Modify Trusted Execution Environment, Technique T1399 - Mobile

Archived: 2026-04-05 16:47:36 UTC

Deprecation Warning

If an adversary can escalate privileges, he or she may be able to use those privileges to place malicious code in the device's Trusted Execution Environment (TEE) or other similar isolated execution environment where the code can evade detection, may persist after device resets, and may not be removable by the device user. Running code within the TEE may provide an adversary with the ability to monitor or tamper with overall device behavior.

Source: https://attack.mitre.org/techniques/T1399