Supply Chain Compromise: Compromise Hardware Supply Chain, Sub-technique T1195.003 - Enterprise

Archived: 2026-04-02 11:22:10 UTC

Other sub-techniques of Supply Chain Compromise (3)

Adversaries may manipulate hardware components in products prior to receipt by a final consumer for the purpose of data or system compromise. By modifying hardware or firmware in the supply chain, adversaries can insert a backdoor into consumer networks that may be difficult to detect and give the adversary a high degree of control over the system. Hardware backdoors may be inserted into various devices, such as servers, workstations, network infrastructure, or peripherals.

ⓘ

Platforms: Linux, Windows, macOS

Last Modified: 24 October 2025

Mitigations

ID	Mitigation	Description
M1046	Boot Integrity	Use Trusted Platform Module technology and a secure or trusted boot process to prevent system integrity from being compromised. Check the integrity of the existing BIOS or EFI to determine if it is vulnerable to modification. [1] [2]

Detection Strategy

ID	Name	Analytic ID	Analytic Description
DET0368	Hardware Supply Chain Compromise Detection via Host Status & Boot Integrity Checks	AN1035	Detects tampered hardware or firmware via anomalous host status telemetry. Behavioral chain: (1) Pre-OS or firmware components exhibit unexpected version changes, signature failures, or modified boot paths; (2) System management/firmware tools log hardware inventory drift; (3) Sensor health telemetry or boot attestation events fail baseline checks; (4) Follow-on process execution from altered firmware or unknown drivers after boot.
		AN1036	Monitors for hardware or firmware tampering by correlating system boot logs, hardware inventory changes, and secure boot/firmware verification failures. Behavioral chain: (1) UEFI/BIOS version drift; (2) secure boot disabled or signature verification errors; (3) unexpected modules or hardware devices enumerated at boot; (4) new device firmware images loaded from non-approved sources.
		AN1037	Detects tampered Mac hardware/firmware by analyzing unified logs, EndpointSecurity events, and Apple Mobile File Integrity (AMFI) checks. Behavioral chain: (1) Boot process reports firmware signature mismatch; (2) Secure Boot policy altered; (3) new EFI drivers or hardware devices appear in inventory; (4) system extension loads from unapproved developer IDs post-boot.

References

1. Trusted Computing Group. (2008, April 29). Trusted Platform Module (TPM) Summary. Retrieved June 8, 2016.
2. Microsoft. (n.d.). Secure the Windows 10 boot process. Retrieved April 23, 2020.