

Device: Rockwell Automation MicroLogix 1400 Controllers Series B  
EPSS Score: 0.000420000  
CVSS Score: 3.3  
CVSS Severity: LOW

CVE ID: CVE-2020-6980

Attack ID: T1070  
Description: Indicator Removal  
Score: 0.07732568000696391

Remote Data Storage (ID: M1029)

Restrict File and Directory Permissions (ID: M1022)

Encrypt Sensitive Information (ID: M1041)

No Defense Measure  
Reason: IT disaster recovery plans are outside the current scope of D3FEND.

D3-LFP Local File Permissions

D3-DENCR Disk Encryption

D3-ET Encrypted Tunnels

D3-FE File Encryption

D3-MENCR Message Encryption

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