



LDAP SSL/TLS CVE-2017-8563

Ungeschützte Schwachstelle im LDAP Protokoll sowie im RDP Protokoll mit dem Optionsschalter RestrictedAdmin.

<https://portal.msrc.microsoft.com/en-us/security-guidance>

Microsoft hat zum Schließen der Lücke am 11.7.2017 ein Patch rausgebracht.

Download:

<https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8563>

Das Update sollte schnellst möglich ausgerollt werden, jedoch gibt es nach der Installation weitere Konfigurationsschritte umzusetzen. Das Update bringt lediglich eine Schalterfunktion mit, die erst über einen Eintrag in der Registry aktiviert werden muss.

Und zwar geht es hier um den Schalter **LdapEnforceChannelBinding**. Erst wenn dieser Schalter mit dem Wert = 1 aktiviert wird, steht der erhöhte Schutz zur Verfügung.

Pfad: **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters**

Schlüssel: **LdapEnforceChannelBinding**

- DWORD-Wert = **0**
> deaktiviert
- DWORD-Wert = **1**
> aktiviert wenn vom Client unterstützt wird
- DWORD-Wert = **2**
> immer aktiviert; alle Clients müssen die die Kanalbindungsinformation vorlegen

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters]

"LdapEnforceChannelBinding"=dword:00000002

Folgende Schritte sind zu tun:

- Installation des jeweiligen Updates passend zum OS
- Aktivieren der Funktion auf den DCs über den Registry-Schalter
 - Zur Kompatibilitätsverbesserung den Wert = 1 setzen
 - Wer keinen Windows Server 2008 mehr einsetzt sollte den Wert = 2 setzen

Darüber hinaus sollte geprüft werden ob LDAP Signing und SMB Signing aktiviert ist.

Mit diesem Befehl prüfen wir z.B. WIN10 v1703, ob das Update bereits installiert ist:

wmic qfe | findstr KB4025342

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> wmic qfe | findstr KB4025342
http://support.microsoft.com/?kbid=4025342  WORKER  Security Update  KB4025342  NT-AUTORIT?T\SYSTEM  7/30/2017
PS C:\WINDOWS\system32> winver
PS C:\WINDOWS\system32>
```



LDAP SSL/TLS CVE-2017-8563

Server 2016 = DC01

```
Administrator: Eingabeaufforderung
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Windows\system32>wmic qfe | findstr KB4025339
http://support.microsoft.com/?kbid=4025339 DC01 Security Update KB4025339 NT-AUTORITÄT\SYSTEM 7/11/2017

C:\Windows\system32>whoami
ndsedv\nds

C:\Windows\system32>hostname
DC01

C:\Windows\system32>_
```

Server 2012 R2 = SRV01

```
Administrator: Eingabeaufforderung
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Windows\system32>wmic qfe | findstr KB4025333

C:\Windows\system32>wmic qfe | findstr KB4025336
http://support.microsoft.com/?kbid=4025336 SRV01 Security Update
KB4025336 NT-AUTORITÄT\SYSTEM 7/23/2017

C:\Windows\system32>hostname
SRV01

C:\Windows\system32>whoami
ndsedv\nds

C:\Windows\system32>
```