Impair Defenses: Safe Mode Boot, Sub-technique T1562.009 - Enterprise

Archived: 2026-04-05 15:58:41 UTC

Adversaries may abuse Windows safe mode to disable endpoint defenses. Safe mode starts up the Windows operating system with a limited set of drivers and services. Third-party security software such as endpoint detection and response (EDR) tools may not start after booting Windows in safe mode. There are two versions of safe mode: Safe Mode and Safe Mode with Networking. It is possible to start additional services after a safe mode boot.[1][2]

Adversaries may abuse safe mode to disable endpoint defenses that may not start with a limited boot. Hosts can be forced into safe mode after the next reboot via modifications to Boot Configuration Data (BCD) stores, which are files that manage boot application settings.[3]

Adversaries may also add their malicious applications to the list of minimal services that start in safe mode by modifying relevant Registry values (i.e. Modify Registry). Malicious Component Object Model (COM) objects may also be registered and loaded in safe mode.[2][4][5][6]

Source: https://attack.mitre.org/techniques/T1562/009