Audit, Mitigation M0947 - ICS

Archived: 2026-04-05 17:59:19 UTC

ICS T0830 Adversary-in-the-Middle

Limit access to network infrastructure and resources that can be used to reshape traffic or otherwise produce AiTM conditions.

ICS T0811 Data from Information Repositories

Consider periodic reviews of accounts and privileges for critical and sensitive repositories.

ICS T0874 Hooking

Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses. Perform periodic integrity checks of the device to validate the correctness of the firmware, software, programs, and configurations. Integrity checks, which typically include cryptographic hashes or digital signatures, should be compared to those obtained at known valid states, especially after events like device reboots, program downloads, or program restarts.

ICS T0821 Modify Controller Tasking

Provide the ability to verify the integrity of controller tasking. While techniques like CRCs and checksums are commonly used, they are not cryptographically secure and can be vulnerable to collisions. Preferably cryptographic hash functions (e.g., SHA-2, SHA-3) should be used. [1]

ICS T0836 Modify Parameter

Provide the ability to verify the integrity and authenticity of changes to parameter values.

ICS T0889 Modify Program

Provide the ability to verify the integrity of control logic or programs loaded on a controller. While techniques like CRCs and checksums are commonly used, they are not cryptographically strong and can be vulnerable to collisions. Preferably cryptographic hash functions (e.g., SHA-2, SHA-3) should be used. [1]

ICS T0839 Module Firmware

Perform integrity checks of firmware before uploading it on a device. Utilize cryptographic hashes to verify the firmware has not been tampered with by comparing it to a trusted hash of the firmware. This could be from trusted data sources (e.g., vendor site) or through a third-party verification service.

ICS T0843 Program Download

Provide the ability to verify the integrity of programs downloaded on a controller. While techniques like CRCs and checksums are commonly used, they are not cryptographically secure and can be vulnerable to collisions. Preferably cryptographic hash functions (e.g., SHA-2, SHA-3) should be used. [1]

ICS T0873 Project File Infection

Review the integrity of project files to verify they have not been modified by adversary behavior. Verify a cryptographic hash for the file with a known trusted version, or look for other indicators of modification (e.g., timestamps).

ICS T0851 Rootkit

Audit the integrity of PLC system and application code functionality, such as the manipulation of standard function blocks (e.g., Organizational Blocks) that manage the execution of application logic programs. [1]

ICS T0862 Supply Chain Compromise

Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses. Perform periodic integrity checks of the device to validate the correctness of the firmware, software, programs, and configurations. Integrity checks, which typically include cryptographic hashes or digital signatures, should be compared to those obtained at known valid states, especially after events like device reboots, program downloads, or program restarts.

ICS T0857 System Firmware

Perform integrity checks of firmware before uploading it on a device. Utilize cryptographic hashes to verify the firmware has not been tampered with by comparing it to a trusted hash of the firmware. This could be from trusted data sources (e.g., vendor site) or through a third-party verification service.

ICS T0864 Transient Cyber Asset

Integrity checking of transient assets can include performing the validation of the booted operating system and programs using TPM-based technologies, such as Secure Boot and Trusted Boot. [2] It can also include verifying filesystem changes, such as programs and configuration files stored on the system, executing processes, libraries, accounts, and open ports. [3]

ICS T0859 Valid Accounts

Routinely audit source code, application configuration files, open repositories, and public cloud storage for insecure use and storage of credentials.
