Disable or Remove Feature or Program, Mitigation M0942 - ICS

By Authorization Enforcement

Archived: 2026-04-05 16:14:26 UTC

Domain	ID	Name	Use
ICS	T0830	Adversary-in-the-Middle	Disable unnecessary legacy network protocols that may be used for AiTM if applicable.
ICS	T0807	Command-Line Interface	Consider removing or restricting features that are unnecessary to an asset's intended function within the control environment.
ICS	T0885	Commonly Used Port	Ensure that unnecessary ports and services are closed to prevent risk of discovery and potential exploitation.
ICS	T0816	Device Restart/Shutdown	Ensure remote commands that enable device shutdown are disabled if they are not necessary. Examples include DNP3's 0x0D function code or unnecessary device management functions.
ICS	T0866	Exploitation of Remote Services	Ensure that unnecessary ports and services are closed to prevent risk of discovery and potential exploitation.
ICS	T0822	External Remote Services	Consider removal of remote services which are not regularly in use, or only enabling them when required (e.g., vendor remote access). Ensure all external remote access point (e.g., jump boxes, VPN concentrator) are configured with least functionality, especially the removal of unnecessary services. [1]
ICS	T0847	Replication Through Removable Media	Consider the disabling of features such as AutoRun.

Domain	ID	Name	Use
ICS	T0853	Scripting	Consider removal or disabling of programs and features which may be used to run malicious scripts (e.g., scripting language IDEs, PowerShell, visual studio).

Source: https://attack.mitre.org/mitigations/M0942