Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

nasbench / Misc-Research Public

Notifications Fork 16 Star 111

Code Issues Pull requests Actions Security Insights

Files

8ee690e

Go to file

BlueTeam-Atomics
LOLBINs
Other
Built-In-PowerShell-Aliases.md
Dism-Temporary-Directory.md
Documented-Compat-Applicati...
Documented-Compat-Applicati...
Finding-ShimDBC.md
Invoke-CommandInDesktopPac...
LibZ-Inject-Dll-Artefact.md
List-Of-Application-Calling-Regi...
Living-Of-The-SHIMS.md
Microsoft-Windows-Windows-F...
Notepad-TabState.md
Persistence-Via-RegisterAppRes...
PowerShell-Suspicious-Keyword...
UWP-Applications-Persistence.md
Undocumented-Flags-Sdbinst.md
POCs
Pentest
README.md

Misc-Research / Other / Undocumented-Flags-Sdbinst.md

nasbench Update Undocumented-Flags-Sdbinst.md 253a830 · last year History

Preview Code Blame 87 lines (60 loc) · 3.32 KB Raw

Undocumented CLI Flags - Sdbinst.EXE

The Application Compatibility Database Installer (sdbinst.exe) possess some undocumented flags that are often used by Windows itself.

Registry Cleaning - `-f`

> Note
>
> Available on Windows 10 & 11 versions

The `-f` flag will clean/delete the following registry keys and their values related to AppCompat

- `HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Persisted`
- `HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store`
- `HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers`
- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers`

SDB Cache Flush - `-c`

> Note
>
> Available on Windows 10 & 11 versions

The `-c` flag will call an internal function called `FlushCache` that flushes the cash by calling the API function ShimFlushCache from the `apphelp.dll`.

Testing Flag - `-t`

> Note
>
> Available on Windows 11 versions

The `-t` must be combined with the `w` flag. The purpose of this flag is to set an internal global variable called `g_msdbOperations` to the value of `0x20` (Hex) / `32` (Decimal)

```
case 't':
    if ( *((_WORD *)*v11 + 2) != 119 )
    {
LABEL_68:
        PrintMessage(0x3FEu);
        goto LABEL_284;
    }
    g_msdbOperations |= 0x20u;
    break;
```

When this value is set, the program will sleep for 20 seconds and then exit.

SDB Merges - `-m`

> Note
>
> Available on Windows 11 versions

The `-m` flag is used to initate the process of merging SBDs.

It can also be followed by another `m` (example: `-mm`) in order to perform a bitwise on the global variable `g_msdbFlags` with `1`. To be later tested to check if the process will enable background mode (see `-b` flag for more information).

During merge operations a temporary file might get created in the `%TEMP%` directory with the format `temp.{16-Random-Hex-Chars}.sdb` (Example: `temp.01DA2456E502A0F0.sdb`)

Usually this flag is called by the `PcaSvc` service from `svchost` in the following form

```
sdbinst.exe -mm
sdbinst.exe  -m -bg
```

Information about the merged SDBs and others are stored in the registry key `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\SdbUpdates`

Internally this operation is via a function called `MergeSdb_FindAndMergeForTarget` called from `HandleCheckForMergeUpdate`.

Background Execution - `-b`

> Note
>
> Available on Windows 11 versions

he `-b` must be combined with the `g` flag. The purpose is to set an internal global variable called `g_msdbFlags` to the value of `4`. Which is later used to call SetPriorityClass in order to set the process mode to background or in other terms `PROCESS_MODE_BACKGROUND_BEGIN`.

And it also calls SetProcessWorkingSetSizeEx to set the minimum and maximum working set sizes for the specified process.

```
case 'b':
    if ( *((_WORD *)*v11 + 2) != 103 )
        goto LABEL_68;
    g_msdbFlags |= 4u;
    goto LABEL_61
```