SI

Análisis de Seguridad en Dispositivos Biométricos de Control de Acceso: Caso de Estudio ZMM220

Mg. Ing. Rodrigo Atilio Elgueta[a], Dr. Ing. Miguel Méndez-Garabetti[a], Ing. Diego Germán Gomez[a]

[a]Univerisdad de Champagnat, Facultad de Informática y Diseño, General Juan Manuel Belgrano 721,CP: 5501 Godoy Cruz, Mendoza, Argentina
elguetarodrigo@uch.edu.ar, mendez-garabettimiguel@uch.edu.ar, gomezdiego@uch.edu.ar

INTRODUCCIÓN

Los sistemas biométricos son ampliamente utilizados en entornos organizacionales, no solo para la gestión de asistencia y reportes de recursos humanos, sino también en contextos críticos como el control de salidas transitorias de personas privadas de la libertad y la identificación de personas. Sin embargo, estos dispositivos pueden presentar vulnerabilidades que comprometen la seguridad de la información y de los procesos que soportan. En este trabajo se propone una metodología reproducible para evaluar su seguridad, validada mediante un caso de estudio sobre el dispositivo ZMM220.

I + D :

La I+D se centra en el desarrollo de metodologías de evaluación de seguridad para dispositivos biométricos, integrando análisis técnico, forense y normativo, con el objetivo de identificar vulnerabilidades y generar contramedidas aplicables en entornos reales.

Metodología
↓
Evaluación técnica
↓
Análisis forense
↓
Evaluación normativa
↓
Hardening

RESULTADOS CLAVE

- **Credenciales por Defecto** → Acceso Total al sistema
- **Telnet sin Cifrado** → Exposición de credenciales
- **SQLite sin Protección** → Manipulación de datos
- **Vulnerabilidades en Kernel** → Escalada de privilegios

```
Telnet
    Data: \r\r\n
    Data: Welcome to Linux (ZMM220) for MIPS\r\n
    Data: \rKernel 3.0.8 on an MIPS\r\n
    Data: \r
```

```
# ls *.db && ls *sql*
ZKDB.db       ZKSystem.db
sql-generator.sh        update_language.sql     update_shortcutkey.sql  update_wiegand_new.sql
sqlite3_mips            update_menu.sql         update_wiegand.sql
#
```

```
# ./sqlite3_mips ZKDB.db
SQLite version 3.7.15.2 2013-01-09 11:53:05
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> .tables
ACC_ATT_LOG                 LARGE_MQ
ACC_DAT_OTHERNAME           MESSAGE_QUEUE
ACC_FIRST_OPEN              Nation_LIST
ACC_HOLIDAY_TAB             OPTION_INFO
ACC_INOUT_FUN               OP_LOGS
ACC_MULTI_USER              Options
ACC_OP_LOG                  PERMISSION
ACC_RULE_NAME               PERSONAL_PERDAY_SCHEDULING
ACC_RULE_TIME               PERSONAL_SCHEDULING
ACC_TIME_ZONE               PHOTO_INDEX
ACC_TIME_ZONE_RULE          RES_LIST
ACC_USER_AUTHORIZE          ROLE
APN_LIST                    ROLE_INFO
```

Se confirmaron y explotaron vulnerabilidades críticas en el dispositivo ZMM220, incluyendo credenciales predeterminadas, bases de datos SQLite sin cifrado, uso de Telnet en texto plano y un kernel vulnerable (DirtyCow en MIPS). A diferencia de reportes previos, este trabajo aporta evidencia técnica reproducible mediante herramientas como Hydra, Wireshark y sqlite3, demostrando el acceso no autorizado y la manipulación de registros. Como contribución, se proponen medidas de mitigación concretas basadas en estándares, tales como hardening de credenciales, migración a SSH, cifrado de bases de datos y actualización del sistema. Actualmente, las organizaciones participantes se encuentran en proceso de parcheo de las vulnerabilidades detectadas, y se proyecta la elaboración de una guía de hardening y la extensión del análisis a otros dispositivos biométricos.

IMPACTO

Exposición de datos biométricos

- Acceso no autorizado
- Manipulación sin trazabilidad

CONCLUSIÓN

Los resultados evidencian que dispositivos biométricos comerciales pueden comprometer la seguridad organizacional si no se implementan configuraciones seguras desde su despliegue.

RRHH

Formación de recursos humanos en ciberseguridad aplicada, fortaleciendo capacidades en análisis de sistemas embebidos y transferencia tecnológica.

Acceso al trabajo Completo
Escanee para más información

*IAs utilizadas en el trabajo: Audio - elevenlabs.io/ - Ayudas de Diseño: - https://chatgpt.com - General: https://chat.deepseek.com