

AppInit DLLs and Secure Boot - Win32 apps

By stevewhims

Archived: 2026-04-05 17:12:31 UTC

Starting in Windows 8, the AppInit_DLLs infrastructure is disabled when secure boot is enabled.

About AppInit_DLLs

The AppInit_DLLs infrastructure provides an easy way to hook system APIs by allowing custom DLLs to be loaded into the address space of every interactive application. Applications and malicious software both use AppInit DLLs for the same basic reason, which is to hook APIs; after the custom DLL is loaded, it can hook a well-known system API and implement alternate functionality. Only a small set of modern legitimate applications use this mechanism to load DLLs, while a large set of malware use this mechanism to compromise systems. Even legitimate AppInit_DLLs can unintentionally cause system deadlocks and performance problems, therefore usage of AppInit_DLLs is not recommended.

AppInit_DLLs and secure boot

Windows 8 adopted UEFI and secure boot to improve the overall system integrity and to provide strong protection against sophisticated threats. When secure boot is enabled, the AppInit_DLLs mechanism is disabled as part of a no-compromise approach to protect customers against malware and threats.

Please note that secure boot is a UEFI protocol and not a Windows 8 feature. More info on UEFI and the secure boot protocol specification can be found at <https://www.uefi.org>.

AppInit_DLLs certification requirement for Windows 8 desktop apps

One of the certification requirements for Windows 8 desktop apps is that the app must not load arbitrary DLLs to intercept Win32 API calls using the AppInit_DLLs mechanism. For more detailed information about the certification requirements, refer to section 1.1 of [Certification requirements for Windows 8 desktop apps](#).

Summary

- The AppInit_DLLs mechanism is not a recommended approach for legitimate applications because it can lead to system deadlocks and performance problems.
- The AppInit_DLLs mechanism is disabled by default when secure boot is enabled.
- Using AppInit_DLLs in a Windows 8 desktop app is a Windows desktop app certification failure.

To download a whitepaper with info about AppInit_DLLs on Windows 7 and Windows Server 2008 R2, visit the [Windows Hardware Dev Center Archive](#), and search for *AppInit DLLs in Windows 7 and Windows Server 2008 R2*.

Source: <https://msdn.microsoft.com/en-us/library/dn280412>