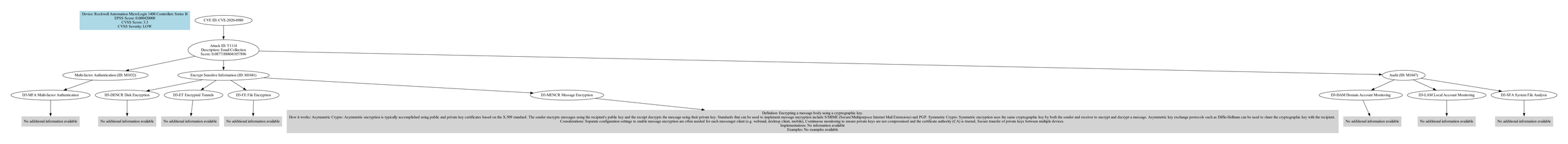
Device: Rockwell Automation MicroLogix 1400 Controllers Series B
EPSS Score: 0.00042000
CVSS Score: 3.3
CVSS Severity: LOW
CVE ID: CVE-2020-6980
Attack ID: T1114
Description: Email Collection
Score: 0.08771888041857896
Multi-factor Authentication (ID: M1032)
Encrypt Sensitive Information (ID: M1041)
Audit (ID: M1047)
D3-MFA Multi-factor Authentication
D3-DENCR Disk Encryption
D3-ET Encrypted Tunnels
D3-FE File Encryption
D3-MENCR Message Encryption
D3-DAM Domain Account Monitoring
D3-LAM Local Account Monitoring
D3-SFA System File Analysis
No additional information available
No additional information available
No additional information available
No additional information available
Definition: Encrypting a message body using a cryptographic key.
How it works: Asymmetric Crypto: Asymmetric encryption is typically accomplished using public and private key certificates based on the X.509 standard. The sender encrypts messages using the recipient's public key and the receipt decrypts the message using their private key. Standards that can be used to implement message encryption include S/MIME (Secure/Multipurpose Internet Mail Extensions) and PGP. Symmetric Crypto: Symmetric encryption uses the same cryptographic key by both the sender and receiver to encrypt and decrypt a message. Asymmetric key exchange protocols such as Diffie-Hellman can be used to share the cryptographic key with the recipient.
Considerations: Separate configuration settings to enable message encryption are often needed for each messenger client (e.g. webmail, desktop client, mobile). Continuous monitoring to ensure private keys are not compromised and the certificate authority (CA) is trusted. Secure transfer of private keys between multiple devices.
Implementations: No information available
Examples: No examples available
No additional information available
No additional information available
No additional information available