# Code Signing, Mitigation M0945 - ICS

By Authorization Enforcement

Archived: 2026-04-05 13:13:28 UTC

| Domain | ID | Name | Use |
|---|---|---|---|
| ICS | T0849 | Masquerading | Require signed binaries. |
| ICS | T0821 | Modify Controller Tasking | Utilize code signatures to verify the integrity and authenticity of programs installed on safety or control assets, including the associated controller tasking. |
| ICS | T0889 | Modify Program | Utilize code signatures to verify the integrity and authenticity of programs installed on safety or control assets. |
| ICS | T0839 | Module Firmware | Devices should verify that firmware has been properly signed by the vendor before allowing installation. |
| ICS | T0843 | Program Download | Utilize code signatures to verify the integrity and authenticity of programs downloaded to the device. |
| ICS | T0873 | Project File Infection | Allow for code signing of any project files stored at rest to prevent unauthorized tampering. Ensure the signing keys are not easily accessible on the same system. |
| ICS | T0851 | Rootkit | Digital signatures may be used to ensure application DLLs are authentic prior to execution. |
| ICS | T0862 | Supply Chain Compromise | When available utilize hardware and software root-of-trust to verify the authenticity of a system. This may be achieved through cryptographic means, such as digital signatures or hashes, of critical software and firmware throughout the supply chain. |

| Domain | ID | Name | Use |
| --- | --- | --- | --- |
| ICS | T0857 | System Firmware | Devices should verify that firmware has been properly signed by the vendor before allowing installation. |
| ICS | T0863 | User Execution | Prevent the use of unsigned executables, such as installers and scripts. |

---

Source: https://attack.mitre.org/mitigations/M0945