Modify Alarm Settings, Technique T0838 - ICS

Archived: 2026-04-02 12:05:41 UTC

Adversaries may modify alarm settings to prevent alerts that may inform operators of their presence or to prevent responses to dangerous and unintended scenarios. Reporting messages are a standard part of data acquisition in control systems. Reporting messages are used as a way to transmit system state information and acknowledgements that specific actions have occurred. These messages provide vital information for the management of a physical process, and keep operators, engineers, and administrators aware of the state of system devices and physical processes.

If an adversary is able to change the reporting settings, certain events could be prevented from being reported. This type of modification can also prevent operators or devices from performing actions to keep the system in a safe state. If critical reporting messages cannot trigger these actions then a Impact could occur.

In ICS environments, the adversary may have to use Alarm Suppression or contend with multiple alarms and/or alarm propagation to achieve a specific goal to evade detection or prevent intended responses from occurring. [1] Methods of suppression often rely on modification of alarm settings, such as modifying in memory code to fixed values or tampering with assembly level instruction code.

Source: https://attack.mitre.org/techniques/T0838