Situatie:
t.b.v. testdoeleinden heb ik op mijn testomgeving de Secunia SCI software geïnstalleerd. Deze mocht ik voor ca. 14 dagen gebruiken. Toen de testperiode voorbij was lukt het niet meer om in te loggen op de console. Omdat ik klaar was met testen heb ik de secunia CSI software gedeinstalleerd en de agents gedeinstalleerd van de clients. Nu treed het verschijnsel op dat na het deinstalleren van de CSI-Agent deze door het Windows-Update mechanisme weer wordt gedetecteerd om te worden geinstalleerd. Een blik in WindowsUpdate.log van een client.

2011-06-05 16:30:52:391 1084 edc DnldMgr ** START ** DnldMgr: Downloading updates [CallerId = AutomaticUpdates]
2011-06-05 16:30:52:391 1084 edc DnldMgr *********
2011-06-05 16:30:52:391 1084 edc DnldMgr * Call ID = {A4A605F8-C0A3-44DA-A7FA-D29D8C2C0AEA}
2011-06-05 16:30:52:391 1084 edc DnldMgr * Priority = 2, Interactive = 0, Owner is system = 1, Explicit proxy = 0, Proxy session id = -1, ServiceId = {3DA21691-E39D-4DA6-8A4B-B43877BCB1B7}
2011-06-05 16:30:52:391 1084 edc DnldMgr * Updates to download = 1
2011-06-05 16:30:52:391 1084 edc Agent * Title = Deployment package for Secunia CSI Agent 4.x, version 4.1.0.2002, created Mon May 16 16:55:07 UTC+0200 2011
2011-06-05 16:30:52:391 1084 edc Agent * UpdateId = {0E663A62-E62B-422E-938B-A2A55467A056}.1
2011-06-05 16:30:52:407 1084 edc DnldMgr ********** DnldMgr: New download job [UpdateId = {0E663A62-E62B-422E-938B-A2A55467A056}.1] **********
2011-06-05 16:30:52:969 1084 edc DnldMgr * BITS job initialized, JobId = {634BF3A5-3B54-4520-B7C5-A113482A27A5}
2011-06-05 16:30:53:031 1084 edc DnldMgr * Downloading from http://xxxx-3.int.xxx.xx:8530/Content/A4/F3A01EE11E7223B03B6D92BEA88245C4EEB13DA4.cab
to C:WINDOWSSoftwareDistributionDownload2b2a9a54bdbfe944aada70d198f07596f3a01ee11e7223b03b6d92bea88245c4eeb13da4 (full file).
2011-06-05 16:30:53:156 1084 edc Agent *********
2011-06-05 16:30:53:156 1084 edc Agent ** END ** Agent: Downloading updates [CallerId = AutomaticUpdates]
2011-06-05 16:30:53:156 1084 edc Agent **********

Probleem/Problem:
De updates die waren gepubliceerd door de Secunia CSI (via SCUP Api) staan nog op de WSUS server. In het Wsus console zijn deze updates - helaas - niet te zien, dus daarmee zijn ze niet verwijderen/deactiveren. Tevens is het console van de Secunia SCI niet meer te openen omdat het inlogaccount is verlopen.

Oplossing/Sollution:

Met Windows PowerShell op de Wsus server zijn de updates te verwijderen.

1 - Start Powershell

2 -

```
PS C:> [reflection.assembly]::LoadWithPartialName("Microsoft.UpdateServices.Administration")
GAC    Version        Location
---    -------        --------
True   v2.0.50727
C:WINDOWSassemblyGAC_MSILMicrosoft.UpdateServices.Administration3.1.6001.1__31bf3856  3-
PS C:> $wsussrv = [Microsoft.UpdateServices.Administration.AdminProxy]::GetUpdateServer()
PS C:> $wsussrv

WebServiceUrl                :  https://xxx-3.int.xxx.xx:8531/ApiRemoting30/WebService.asmx
BypassApiRemoting            : False
IsServerLocal                : True
Name                         : xxx-3.int.xxx.xx
Version                      : 3.2.7600.226
IsConnectionSecureForApiRemoting : True
PortNumber                   : 8531
PreferredCulture             : en
ServerName                   : xxx-3.int.xxx.xx
ServerProtocolVersion        : 1.8
```

4- Selecteer / Select Secunia CSI updates

```
PS C:> $secuniaupdates = $wsussrv.GetUpdates() | select * | Where-Object {$_.Description
-like "*Made by the Secunia CSI*"}
```

5- Show update ID's (vergelijk ter controle de update-ID met het ID uit WindowsUpdate.log)

```
  PS C:> $secuniaupdates|ForEach-Object {$_.id.updateid.tostring()}
0e663a62-e62b-422e-938b-a2a55467a056
8597335e-4852-40f0-97c2-cb30f98cec8a
db86f422-839b-4f07-b019-7a78e6deda07
07153032-e03f-48c5-b272-ac57fe198bce
2764f572-b79a-4f83-a51c-b5e5e5c90487
2f71f044-a739-4eee-8559-1dfbbffbbe5f
3761c4b8-6c61-4ac7-8474-493e53b1ed94
e92b0563-7a65-419c-98d3-b0d4fa23ba84
745845ed-be97-4c42-aa14-47f553be2518
4425d811-915b-4ba0-bdc1-022b3d291cb2
```

05add902-872e-4dbb-a919-7002ae6d76cf
d792ea97-bbd2-49ec-b7d9-910a345f3c3b
79799435-66a8-47cb-9209-dc9aa1a24eec
2210c0b2-2925-4eac-9b6e-bb5059f2b01b
b899ce0d-ba9e-42f0-b5a3-7479f80b437e
c10ba14e-0c95-44e9-8b39-0912b2cbc16f

6- Expire the Secunia CSI updates

```
PS C:> $secuniaupdates|ForEach-Object {$wsusrv.ExpirePackage($_.id)}
```

7- Start in de Wsus console , Options, Server Cleanup Wizard (selecteer alles)

8- Start op een client wuauclt /detectnow en controleer windowsupdate.log
> WindowsUpdate.log
Windows Update Client successfully detected 0 updates.

9- De status in Wsus is aangepast
before/voor:

```
UpdateServer  : Microsoft.UpdateServices.Internal.BaseApi.UpdateServer
Id            : Microsoft.UpdateServices.Administration.UpdateRevisionId
Title                 : Wireshark 0.x, version 1.x, Highly critica
                        l
Description               : Made by the Secunia CSI
                      csi_product_id:1228
                      csi_version:1.x
LegacyName                :
MsrcSeverity              : Unspecified
KnowledgebaseArticles     : {}
SecurityBulletins         : {}
AdditionalInformationUrls : {}
ReleaseNotes              :
UpdateClassificationTitle : Security Updates
CompanyTitles             : {Wireshark Foundation}
ProductTitles             : {Wireshark 0.x}
ProductFamilyTitles       : {}
IsLatestRevision          : True
HasEarlierRevision        : False
Size                  : 0
CreationDate              : 17-5-2011 10:19:01
ArrivalDate               : 17-5-2011 10:20:00
```

UpdateType : Software
PublicationState : Published
InstallationBehavior : Microsoft.UpdateServices.Administration.In
stallationBehavior
UninstallationBehavior : Microsoft.UpdateServices.Administration.In
stallationBehavior
IsBeta : False
HasStaleUpdateApprovals : False
IsApproved : True
IsDeclined : False
DefaultPropertiesLanguage :
HasLicenseAgreement : False
RequiresLicenseAgreementAcceptance : False
State : Ready
HasSupersededUpdates : False
IsSuperseded : False
IsWsusInfrastructureUpdate : False
IsEditable : True
UpdateSource : Other

after/na:

UpdateServer : Microsoft.UpdateServices.Internal.BaseApi.UpdateServer
Id : Microsoft.UpdateServices.Administration.UpdateRevisionId
Title : Wireshark 0.x, version 1.x, Highly critical
Description : Made by the Secunia CSI
csi_product_id:1228
csi_version:1.x
LegacyName :
MsrcSeverity : Unspecified
KnowledgebaseArticles : {}
SecurityBulletins : {}
AdditionalInformationUrls : {}
ReleaseNotes :
UpdateClassificationTitle : Security Updates
CompanyTitles : {Wireshark Foundation}
ProductTitles : {Wireshark 0.x}
ProductFamilyTitles : {}
IsLatestRevision : True
HasEarlierRevision : False
Size : 0
CreationDate : 17-5-2011 10:19:01
ArrivalDate : 14-6-2011 12:27:43
UpdateType : Software
PublicationState : Expired
InstallationBehavior : Microsoft.UpdateServices.Administration.InstallationBehavior

UninstallationBehavior : Microsoft.UpdateServices.Administration.InstallationBehavior
IsBeta : False
HasStaleUpdateApprovals : False
IsApproved : False
IsDeclined : True
DefaultPropertiesLanguage :
HasLicenseAgreement : False
RequiresLicenseAgreementAcceptance : False
State : NotNeeded
HasSupersededUpdates : False
IsSuperseded : False
IsWsusInfrastructureUpdate : False
IsEditable : True
UpdateSource : Other

bronnen: How to remove orphaned SCUP updates… en How to: Expire a Custom Update in WSUS Using PowerShell