Multi-factor Authentication, Mitigation M0932 - ICS

By Authorization Enforcement

Archived: 2026-04-05 12:36:52 UTC

Use two or more pieces of evidence to authenticate to a system; such as username and password in addition to a token from a physical smart card or token generator. Within industrial control environments assets such as low-level controllers, workstations, and HMIs have real-time operational control and safety requirements which may restrict the use of multi-factor.

ID: M0932

Security Controls: IEC 62443-3-3:2013 - SR 1.7, IEC 62443-4-2:2019 - CR 1.7, NIST SP 800-53 Rev. 5 - IA-2

Version: 1.0

Created: 10 June 2019

Last Modified: 16 April 2025

Techniques Addressed by Mitigation

Domain	ID	Name	Use
ICS	T0822	External Remote Services	Use strong multi-factor authentication for remote service accounts to mitigate an adversary's ability to leverage stolen credentials. Be aware of multi-factor authentication interception techniques for some implementations.
ICS	T0842	Network Sniffing	Use multi-factor authentication wherever possible.
ICS	T0859	Valid Accounts	Integrating multi-factor authentication (MFA) as part of organizational policy can greatly reduce the risk of an adversary gaining access to valid credentials that may be used for additional tactics such as initial access, lateral movement, and collecting information. MFA can also be used to restrict access to cloud resources and APIs.