Un análisis detallado de un sistema de acceso biométrico híbrido fabricado por ZKTeco, una compañía china, ha revelado veinticuatro fallos de seguridad que podrían ser explotados por atacantes para eludir la autenticación, sustraer datos biométricos e incluso implementar puertas traseras maliciosas.

Según Kaspersky, *«al introducir datos de usuario aleatorios en la base de datos o utilizar un código QR falsificado, un individuo malintencionado puede fácilmente evadir el proceso de verificación y obtener acceso no autorizado».* Además, los atacantes podrían manipular dispositivos de manera remota, filtrar datos biométricos y desplegar puertas traseras.

Las 24 vulnerabilidades incluyen seis inyecciones SQL, siete desbordamientos de búfer basados en pila, cinco inyecciones de comandos, cuatro escrituras de archivos arbitrarios y dos lecturas de archivos arbitrarios. A continuación se ofrece una breve descripción de cada tipo de vulnerabilidad:

- CVE-2023-3938 (CVSS score: 4.6) – Una vulnerabilidad de inyección SQL que se activa al mostrar un código QR en la cámara del dispositivo mediante una solicitud especialmente manipulada que contiene una comilla, lo que permite a un atacante autenticarse como cualquier usuario en la base de datos.
- CVE-2023-3939 (CVSS score: 10.0) – Un conjunto de vulnerabilidades de inyección de comandos que permite la ejecución de comandos arbitrarios del sistema operativo con privilegios de root.
- CVE-2023-3940 (CVSS score: 7.5) – Un conjunto de vulnerabilidades de lectura de archivos arbitrarios que permite a un atacante eludir los controles de seguridad y acceder a cualquier archivo en el sistema, incluidos datos sensibles de usuarios y configuraciones del sistema.
- CVE-2023-3941 (CVSS score: 10.0) – Un conjunto de vulnerabilidades de escritura de archivos arbitrarios que permite a un atacante escribir cualquier archivo en el sistema con privilegios de root, incluida la modificación de la base de datos de usuarios para agregar usuarios falsos.
- CVE-2023-3942 (CVSS score: 7.5) – Un conjunto de vulnerabilidades de inyección SQL que permite a un atacante insertar código SQL malicioso y realizar operaciones no

autorizadas en la base de datos, extrayendo datos sensibles.
- CVE-2023-3943 (CVSS score: 10.0) – Un conjunto de vulnerabilidades de desbordamiento de búfer basado en pila que permite a un atacante ejecutar código arbitrario.

> *«El impacto de las vulnerabilidades encontradas es preocupantemente amplio. Inicialmente, los atacantes podrían vender datos biométricos robados en la dark web, exponiendo a los afectados a mayores riesgos de deepfakes y sofisticados ataques de ingeniería social»,* afirmó el investigador de seguridad Georgy Kiguradze.

Además, la explotación exitosa de estas vulnerabilidades podría permitir a los actores maliciosos acceder a áreas restringidas e incluso instalar puertas traseras para infiltrarse en redes críticas, facilitando así el ciberespionaje o ataques disruptivos.

La empresa rusa de ciberseguridad, que identificó estas vulnerabilidades mediante ingeniería inversa del firmware (versión ZAM170-NF-1.8.25-7354-Ver1.0.0) y el protocolo propietario utilizado para la comunicación con el dispositivo, señaló que no tiene información sobre si estos problemas han sido corregidos.

Para mitigar el riesgo de ataques, se recomienda separar el uso de lectores biométricos en segmentos de red distintos, utilizar contraseñas de administrador robustas, mejorar la configuración de seguridad del dispositivo, reducir el uso de códigos QR y mantener actualizados los sistemas.

> *«Los dispositivos biométricos diseñados para mejorar la seguridad física pueden ofrecer funcionalidades convenientes y útiles, pero también introducen nuevos riesgos en el sistema de TI»,* advirtió Kaspersky.

> *«Cuando tecnologías avanzadas como la biometría se implementan en dispositivos con insuficiente seguridad, esto prácticamente anula los beneficios de la autenticación biométrica. Así, un terminal mal configurado se vuelve vulnerable a ataques simples, facilitando a los intrusos comprometer la seguridad física de las áreas críticas de la organización».*