Encryption in Industrial HiVision

Christoph Strauss - 2022-01-25 - Industrial HiVision

1. **Data in Transit**
    - Within Industrial HiVision:
        - GUI – Kernel: Corba over SSL (encrypted)
        - Kernel – Kernel: Corba over SSL (encrypted)
    - Industrial HiVision – Devices (dependent on the device / the configuration of the device):
        - Unencrypted:
            - SNMP V1, HTTP, Telnet, HiDiscoveryV1, HiDiscoveryV2, EtherNet/IP
        - Encrypted:
            - SNMP V3, HTTPS, SSH
2. **Data at Rest**
    - Most data is stored unencrypted in the Industrial HiVision database
        - All passwords and community strings (SNMP V1) are encrypted in the database
    - Some data is stored unencrypted in files, for example the IP address of the server to which the GUI is connected
    - Industrial HiVision User Management: stored in an unencrypted file, passwords saved as a hash
3. **Authentication and Management of Security Services**
    - User Management in Industrial HiVision: configurable:
        - None
        - LDAP (secure or unsecure)
        - RADIUS (unsecure)
        - Local (Industrial HiVision User Management)
    - Password to protect Edit Mode (optional and configurable)
4. **Protocol Security**
    - SNMP V3: depending on the settings: MD5, SHA / DES, AES128
    - All passwords and community strings in the database: DES