Driver Load, Data Component DC0079

Archived: 2026-04-05 12:39:34 UTC

The process of attaching a driver, which is a software component that allows the operating system and applications to interact with hardware devices, to either user-mode or kernel-mode of a system. This can include benign actions (e.g., hardware drivers) or malicious behavior (e.g., rootkits or unsigned drivers). Examples:

- Legitimate Driver Loading: A new graphics driver from a vendor like NVIDIA or AMD is loaded into the system.
- Unsigned Driver Loading: A driver without a valid digital signature is loaded into the kernel.
- Rootkit Installation: A malicious rootkit driver is loaded to manipulate kernel-mode processes.
- Anti-Virus or EDR Driver Loading: An Endpoint Detection and Response (EDR) solution loads its driver to monitor system activities.
- Driver Misuse: A legitimate driver is loaded and exploited to execute malicious actions, such as using vulnerable drivers for bypassing defenses (e.g., Bring Your Own Vulnerable Driver (BYOVD) attacks).

Source: https://attack.mitre.org/datacomponents/DC0079