AppCert DLLs Registry Modification

Dynamic-link libraries (DLLs) that are specified in the AppCertDLLs value in the Registry key can be abused to obtain persistence and privilege escalation by causing a malicious DLL to be loaded and run in the context of separate processes on the computer.

id:	14f90406-10a0-4d36-a672-31cabe149f2f
categories:	enrich
confidence:	low
os:	windows
created:	7/26/2019
updated:	7/26/2019

MITRE ATT&CK™ Mapping

tactics:	Privilege Escalation, Persistence
techniques:	T1182 AppCert DLLs

Query

```
registry where registry_path == "*\\System\\ControlSet*\\Control\\Session Manager\\AppCertD
```

Contributors

- Endgame

Previous Next