Software Process and Device Authentication, Mitigation M0813 - ICS

By Authorization Enforcement

Archived: 2026-04-05 15:07:07 UTC

ICS T0800 Activate Firmware Update Mode

Authenticate connections fromsoftware and devices to prevent unauthorized systems from accessing protected management functions.

ICS T0830 Adversary-in-the-Middle

To protect against AiTM, authentication mechanisms should not send credentials across the network in plaintext and should also implement mechanisms to prevent replay attacks (such as nonces or timestamps). Challenge-response based authentication techniques that do not directly send credentials over the network provide better protection from AiTM.

ICS T0806 Brute Force I/O

Devices should authenticate all messages between master and outstation assets.

ICS T0858 Change Operating Mode

Authenticate connections fromsoftware and devices to prevent unauthorized systems from accessing protected management functions.

ICS T0868 Detect Operating Mode

Authenticate connections from software and devices to prevent unauthorized systems from accessing protected management functions.

ICS T0816 Device Restart/Shutdown

Authenticate connections from software and devices to prevent unauthorized systems from accessing protected management functions.

ICS T0838 Modify Alarm Settings

Authenticate connections fromsoftware and devices to prevent unauthorized systems from accessing protected management functions.

ICS T0839 Module Firmware

Authenticate connections fromsoftware and devices to prevent unauthorized systems from accessing protected management functions.

ICS T0861 Point & Tag Identification

Devices should authenticate all messages between master and outstation assets.

ICS T0843 Program Download

Authenticate connections from software and devices to prevent unauthorized systems from accessing protected management functions.

ICS T0845 Program Upload

Authenticate connections from software and devices to prevent unauthorized systems from accessing protected management functions.

ICS T0886 Remote Services

All communication sessions to remote services should be authenticated to prevent unauthorized access.

ICS T0848 Rogue Master

Devices should authenticate all messages between master and outstation assets.

ICS T0856 Spoof Reporting Message

Devices should authenticate all messages between master and outstation assets.

ICS T0857 System Firmware

Authenticate connections fromsoftware and devices to prevent unauthorized systems from accessing protected management functions.

ICS T0855 Unauthorized Command Message

Devices should authenticate all messages between master and outstation assets.

ICS T0860 Wireless Compromise

Ensure wireless networks require the authentication of all devices, and that all wireless devices also authenticate network infrastructure devices (i.e., mutual authentication). For defense-in-depth purposes, utilize VPNs or ensure that application-layer protocols also authenticate the system or device. Use protocols that provide strong authentication (e.g., IEEE 802.1X), and enforce basic protections, such as MAC filtering, when stronger cryptographic techniques are not available.
