



## KB4078130 deaktiviert den Spectre 2 Patch

### Microsoft Update Catalog:

Download für

Windows 10, Windows 10 LTSB, Windows 7, Windows 8.1, Windows Embedded Standard 7, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016

<https://www.catalog.update.microsoft.com/Search.aspx?q=KB4078130>

### Was macht das Update?

Der Critical Patch setzt diese Registrierungseinträge, um die vorrangegangenen [Patche gegen Spectre 2](#) zu deaktivieren,

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverride /t REG_DWORD /d 3 /f
```

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverrideMask /t REG_DWORD /d 3 /f
```

```
Administrator: Eingabeaufforderung
Microsoft Windows [Version 10.0.16299.192]
(c) 2017 Microsoft Corporation. Alle Rechte vorbehalten.

C:\WINDOWS\system32>reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverride /t REG_DWORD /d 3 /f
Der Vorgang wurde erfolgreich beendet.

C:\WINDOWS\system32>reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverrideMask /t REG_DWORD /d 3 /f
Der Vorgang wurde erfolgreich beendet.

C:\WINDOWS\system32>
```

Wer den Patch wieder aktivieren möchte, der führt diese Befehle aus:

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverride /t REG_DWORD /d 0 /f
```

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverrideMask /t REG_DWORD /d 3 /f
```

```
Administrator: Eingabeaufforderung
C:\WINDOWS\system32>reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverride /t REG_DWORD /d 0 /f
Der Vorgang wurde erfolgreich beendet.

C:\WINDOWS\system32>reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverrideMask /t REG_DWORD /d 3 /f
Der Vorgang wurde erfolgreich beendet.

C:\WINDOWS\system32>
```



## KB4078130 deaktiviert den Spectre 2 Patch

Weitere Informationen auf den Seiten von Microsoft

<https://support.microsoft.com/en-us/help/4073119/protect-against-speculative-execution-side-channel-vulnerabilities-in>

### Powershell – Spectre Schutz Check:

Install-Module SpeculationControl

\$SaveExecutionPolicy = Get-ExecutionPolicy

Set-ExecutionPolicy RemoteSigned -Scope Currentuser

Import-Module SpeculationControl

Get-SpeculationControlSettings

Set-ExecutionPolicy \$SaveExecutionPolicy -Scope Currentuser

```
Administrator: Windows PowerShell ISE (x86)
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe
Spectre Schutz Check.ps1 X
1 Install-Module SpeculationControl
2
3 $SaveExecutionPolicy = Get-ExecutionPolicy
4
5 Set-ExecutionPolicy RemoteSigned -Scope Currentuser
6 Import-Module SpeculationControl
7 Get-SpeculationControlSettings
8
9 Set-ExecutionPolicy $SaveExecutionPolicy -Scope Currentuser

PS C:\WINDOWS\system32> Install-Module SpeculationControl
PS C:\WINDOWS\system32> $SaveExecutionPolicy = Get-ExecutionPolicy
PS C:\WINDOWS\system32> Set-ExecutionPolicy RemoteSigned -Scope Currentuser
Import-Module SpeculationControl
Get-SpeculationControlSettings
Speculation control settings for CVE-2017-5715 [branch target injection]
For more information about the output below, please refer to https://support.microsoft.com/en-in/help/4074629

Hardware support for branch target injection mitigation is present: False
Windows OS support for branch target injection mitigation is present: True
Windows OS support for branch target injection mitigation is enabled: False
Windows OS support for branch target injection mitigation is disabled by system policy: False
Windows OS support for branch target injection mitigation is disabled by absence of hardware support: True

Speculation control settings for CVE-2017-5754 [rogue data cache load]

Hardware requires kernel VA shadowing: True
Windows OS support for kernel VA shadow is present: True
Windows OS support for kernel VA shadow is enabled: True
Windows OS support for PCID performance optimization is enabled: True [not required for security]

Suggested actions

* Install BIOS/firmware update provided by your device OEM that enables hardware support for the branch target i
njection mitigation.

BTIHardwarePresent           : False
BTIWindowsSupportPresent    : True
BTIWindowsSupportEnabled    : False
BTIDisabledBySystemPolicy    : False
BTIDisabledByNoHardwareSupport : True
KVAshadowRequired           : True
KVAshadowWindowsSupportPresent : True
KVAshadowWindowsSupportEnabled : True
KVAshadowPcidEnabled        : True
```

<https://gallery.technet.microsoft.com/scriptcenter/Speculation-Control-e36f0050>