

Application Shimming Mitigation, Mitigation T1138 - Enterprise

By Authorization Enforcement

Archived: 2026-04-05 13:47:08 UTC

There currently aren't a lot of ways to mitigate application shimming. Disabling the Shim Engine isn't recommended because Windows depends on shimming for interoperability and software may become unstable or not work. Microsoft released an optional patch update - KB3045645 - that will remove the "auto-elevate" flag within the sdbinst.exe. This will prevent use of application shimming to bypass UAC.

Source: <https://attack.mitre.org/mitigations/T1138>