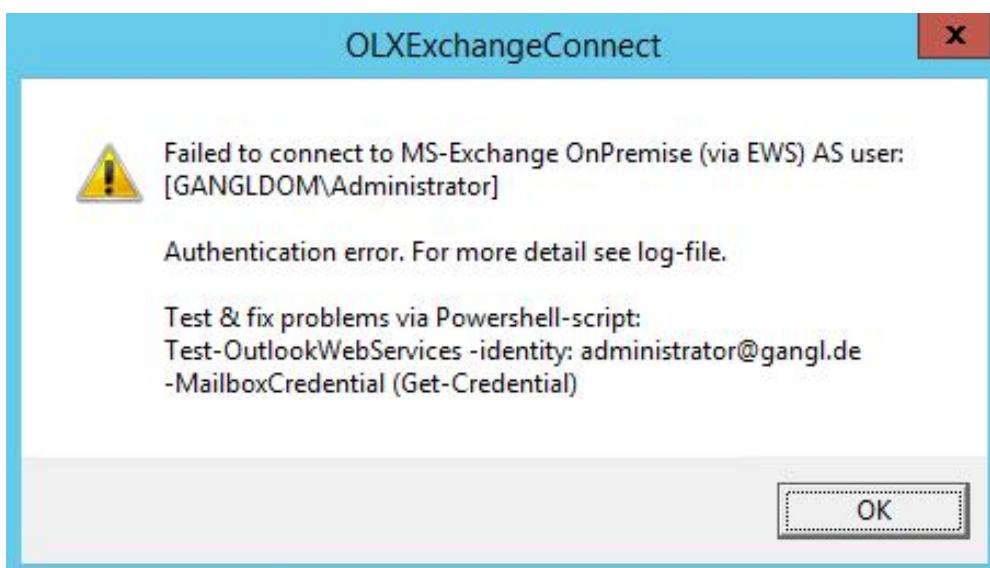


Was tun bei Authentication error?



Ursache

CVE-2019-0586 | Microsoft Exchange Memory Corruption Vulnerability

CVE-2019-0588 | Microsoft Exchange Information Disclosure Vulnerability

CVE-2018-8581 | Microsoft Exchange Server Elevation of Privilege Vulnerability

Exchange 2013 CU 22 (und folgende)

Exchange 2016 CU 12 (und folgende)

Exchange 2019 CU 1 (und folgende)

Registrykey: DisableLoopBackCheck

Hinweis

Es handelt sich hierbei grundsätzlich um fehlschlagendes AutoDiscover!

Das Problem existiert NUR direkt auf dem Exchange!

Alternativ könnten Sie den OLXAgent auch auf einem anderen Computer installieren und betreiben denn dann existiert dies MS-Problem nicht.

Nachstehende Schritte sind somit nur dann durchzuführen wenn der OLXAgent DIREKT auf dem Exchange betrieben wird

Schritt 1

Nachstehender Registrykey wird von obigen neuen Exchange-Versionen automatisch entfernt:

Registrierungs-Editor																																																																					
Datei	Bearbeiten	Ansicht	Favoriten ?																																																																		
			<table><thead><tr><th>Name</th><th>Typ</th><th>Daten</th></tr></thead><tbody><tr><td>(Standard)</td><td>REG_SZ</td><td>(Wert nicht festgelegt)</td></tr><tr><td>auditbasedirectories</td><td>REG_DWORD</td><td>0x00000000 (0)</td></tr><tr><td>auditbaseobjects</td><td>REG_DWORD</td><td>0x00000000 (0)</td></tr><tr><td>Authentication Packages</td><td>REG_MULTI_SZ</td><td>msv1_0</td></tr><tr><td>Bounds</td><td>REG_BINARY</td><td>00 30 00 00 00 20 00 00</td></tr><tr><td>crashonauditfail</td><td>REG_DWORD</td><td>0x00000000 (0)</td></tr><tr><td>disabledomaincreds</td><td>REG_DWORD</td><td>0x00000000 (0)</td></tr><tr><td>DisableLoopbackCheck</td><td>REG_DWORD</td><td>0x00000001 (1)</td></tr><tr><td>everyoneincludesanonymous</td><td>REG_DWORD</td><td>0x00000000 (0)</td></tr><tr><td>forceguest</td><td>REG_DWORD</td><td>0x00000000 (0)</td></tr><tr><td>fullprivilegeauditing</td><td>REG_BINARY</td><td>00</td></tr><tr><td>LimitBlankPasswordUse</td><td>REG_DWORD</td><td>0x00000001 (1)</td></tr><tr><td>LsaPid</td><td>REG_DWORD</td><td>0x00000260 (608)</td></tr><tr><td>NoLmHash</td><td>REG_DWORD</td><td>0x00000001 (1)</td></tr><tr><td>Notification Packages</td><td>REG_MULTI_SZ</td><td>rassfm scecli</td></tr><tr><td>ProductType</td><td>REG_DWORD</td><td>0x00000007 (7)</td></tr><tr><td>restrictanonymous</td><td>REG_DWORD</td><td>0x00000000 (0)</td></tr><tr><td>restrictanonymoussam</td><td>REG_DWORD</td><td>0x00000001 (1)</td></tr><tr><td>SecureBoot</td><td>REG_DWORD</td><td>0x00000001 (1)</td></tr><tr><td>Security Packages</td><td>REG_MULTI_SZ</td><td>""</td></tr><tr><td>UseMachineId</td><td>REG_DWORD</td><td>0x00000001 (1)</td></tr></tbody></table>	Name	Typ	Daten	(Standard)	REG_SZ	(Wert nicht festgelegt)	auditbasedirectories	REG_DWORD	0x00000000 (0)	auditbaseobjects	REG_DWORD	0x00000000 (0)	Authentication Packages	REG_MULTI_SZ	msv1_0	Bounds	REG_BINARY	00 30 00 00 00 20 00 00	crashonauditfail	REG_DWORD	0x00000000 (0)	disabledomaincreds	REG_DWORD	0x00000000 (0)	DisableLoopbackCheck	REG_DWORD	0x00000001 (1)	everyoneincludesanonymous	REG_DWORD	0x00000000 (0)	forceguest	REG_DWORD	0x00000000 (0)	fullprivilegeauditing	REG_BINARY	00	LimitBlankPasswordUse	REG_DWORD	0x00000001 (1)	LsaPid	REG_DWORD	0x00000260 (608)	NoLmHash	REG_DWORD	0x00000001 (1)	Notification Packages	REG_MULTI_SZ	rassfm scecli	ProductType	REG_DWORD	0x00000007 (7)	restrictanonymous	REG_DWORD	0x00000000 (0)	restrictanonymoussam	REG_DWORD	0x00000001 (1)	SecureBoot	REG_DWORD	0x00000001 (1)	Security Packages	REG_MULTI_SZ	""	UseMachineId	REG_DWORD	0x00000001 (1)
Name	Typ	Daten																																																																			
(Standard)	REG_SZ	(Wert nicht festgelegt)																																																																			
auditbasedirectories	REG_DWORD	0x00000000 (0)																																																																			
auditbaseobjects	REG_DWORD	0x00000000 (0)																																																																			
Authentication Packages	REG_MULTI_SZ	msv1_0																																																																			
Bounds	REG_BINARY	00 30 00 00 00 20 00 00																																																																			
crashonauditfail	REG_DWORD	0x00000000 (0)																																																																			
disabledomaincreds	REG_DWORD	0x00000000 (0)																																																																			
DisableLoopbackCheck	REG_DWORD	0x00000001 (1)																																																																			
everyoneincludesanonymous	REG_DWORD	0x00000000 (0)																																																																			
forceguest	REG_DWORD	0x00000000 (0)																																																																			
fullprivilegeauditing	REG_BINARY	00																																																																			
LimitBlankPasswordUse	REG_DWORD	0x00000001 (1)																																																																			
LsaPid	REG_DWORD	0x00000260 (608)																																																																			
NoLmHash	REG_DWORD	0x00000001 (1)																																																																			
Notification Packages	REG_MULTI_SZ	rassfm scecli																																																																			
ProductType	REG_DWORD	0x00000007 (7)																																																																			
restrictanonymous	REG_DWORD	0x00000000 (0)																																																																			
restrictanonymoussam	REG_DWORD	0x00000001 (1)																																																																			
SecureBoot	REG_DWORD	0x00000001 (1)																																																																			
Security Packages	REG_MULTI_SZ	""																																																																			
UseMachineId	REG_DWORD	0x00000001 (1)																																																																			

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

- > Ohne diesen Registrykey schlägt jegliches Autodiscover fehl
- > 401 Unauthorized wird erscheinen

Schritt 2 Exchange-ManagementShell

Prüfen ob Autodiscover (direkt auf dem Server) ohne Fehler klappt:

```
Test-OutlookWebServices -identity: xxx@mydomain.com -MailboxCredential (Get-Credential)
```

Source	ServiceEndpoint	Scenario	Result	Latency (MS)
EX2013.gangldom.intern	XXX	AutoErmittlung: Outlook-Anb...	Failure	44
EX2013.gangldom.intern		Exchange-Webservices	Skipped	0
EX2013.gangldom.intern		Verfügbarkeitsdienst	Skipped	0
EX2013.gangldom.intern		Offlineaddressbuch	Skipped	0

Wenn bei Autodiscover **Failure** erscheint:

```
Test-OutlookWebServices -identity: xxx@mydomain.com -MailboxCredential (Get-Credential) | fl
```

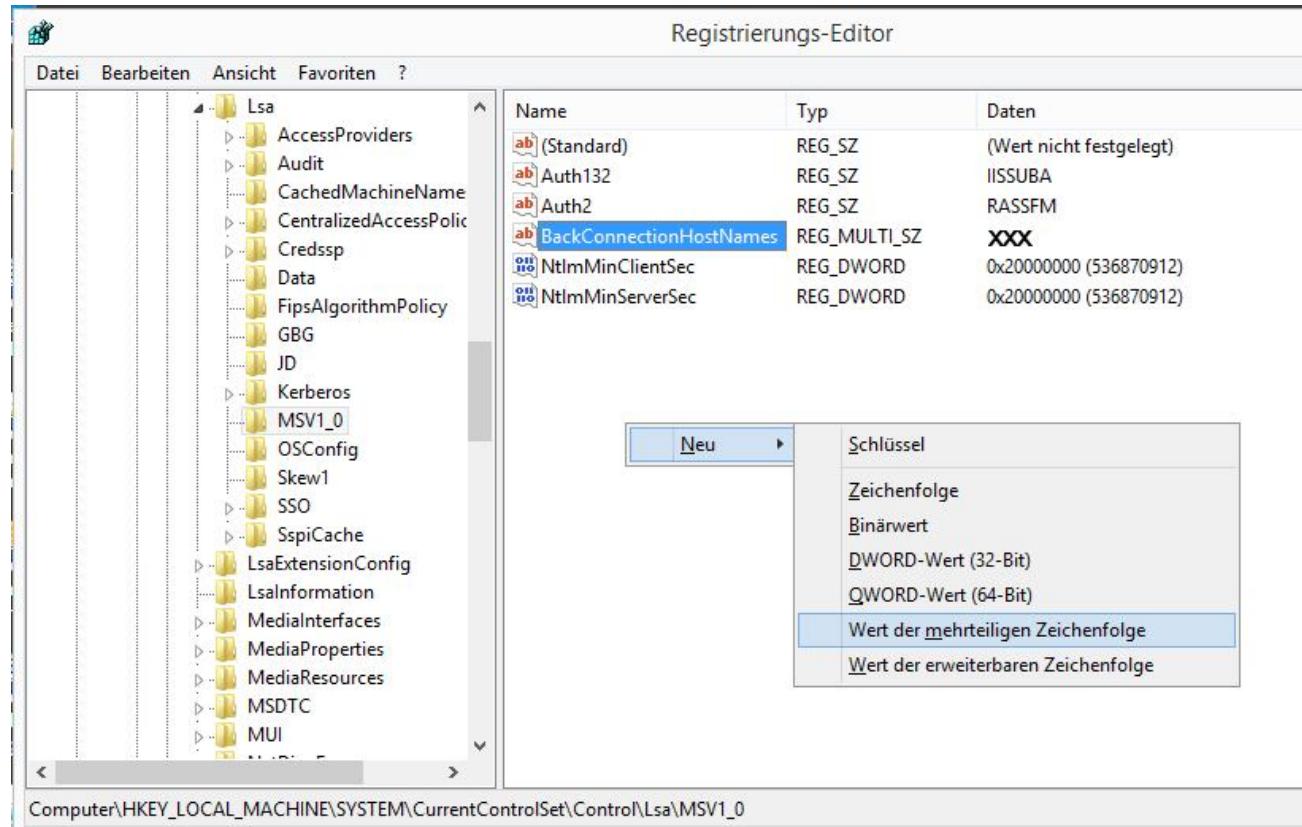
Im Output diesen Eintrag suchen:

```
</Autodiscover>
[2019-03-14 06:02:14Z] Antwort von AutoErmittlung:
request-id: e6292b6e-d4e4-4390-882b-bf165bf9903b
Server: Microsoft-IIS/8.5
WWW-Authenticate: NTLM,Negotiate,Basic realm="XXX "
X-Powered-By: ASP.NET
X-FEServer: EX2013
Date: Thu, 14 Mar 2019 06:02:14 GMT
Content-Length: 0
[2019-03-14 06:02:14Z] Antwort von AutoErmittlung:
System.Net.WebException: Der Remoteserver hat einen Fehler zurückgegeben: <401> Nicht
autorisiert.
bei System.Net.HttpWebRequest.GetResponse()
bei
Microsoft.Exchange.Management.SystemConfigurationTasks.ServiceValidatorBase.InternalInvoke()
bei Microsoft.Exchange.Management.SystemConfigurationTasks.ServiceValidatorBase.Invoke()
```

Dieser Wert (**XXX**) muss für den nachfolgenden neuen Registrykey verwendet werden!

Schritt 3 Regedit

Diesen Registrykey neu erstellen:



<https://support.microsoft.com/en-ca/help/896861/you-receive-error-401-1-when-you-browse-a-web-site-that-uses-integrate>

Schritt 4 IIS

Gegebenenfalls den IIS restarten. Allerdings war dies in unseren Tests nicht einmal nötig.

Schritt 5 Exchange-ManagementShell

Erneut prüfen ob Autodiscover (direkt auf dem Server) ohne Fehler klappt:

`Test-OutlookWebServices -identity: xxx@mydomain.com -MailboxCredential (Get-Credential)`

Source	ServiceEndpoint	Scenario	Result	Latency (MS)
EX2013.gangldom.intern	XXX	AutoErmittlung: Outlook-Anb...	Success	44
EX2013.gangldom.intern		Exchange-Webdienste	Success	0
EX2013.gangldom.intern		Verfügbarkeitsdienst	Success	0
EX2013.gangldom.intern		Offlineaddressbuch	Success	0

BINGO!

Schritt 6 Exchange-ManagementShell

Vulnerability prüfen!

HealthChecker.ps1

<https://gallery.technet.microsoft.com/office/Exchange-2013-Performance-23bcca58>

```
Hotfix Check:  
KB3041832 is Installed  
  
Exchange Web App Pools - GC Server Mode Enabled : Status:  
MSExchangeOWAAppPool: false | Started  
MSExchangeRpcProxyAppPool: false | Started  
MSExchangeMapiAddressBookAppPool: false | Started  
MSExchangeRpcProxyFrontEndAppPool: false | Started  
MSExchangePowerShellAppPool: false | Started  
MSExchangePowerShellFrontEndAppPool: false | Started  
MSExchangeMapiFrontEndAppPool: false | Started  
MSExchangeMapiMailboxAppPool: false | Started  
MSExchangeOABAAppPool: false | Started  
MSExchangePushNotificationsAppPool: false | Started  
MSExchangeOWACalendarAppPool: false | Started  
MSExchangeAutodiscoverAppPool: false | Started  
MSExchangeECPAppPool: false | Started  
MSExchangeSyncAppPool: false | Started  
MSExchangeServicesAppPool: false | Started  
  
Vulnerability Check:  
All known security issues in this version of the script passed.
```

OLXAgents

Microsoft Outlook®
Microsoft Exchange®
aus der Reihe **Solutions** 
„Praxisorientierte Tools“ für

MS-Outlook

und

MS-ExchangeServer

Copyright by

GANGL
DIENSTLEISTUNGEN

Nelkenstrasse 16
73540 Heubach-Lautern
Tel: +49 (7173) 92 90 53
E-Mail: info@gangl.de
Internet: <https://www.gangl.de>