Communication Authenticity, Mitigation M0802 - ICS

Archived: 2026-04-05 12:53:21 UTC

ICS T0800 Activate Firmware Update Mode

Protocols used for device management should authenticate all network messages to prevent unauthorized system changes.

ICS T0830 Adversary-in-the-Middle

Communication authenticity will ensure that any messages tampered with through AiTM can be detected, but cannot prevent eavesdropping on these. In addition, providing communication authenticity around various discovery protocols, such as DNS, can be used to prevent various AiTM procedures.

ICS T0858 Change Operating Mode

Protocols used for device management should authenticate all network messages to prevent unauthorized system changes.

ICS T0868 Detect Operating Mode

Protocols used for control functions should provide authenticity through MAC functions or digital signatures. If not, utilize bump-in-the-wire devices or VPNs to enforce communication authenticity between devices that are not capable of supporting this (e.g., legacy controllers, RTUs).

ICS T0816 Device Restart/Shutdown

Protocols used for control functions should provide authenticity through MAC functions or digital signatures. If not, utilize bump-in-the-wire devices or VPNs to enforce communication authenticity between devices that are not capable of supporting this (e.g., legacy controllers, RTUs).

ICS T0831 Manipulation of Control

Protocols used for control functions should provide authenticity through MAC functions or digital signatures. If not, utilize bump-in-the-wire devices or VPNs to enforce communication authenticity between devices that are not capable of supporting this (e.g., legacy controllers, RTUs).

ICS T0832 Manipulation of View

Protocols used for control functions should provide authenticity through MAC functions or digital signatures. If not, utilize bump-in-the-wire devices or VPNs to enforce communication authenticity between devices that are not capable of supporting this (e.g., legacy controllers, RTUs).

ICS T0839 Module Firmware

Protocols used for device management should authenticate all network messages to prevent unauthorized system changes.

ICS T0861 Point & Tag Identification

Protocols used for control functions should provide authenticity through MAC functions or digital signatures. If not, utilize bump-in-the-wire devices or VPNs to enforce communication authenticity between devices that are not capable of supporting this (e.g., legacy controllers, RTUs).

ICS T0843 Program Download

Protocols used for device management should authenticate all network messages to prevent unauthorized system changes.

ICS T0845 Program Upload

Protocols used for device management should authenticate all network messages to prevent unauthorized system changes.

ICS T0848 Rogue Master

Protocols used for control functions should provide authenticity through MAC functions or digital signatures. If not, utilize bump-in-the-wire devices or VPNs to enforce communication authenticity between devices that are not capable of supporting this (e.g., legacy controllers, RTUs).

ICS T0856 Spoof Reporting Message

Protocols used for control functions should provide authenticity through MAC functions or digital signatures. If not, utilize bump-in-the-wire devices or VPNs to enforce communication authenticity between devices that are not capable of supporting this (e.g., legacy controllers, RTUs).

ICS T0857 System Firmware

Protocols used for device management should authenticate all network messages to prevent unauthorized system changes.

ICS T0855 Unauthorized Command Message

Protocols used for control functions should provide authenticity through MAC functions or digital signatures. If not, utilize bump-in-the-wire devices or VPNs to enforce communication authenticity between devices that are not capable of supporting this (e.g., legacy controllers, RTUs).

ICS T0860 Wireless Compromise

Do not inherently rely on the authenticity provided by the network/link layer (e.g., 802.11, LTE, 802.15.4), as link layer equipment may have long lifespans and protocol vulnerabilities may not be easily patched. Provide defense-in-depth by implementing authenticity within the associated application-layer protocol, or through a network-layer

VPN. [1] Furthermore, ensure communication schemes provide strong replay protection, employing techniques such as timestamps or cryptographic nonces.
