Restrict File and Directory Permissions, Mitigation M0922 - ICS

By Authorization Enforcement

Archived: 2026-04-05 16:58:28 UTC

Domain	ID	Name	Use
ICS	T0809	Data Destruction	Protect files stored locally with proper permissions to limit opportunities for adversaries to impact data storage. [1]
ICS	T0811	Data from Information Repositories	Protect files with proper permissions to limit opportunities for adversaries to interact and collect information from databases. [2] [1]
ICS	T0893	Data from Local System	Protect files stored locally with proper permissions to limit opportunities for adversaries to interact and collect information from the local system. [2] [1]
ICS	T0872	Indicator Removal on Host	Protect files stored locally with proper permissions to limit opportunities for adversaries to remove indicators of their activity on the system. [2] [1]
ICS	T0849	Masquerading	Use file system access controls to protect system and application folders.
ICS	T0873	Project File Infection	Ensure permissions restrict project file access to only engineer and technician user groups and accounts.
ICS	T0881	Service Stop	Ensure proper process and file permissions are in place to inhibit adversaries from disabling or interfering with critical services.

Domain	ID	Name	Use
ICS	T0882	Theft of Operational Information	Protect files stored locally with proper permissions to limit opportunities for adversaries to interact and collect information from databases. [2] [1]

Source: https://attack.mitre.org/mitigations/M0922