

AppCert DLLs Registry Modification

MITRE ATT&CK™ Mapping

Query

Contributors

Audio Capture via PowerShell

Audio Capture via SoundRecorder

Bypass UAC via CMSTP

Bypass UAC via CompMgmtLauncher

Bypass UAC via Fodhelper.exe

Bypass UAC via Fodhelper.exe

Bypass UAC via WSReset.exe

Change Default File Association

Clearing Windows Event Logs with wevtutil

COM Hijack via Script Object

Command-Line Creation of a RAR file

Control Panel Items

Creation of an Archive with Common Archivers

Creation of Kernel Module

Creation of Scheduled Task with schtasks.exe

Creation or Modification of Systemd Service

Credential Enumeration via Credential Vault CLI

Delete Volume USN Journal with fsutil

Disconnecting from Network Shares with net.exe

Discovery and Enumeration of System Information via Rundll32

Discovery of a Remote System's Time

Discovery of Domain Groups

Discovery of Network Environment via Built-in Tools

Discovery of Network Environment via Built-in Tools

DLL Search Order Hijacking with known programs

Domain Trust Discovery

Domain Trust Discovery via Nltest.exe

Encoding or Decoding Files via CertUtil

Enumeration of Local Shares

Enumeration of Mounted Shares

Enumeration of Remote Shares

Enumeration of System Information

Enumeration of System Information

Executable Written and Executed by Microsoft Office Applications

Execution of a Command via a SYSTEM Service

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 ⏩

© Copyright 2019, Endgame Revision 30243396.

Built with [Sphinx](#) using a [theme](#) provided by [Read the Docs](#).