Impair Defenses: Downgrade Attack, Sub-technique T1562.010 - Enterprise

Archived: 2026-04-05 15:13:26 UTC

Adversaries may downgrade or use a version of system features that may be outdated, vulnerable, and/or does not support updated security controls. Downgrade attacks typically take advantage of a system's backward compatibility to force it into less secure modes of operation.

Adversaries may downgrade and use various less-secure versions of features of a system, such as Command and Scripting Interpreters or even network protocols that can be abused to enable Adversary-in-the-Middle or Network Sniffing.[1] For example, PowerShell versions 5+ includes Script Block Logging (SBL), which can record executed script content. However, adversaries may attempt to execute a previous version of PowerShell that does not support SBL with the intent to Impair Defenses while running malicious scripts that may have otherwise been detected.[2][3][4]

Adversaries may similarly target network traffic to downgrade from an encrypted HTTPS connection to an unsecured HTTP connection that exposes network data in clear text.[5][6] On Windows systems, adversaries may downgrade the boot manager to a vulnerable version that bypasses Secure Boot, granting the ability to disable various operating system security mechanisms.[7]

Source: https://attack.mitre.org/techniques/T1562/010