y utilizar, un software anti-virus
- Mantener actualizados, y, bajo licenciamiento, (ya sea a nivel de software libre o de paga, de ser el caso), todos y cada uno de los sistemas y subsistemas de software y hardware de toda la infraestructura de IT y OT de la Institución, esto es, incluido a nivel de Firmware de todos los componentes.
- Diseñar una política de revisión de logs, que permita detectar comportamientos fuera de lo normal en procesos legítimos del sistema.
- Mantener listas de control de acceso para las unidades mapeadas en red restringiendo los privilegios de escritura. Con esto podrá identificar el impacto generado por el cifrado de archivos, entendiendo que el secuestro de información se producirá en todas las unidades de red mapeadas en el equipo víctima.
- Capacitar a todos los usuarios, mediante la concientización y simulaciones para reconocer e informar sobre intentos de phishing e ingeniería social. Seguir las normativas internacionales tales como ISO 27001/27002 en su control “Concientización con educación y capacitación en seguridad de la información” o “Todos los usuarios se encuentran entrenados e informados”, a fin de tener bases para divulgar campañas educativas orientadas a nivel de usuarios respecto al correcto uso de las herramientas tecnológicas
- Implementar un plan de respuesta a emergencias de la Organización/Institución.
- En el caso de sufrir un ataque de proporciones mayores, contacte a las Autoridades competentes en base a la Normativa Legal Vigente a nivel Nacional.



| | | | |
|--------------|---|--|--|
| Nro. Alerta: | AL-2023-057 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR |  ecucert |
| TLP: |  | | |
| Fecha: | 04-dic-2023 | Fallas en los sensores de huellas dactilares | V 1.1 Pág.: 8 of 8 |

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

- **The Hacker News (2023).** *New Flaws in Fingerprint Sensors Let Attackers Bypass Windows Hello Login.* <https://thehackernews.com/2023/11/new-flaws-in-fingerprint-sensors-let.html>
- **D'Aguanno, J & Teras T (2023).** *A Touch of PWN – Part I.* <https://blackwinghq.com/blog/posts/a-touch-of-pwn-part-i/>

